မျက်မှောင်စေပေ

INTERNET Security

မျိုးသူရ

- Virus များအား ရှာဖွေရှင်းလင်းနည်းများ
- Virus Definiction အသစ်များ Update လုပ်နည်းများအကြောင်း
- လျှို့ဝှက်ထောက်လှမ်းနိုင်သောနှင့် Spy Software များအကြောင်း
- Computer Virus ဆိုတာဘာလဲ၊ ဘယ်လိုပြန့်နှံ့သွားကြသလဲ
- Virus ကာကွယ်နိုင်သော Software အသုံးပြုနည်းများ
- Virus အန္တရာယ်ကာကွယ်နိုင်မည့် Avira နှင့် KasperSky Software
- Hacker များနှင့် Introder များရန်မှ ကာကွယ်ပေးနေသည့် Firewall များအကြောင်း
- မလိုလားအပ်သော Mail များရှင်းလင်းတားဆီးခြင်း၊ Window Registry လုပ်ခြင်း

မျိုးသူရ

openeyes@mail4u.com.mm

INTERNET Security

ပုံနှိပ်မှတ်တမ်း

စာမူခွင့်ပြုချက်အမှတ် – ၄၀၁၁၈၇၀၉၀၉

မျက်နှာဖုံးခွင့်ပြုချက် - ၄၀၁၁၁၄၁၁၀၉

ပုံနှိပ်ခြင်း – ပထမအကြိမ်၊ အုပ်ရေ–(၅၀၀)

ထုတ်ဝေသည့်ကာလ – ၂၀၀၉ ခုနှစ်၊ နိုဝင်ဘာ

ထုတ်ဝေသူ – ဦးမျိုးမင်းသန်း

မျက်ပွင့်စာပေ (၀၄၁၃၃)

အမှတ် (၃၆၇)၊ ဗိုလ်ချုပ်အောင်ဆန်းလမ်း၊

ပန်းဘဲတန်းမြို့နယ်၊ ရန်ကုန်မြို့။

အတွင်းမျက်နှာဖုံးပုံနှိပ် – ဦးဇော်မင်းအေး

ဇော်ပုံနှိပ်တိုက် (၀၅၀၁၂၅)

အမှတ် (၃၈၆)၊ အင်ကြင်းမြို့ငယ်လမ်း၊

သဃ်္ခန်းကျန်းမြို့နယ်၊ ရန်ကုန်မြို့။

တန်ဖိုး

မျိုးသူရ CIP - ၂ ၀၀၆

Internet Security

- ရန်ကုန်။

မျက်ပွင့်စာပေ၊ ၂၀၀၉။

၁၅၂ – စာ၊ ၁၈ x ၂၅ စင်တီ။

(၁) Internet Security

ဖြန့်ချိရေး

မျက်ပွင့်စာပေ

အမှတ် (၃၆၇)၊ ဗိုလ်ချုပ်အောင်ဆန်းလမ်း။ (ဗိုလ်ဆွန်ပက်လမ်းထိပ်)၊ ရန်ကုန်မြို့။

ဖုန်း – ၇၀၀၅၇၇၉၊ ၀၉၅၁–၄၈၅၅၀

INTERNET Security

မျိုးသူရ

- Virus များအားရှာဖွေ ရှင်းလင်းနည်းများ
- Virus Definiction အသစ်များ Update လုပ်နည်းများအကြောင်း
- လျှို့ဝှက်ထောက်လှမ်းနိုင်သောနှင့် Spy Software များအကြောင်း
- Computer Virus ဆိုတာဘာလဲ၊ ဘယ်လိုပြန့်နှံ့သွားကြသလဲ
- Virus ကာကွယ်နိုင်သော Software အသုံးပြုနည်းများ
- Virus အန္တရာယ်ကာကွယ်နိုင်မည့် Avira နှင့် Kasper Sky Software
- Hacker များနှင့် Introder များရန်မှ ကာကွယ်ပေးနေသည့် Firewall များအကြောင်း
- မလိုလားအပ်သော Mail များရှင်းလင်းတားဆီးခြင်း။ Window Registry လုပ်ခြင်း

မျိုးသူရ

မျက်မှောက် စာပေဖြန့်ချိရေး

openeyes@mail4u.com.mm

(၃၄၇)၊ မိုလ်ချုပ်အောင်ဆန်းလမ်း။ မိုလ်ဆွန်ပတ်လမ်းထိပ်၊ ရန်ကုန်။ ဖုန်း - ၇၀၀၅၅၇၉၊ ၀၉၅၁-၄၀၅၅၀

INTERNET Security

မာတိကာ

INTERNET Security

Part (I)

Internet Security - How And Why To Be Safe

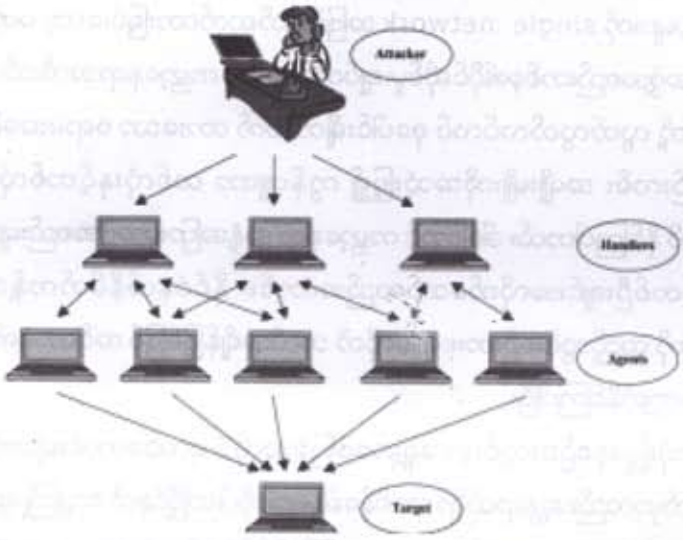
ကမ္ဘာလူဦးရေ၏ ၁၉ရာခိုင်နှုန်းကျော် တနည်းဆိုရရင် လူသန်းပေါင်းတစ်ထောင် ကျော်တို့ဟာ တွန်ပျူတာသန်းပေါင်းများစွာဖြင့် အင်တာနက်အား ချိတ်ဆက်အသုံးပြုလျက်ရှိနေခဲ့ပါတယ်။ အဲဒီသန်းပေါင်း ထောင်ချီသောကွန်ပျူတာများကို single network အဖြစ်ချိတ်ဆက်ထားခြင်းတော့ မဟုတ်ပါဘူး။ တစ်ဦးတစ်ယောက် (သို့) အဖွဲ့အစည်းတစ်ခု၏ပိုင်ဆိုင်မှု၊ ချုပ်ကိုင်မှုမရှိဘဲ ကမ္ဘာ့နေရာအသီးသီးမှာရှိသော network ပေါင်းများစွာတို့ လွတ်လွတ်လပ်လပ် စုပေါင်းချိတ်ဆက် ထားသော ဧရာမအခင်းအကျင်း အစီအမံတစ်ခုဖြစ်ပြီးနည်းလမ်း အမျိုးမျိုးကိုအသုံးပြု၍ ကွန်ပျူတာ တစ်လုံးနှင့်တစ်လုံး သတင်း အချက်အလက်များ ဖလှယ် နိုင်ကြပါတယ်။ ဒါကြောင့် ကမ္ဘာ့နေရာ အနှံ့အပြားမှအဖွဲ့အစည်းများ အလိုက်သော်လည်းကောင်း၊ လူတစ်ဦးချင်းအလိုက်သော်လည်းကောင်း၊ နိုင်ငံနယ်နိမိတ်ကန့်သတ်ချက်၊ အချိန်ကန့်သတ်ချက်များကို ထည့်သွင်းစဉ်းစားစရာမလိုဘဲ ဘယ်အချိန်ဖြစ်ဖြစ် အင်တာနက်ပေါ်ကနေ တစ်နေရာရာမှာရောက်ရှိတွေ့ဆုံနိုင်ကြပါပြီ။

အင်တာနက်အသုံးပြုနေစဉ်အတွင်းမှာ ရေမှာဖေါ်ပြခဲ့သလိုပဲ ရလဒ်ကောင်းများကို ရရှိခံစားနိုင်ကြသလို အခြားတစ်ဖက်မှာလည်းအန္တရာယ်ရှိသော စိန်ခေါ်မှုများကိုပါတပြိုင်နက် တွေ့ကြုံရပါလိမ့်မယ်။ ဘေးအန္တရာယ်ဆိုတာကတော့ hackerများ၊ intruder များကြောင့် မိမိရဲ့လျှို့ဝှက်အပ်သော information များခိုးယူခံရခြင်း၊ ပေါက်ကြားရခြင်း virus များကြောင့် data file များ၊ system များ ဖျက်စီးခံရခြင်း များပင်ဖြစ်ပါတယ်။ မိမိမှာထိပ်တန်းလျှို့ဝှက်အပ်သော information များ၊ အဖိုးတန်သော data များ မရှိသော်လည်းနောက်ထပ်ကြုံတွေ့နိုင်သောစိန်ခေါ်မှုတစ်ခုကတော့ မိမိရဲ့ကွန်ပျူတာမှာရှိသော hard-disk space ၊အင်တာနက် connection၊ operating system အစရှိသည့် Resourceများကို အသုံးပြုပြီး အင်တာနက်ပေါ်ရှိ အခြားကွန်ပျူတာများကို attack လုပ်ခြင်းများလည်းကြုံရနိုင်ပါသေးတယ်။

ဒါကြောင့် ယနေ့မှာတော့ မိမိကိုယ်တိုင်ကော အခြားသူများပါ ဘေးအန္တရာယ်ကင်းရေးအတွက်ပါ security ပိုင်းဟာပိုမိုအရေးပါလာပါတယ်။ အဲဒီလိုခြိမ်းခြောက်မှုများမှကာကွယ်ရန် Antivirus program လိုအပ်သလို Firewall program များကိုလည်းအသုံးပြုပြီး security ပိုင်းကိုတိုးမြင့်ကာကွယ်ဖို့ လိုလာပါတယ်။ Internet security အတွက် Antivirus program များ firewall များ ဘာကြောင့် လိုအပ်သလဲ၊ ဘာကြောင့်အသုံးပြုသင့်သလဲ ဆိုတာကို သဘောပေါက် နားလည်ဖို့ရန် attacker (သို့) intruder တွေဟာ မိမိရဲ့ကွန်ပျူတာကို ဘယ်လိုဝင်ရောက်ထိန်းချုပ်ကြသလဲဆိုတာကို သိထားဖို့လိုပါတယ်။

Attacker အများစုဟာ ကွန်ပျူတာတစ်လုံးတည်းကို သာ ဦးတည်ရည်ရွယ်ပြီး ထိန်းချုပ်နိုင်အောင်ကြိုးပမ်းလေ့မရှိပါဘူး။ ကွန်ပျူတာအရေအတွက်များနိုင်သလောက်များများကိုထိန်းချုပ်နိုင်ဖို့ရန် ရည်ရွယ်ပြီး ကူးစက်ပုံနှံ့စေနိုင်သော Trojan horse လို့ခေါ်တဲ့ virusတစ်မျိုးကို (ဥပမာ - lovegate) ကို

အင်တာနက်ပေါ်သို့လွှတ်တင်ထားလိုက်ပါတယ်။ Trojan ဟာ ကွန်ပျူတာတစ်လုံးမှာ ဝင်ရောက်ကူးစက်နေနိုင်ပြီဆိုလျှင် ထိုကွန်ပျူတာနှင့်ပတ်သက်သော basic information များဖြစ်တဲ့ ip address၊ hardware spec နှင့် OS တို့ကို trojan ရေးသားသူများထံလှှဲပြောင်းပေးပို့ပါတယ်။



Virus (သို့) trojan ရေးသားသူများဟာ လက်ခံရရှိသော information များကိုအသုံးပြုပြီး ကွန်ပျူတာဘယ်လောက်များများကို ထိန်းချုပ်ပိုင်ဆိုင်သွားပြီဆိုတာကို သိနိုင်သလို ထိုကွန်ပျူတာများမှတဆင့် အစိုးရအဖွဲ့စည်းများ၊ ပုဂ္ဂလိကအဖွဲ့များ၏ server များကိုဦးတည်ပြီး large scale attack များကိုစတင်ပါတော့တယ်။ ကွန်ပျူတာအရေအတွက်များများကိုထိန်းချုပ်လာနိုင်တာနဲ့အမျှ attacker များ၏ true location ကို သိဖို့ရန် ပိုမိုခက်ခဲလာပါတယ်။

ဒီနေရာမှာ hacker များ၊ intruder များသည် large scale attack ကို ဘယ်လို လုပ်ဆောင်ကြသလဲ ဆိုတာကိုအနည်းငယ်ရှင်းပြလိုပါတယ်။ Attacking အကြောင်းမပြောခင်မှာဦးစွာပထမ ICMP Ping အကြောင်းကိုသိထားဖို့လိုပါတယ်။ ICMP Ping ဆိုတာ မိမိ access လုပ်လိုသော server (ပါ) ကွန်ပျူတာ နှင့်ချိတ်ဆက်ရန်ိုင်မရနိုင်ဆိုတာကို စစ်ဆေးရာတွင် အသုံးပြုနိုင်သော command တစ်ခုပဲဖြစ်ပါတယ်။ ဆိုရရင်မိမိကွန်ပျူတာမှ server ကွန်ပျူတာတစ်လုံးလုံးသို့ Ping လိုက်တဲ့အခါမှာမိမိကွန်ပျူတာမှ request signal များသည် server ကွန်ပျူတာသို့ရောက်ရှိသွားပါတယ်။ server ကွန်ပျူတာသည် လက်ခံရရှိလာသော request signal ထဲတွင်ပါလာသော source code လို့ခေါ်တဲ့လိပ်စာကိုဖတ်ပြီးမှသာ မိမိအား ဘယ်ကွန်ပျူတာမှ request လုပ်သလဲဆိုတာကိုသိနိုင်ပြီးထိုကွန်ပျူတာများဆီသို့မိမိရှိနေကြောင်းကို reply ပြန်ပို့ပေးနိုင်ပါတယ်။

Attacker များသည် server များကို attack လုပ်တဲ့အခါမျိုးမှာ ICMP command များကို အသုံးပြု၍ တိုက်ခိုက်လေ့ရှိပါတယ်။ attack လုပ်ဖို့ရန်အတွက် ရေမွှာဖေါ်ပြခဲ့သလိုပဲ ကွန်ပျူတာအရေအတွက် များနိုင်သမျှများများကို ထိန်းချုပ်နိုင်အောင် ပထမဦးစွာ လုပ်ဆောင်ပါတယ်။ ထိန်းချုပ်လို့ရလာတဲ့ ကွန်ပျူတာများပေါ်မှာ program တစ်ခုကို အရင် install လုပ်လိုက်ပြီးထို program ကိုအသုံးပြု၍ attack လုပ်လိုသော server ဆီသို့ ICMP ဖြင့် request signal များပို့လွှတ်ပါတယ်။ Attacker များပို့လွှတ်လိုက်သော request signal များထဲတွင် source code များမပါရှိပါဘူး။ ဒါ့ကြောင့် server များသည် request signal များကိုလက်ခံရရှိသော်လည်း မည်သည့်နေရာ(ဂါ)ကွန်ပျူတာဆီသို့ reply ပြန်ရမလဲဆိုတာကို မသိနိုင်ဘဲဝေခွဲမရဖြစ်နေတတ်ပါတယ်။ အဲဒီလို source code မပါသော request signal များအတိုင်းအတာ တစ်ခုအထိများလာတဲ့အခါမှာ server ကွန်ပျူတာသည် သူ၏လုပ်ငန်းများကို ပုံမှန်အတိုင်း ဆက်လက်မလုပ်ဆောင်နိုင်တော့ဘဲရပ်တန့်သွားပါတော့တယ်။

အဲဒီလို large scale attack မျိုးကြုံလာတဲ့အခါမျိုးမှာ မိမိကွန်ပျူတာကို hacker များမှ hijack လုပ်ပြီး attack လုပ်သွားခဲ့ခြင်း ဖြစ်တဲ့အတွက်ကြောင့် မိမိမှာလည်းတာဝန်မကင်းဘူးပေါ့။ ဆိုရရင် ကားပိုင်ရှင်များသည်မောင်းသူမည်သူမည်ဝါဖြစ်စေကာမူအကြောင်းတစ်စုံတစ်ခုကြောင့်ပြဿနာကြုံလာတဲ့ အခါမှာ ကားပိုင်ရှင်မှပထမဦးစွာ ဖြေရှင်းရန် တာဝန်ရှိလာသလိုမျိုးပဲ ဖြစ်ပါတယ်။

တကယ်လို့သာ မိမိရဲ့ကွန်ပျူတာမှာ security ပိုင်းကိုပါလုံခြုံအောင်တိုးမြင့်ကာကွယ်ထားမယ် ဆိုရင် ယခုလိုပြဿနာမျိုးကြုံတွေ့လာနိုင်စရာမရှိတော့ပါဘူး။ ပထမဦးစွာ Antivirus program တစ်ခုကို အမြဲတမ်း update လုပ်ပြီးအသုံးပြုမယ်ဆိုရင် virus များ၊ worm များ၊ trojan များဝင်ရောက်ကူးစက်ခြင်းမှ ကာကွယ်နိုင်ပါတယ်။ အကယ်၍ အကြောင်းတစ်ခုခုကြောင့် ကူးစက်ခံရရင်လည်း firewall သာတပ်ဆင်ထားပါက trojan များအားပို့လွှတ်သော မူလပိုင်ရှင် ထံသို့ မိမိကွန်ပျူတာမှ information များလျှို့ဝှက်စွာ ပြန်ပို့ခြင်းမှ တားဆီးနိုင်ပါတယ်။

သင့် Computer ၏ Security အပေါ်မြှင့်မားခြောက်မှုအများစုကို ကာကွယ်နိုင်ရန် ကြိုတင် သိထားအပ်သော ဆောင်ရန်ရှောင်ရန်အချက်များစွာရှိပါတယ်။

1) အသုံးပြုနေသော Windows Operating system နှင့် Office Software တို့ကို update ဖြစ်စေရန် မှန်မှန် check လုပ်၍လိုအပ်ပါက Microsoft website မှတဆင့် service packs များ security patch များကို download ရယူပါ။

2) Personal firewall တစ်ခုကို install လုပ်၍ကာကွယ်မှုပြုပါ။

3) Anti-spyware တစ်ခုခုကို install လုပ်ထားပါ။

4) သင့်ကွန်ပျူတာတွင် password များအသုံးပြုရာတွင် ခိုင်မာစိတ်ချရသော password ဖြစ်စေရန် letter များ၊ number များပါဝင်သော character စာလုံးအရေအတွက် ရလုံးထက်မနည်းသော password များကိုအသုံးပြုပါ။ password ကိုမကြာခဏ ပြောင်းလဲသုံးစွဲခြင်းများပြုလုပ်ပါ။

5) Email application (Outlook၊ Outlook Express) တို့အတွက် Security update များကိုလည်း မှန်မှန်စစ်ဆေး၍ download ရယူ install လုပ်ပါ။

6) Antivirus software တစ်ခုကို install လုပ်ထားပြီး virus definition ကိုအမြဲ update ဖြစ်နေစေရန်ဂရုပြုလုပ်ဆောင်ပါ။

7) သင်ကွန်ပျူတာ၏ Security ပိုင်းကိုထိခိုက်စေနိုင်သည့် မကြာခဏ ထွက်ပေါ်နေသော ခြိမ်းခြောက်မှု threats များကို မျက်ခြေမပြတ်အမြဲသိရှိနေနိုင်ရန် သင်အသုံးပြုနေသော Operating system ထုတ်လုပ်သည့် website (ဥပမာ Microsoft)၊ Antivirus Company များ၏ website (ဥပမာ Symantec ၊ McAfee ၊ Kaspersky ၊ Antivir) သို့မကြာခဏဝင်ရောက်ကြည့်ရှုစစ်ဆေးရှာဖွေပါ။

8) မိမိထံရောက်လာသော Email များကိုအလွယ်တကူမယုံကြည်ပါနှင့် **From**: field တွင်တွေ့ရသော အမည်သည်မိမိသိရှိသောသူ၏အမည်ဖြစ်စေကာမူ ထိုသူအမှန်တကယ်ပို့လွှတ်သည်ဟုယုံကြည်ရမည့် နောက်ထပ်အကြောင်တစ်စုံတစ်ရာမရှိဘဲထိုသူထံမှပို့လွှတ်သည်ဟုမယူဆပါနှင့်။ email နှင့်ပါလာသော attachment file များကိုအလွယ်တကူအလျင်လိုစွာ မဖွင့်ပါနှင့်။ attachment file သည်မည်သည့် အရာဖြစ်သည်ဟု ဖေါ်ပြထားစေကာမူ attachment တွင်ပါသော အရာသည် ၄င်းဖေါ်ပြထားသည် အတိုင်းဖြစ်မည်ဟုယုံကြည်မယူဆပါနှင့်။

Internet အသုံးပြုသူ user များအနေနှင့် ဖေါ်ပြပါဆောင်ရန်ရှောင်ရန်များကို အလေးဂရုပြု လိုက်နာမည်ဆိုပါကမိမိကွန်ပျူတာအတွက် security ပိုင်းဆိုင်ရာလုံခြုံမှုကိုအတိုင်းအတာ တစ်ခုအထိ ရရှိပြီးဖြစ်ပါလိမ့်မယ်။

UPDATES - Security Patch (or) Windows Critical Update

အင်တာနက်ကမ္ဘာဟာနေ့စဉ်နှင့်အမျှ ပြောင်းလဲနေပါတယ်။ ထိုအပြောင်းအလဲများသည် လည်းလူအများကို နှစ်သက်စွဲလန်းဖွယ်ဖြစ်အောင် ညှို့ယူဖမ်းစားနိုင်သော အကြောင်းတရားတစ်ခု လည်းဖြစ်ကောင်းဖြစ်နိုင်ပါတယ်။ အပြောင်းအလဲတို့၏ သဘာဝအတိုင်းအကောင်းဘက်သို့ဦးတည်သော တိုးတက်ပြောင်းလဲမှုများရှိသလို အဆိုးဘက်သို့ဦးတည်သော hacker များ၏ လူပ်ရှားမှုများသည်လည်း နေ့စဉ်နဲ့အမျှပိုမို များပြားလာလျက်ရှိပါတယ်။ အဲဒီလိုအကြောင်းတရားများကြောင့်လည်း အင်တာနက် အသုံးပြုသူများ၏ Security နှင့် Privacy ကိုကာကွယ်ပေးရန် Computer Operating System(OS) နှင့် Browser program များကိုထုတ်လုပ်ရောင်း ချသူများဘက်မှလည်း ထို System နှစ်ခုကိုပိုမို တိုးတက်ကောင်းမွန်လာအောင် အမြဲတမ်းပြုပြင် မွမ်းမံပေးရလေ့ရှိပါတယ်။

အဲဒီ System ၂ခုတို့ဟာ complex code ထောင်ပေါင်းများစွာဖြင့် ဖွဲ့စည်းတည်ဆောက် ထားပါတယ်။ ဒီနေရာမှာတစ်ခုသတိထားရမှာကတော့ hacker အားလုံးတို့ဟာ လူဆိုးများမဟုတ်ကြပါဘူး။ အချို့သောသူများသည် မိမိတို့ရဲ့ဝါသနာအရ complex code များ၊ အင်တာနက် website များရှိ လုံခြုံရေးအားနည်းနေသော "Security hole" များကိုဝင်ရောက်ရှာဖွေလေ့ရှိပါတယ်။ ဟာကွက်ပျော့ကွက် များကို တွေ့ရှိပါကထို software ရေးသားသူ(သို့) website ဖန်တီးသူများ သိရှိအောင်ပုံစံအမျိုးမျိုးဖြင့် အသိပေးလေ့ရှိပါတယ်။

Security ပိုင်းအရအားနည်းချက်ဟာကွက်များကိုတွေ့ရှိလာတဲ့အခါတိုင်းမှာ ဖန်တီးသူများဘက်မှ ထိုဟာကွက်အားနည်းချက်များကို ပြုပြင်ဖာထေးထားသော Security update များကို အလွယ်တကူ download ရယူ installလုပ်နိုင်ရန် မိမိတို့ရဲ့website များမှာတင်ထားပေးလေ့ရှိပါတယ်။ ဥပမာဆိုရရင် Windows Critical Updates များပဲဖြစ်ပါတယ်။ Critical update များဟာ Windows အသုံးပြုသူ user များ၏ security နှင့် privacy ကို ထိပါးနှောင့်ယှက်ခြင်းများမှ ကာကွယ်ပေးနိုင်ရန် window ၏အားနည်းချက်ဟာကွက်များကို ပြုပြင်ပေးထားသော service pack နှင့် windows new feature များပဲဖြစ်ပါတယ်။ ထို updateများကို patch များဟုလည်းခေါ်ဝေါ်ကြပါတယ်။

Windows "Security Patch" များဟာ သက်ဆိုင်ရာ product များအလိုက် အကြောင်း တစ်ခုခုကြောင့် လိုအပ်တဲ့အချိန်မှာထွက်ပေါ်လာတတ်ပြီး ပုံမှန်ဘယ်နေ့ဘယ်အချိန်မှာ ထွက်ပါမယ်လို့ ပုံသေမရှိပါဘူး။ ဒါကြောင့် မိမိကွန်ပျူတာရဲ့ Windows OS ကို အစဉ်အမြဲ ကြဲခိုင်မှုပြည့်ဝနေအောင် စီမံထားချင်တယ်ဆိုရင်တော့ Microsoft website ထဲကိုမကြာခဏဝင်ရောက်ပြီး မိမိနှင့်သက်ဆိုင်သော patch အသစ်တစ်ခုပေါ်တိုင်းအမြန်ဆုံး download & install လုပ်ထားဖို့လိုပါတယ်။

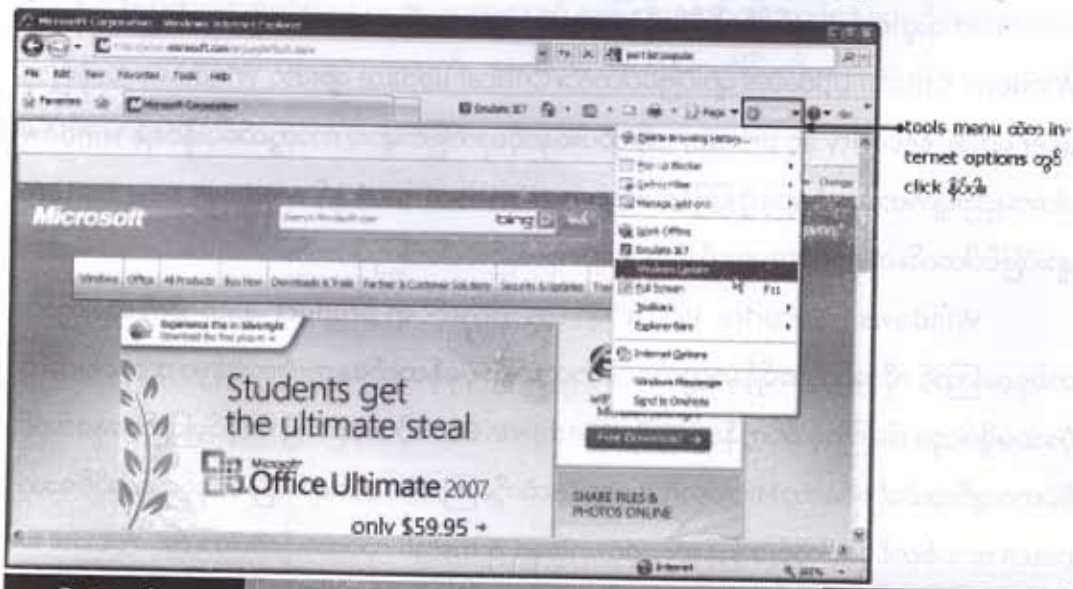
Security patch များကိုနည်း၂နည်းနှင့်download & install လုပ်နိုင်ကြပါတယ်။ပထမနည်းကတော့ Window updateမှတဆင့် Microsoftရဲ့ window updateသို့ဝင်ရောက်ပြီးမိမိကွန်ပျူတာအတွက်လိုအပ်သော Security patchများကို အလိုအလျောက် စစ်ဆေးရှာဖွေပြီး install လုပ်ခြင်းပဲဖြစ်ပါတယ်။ဒုတိယနည်းကတော့အကြောင်းတစ်ခုခုကြောင့် Automatic Updateလုပ်၍မရနိုင်တဲ့အခါမျိုးမှာ microsoft websiteထဲဝင်ရောက်ပြီး သက်ဆိုင်ရာ Security patch (သို့) Critical updateများကိုကိုယ်တိုင်ဖတ်ရှုရွေးချယ် download ရယူ install လုပ်ခြင်းများပဲဖြစ်ပါတယ်။

WINDOWS UPDATE

မိမိရဲ့ကွန်ပျူတာမှာ ဘယ်လို security patch များကို install လုပ်ဖို့ရန် လိုနေသလဲ ဆိုတာကို "Windows Update"တွင်အလွယ်တကူသွားရောက်စမ်းသပ် စစ်ဆေးနိုင်ကြပါတယ်။စစ်ဆေးပြီးသွားတဲ့အခါမှာမိမိအတွက်လိုအပ်သော patch များကိုညွှန်ပြပေးပါလိမ့်မယ်။ဒီနေရာမှာ အထူးသတိထား ရမှာကတော့ windows update မလုပ်ခင်မှာ လက်ရှိအသုံးပြု နေသောprogramများကို ပိတ်ထားရန် နှင့် updateလုပ်နေစဉ်အတွင်းမှာလည်းမိမိရဲ့အခြားလုပ်ငန်းစဉ်များကို ရပ်ဆိုင်းထားဖို့ရန်လိုအပ်ပါတယ်။

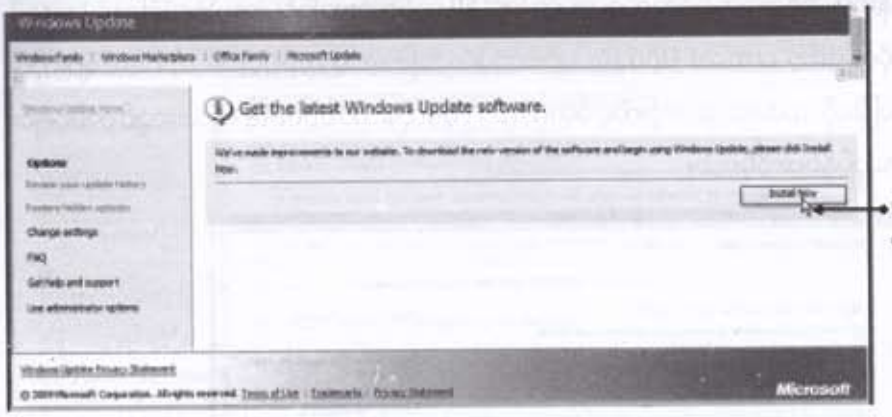
Step 1)Windows Update

Windows update သို့သွားရန်အတွက် Start menu ပေါ်ရှိ **windows update** တွင် click တစ်ချက်နှိပ်ပါ (သို့မဟုတ်) IE window ရှိ **Tools>windows update** တွင် click တစ်ချက်နှိပ်ပါ။ Microsoft ၏windows update page သို့ရောက်ရှိသွားပါမည်။

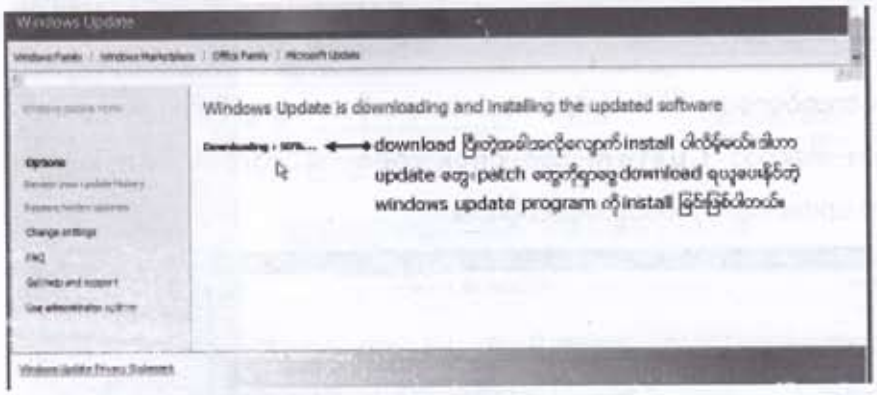


Step 2) Install Update Program

ယခုအချိန်သည် ပထမဦးဆုံး update လုပ်ခြင်းဖြစ်ပါက နောက်ဆုံးထုတ် Windows Update Program ကို install လုပ်ထားခြင်းရှိမရှိစစ်ဆေးပြီး၊ မရှိသေးပါက install လုပ်ခိုင်း ပါလိမ့်မည်။ အောက်ဖေါ်ပြပါပုံတွေက windows xp ကွန်ပျူတာတွေမှာ တွေ့ရမည့်ပုံများပဲဖြစ်ပါတယ်။ Windows Vista ကွန်ပျူတာတွေမှာဆိုရင် update window သီးခြားပွင့်လာပြီး install လုပ်ခိုင်းပါလိမ့်မယ်။ သဘောတရားကတော့ အတူတူပင်ဖြစ်ပါတယ်။



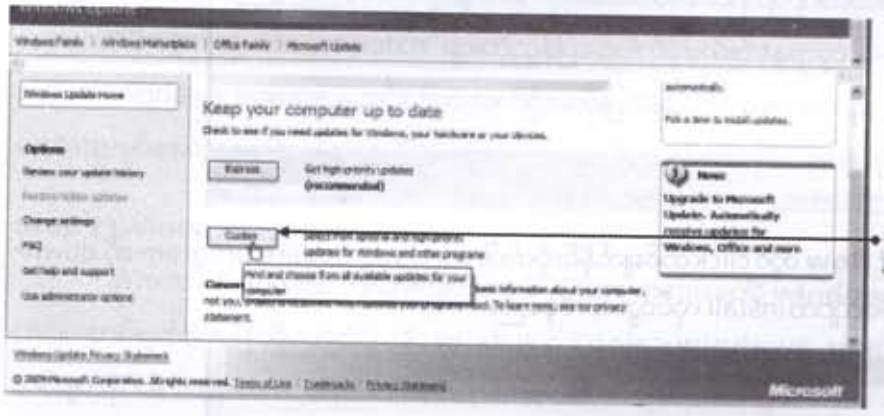
Install Now တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ windows update program ကို download ရယူပြီးအလိုလျောက် install လုပ်သွားပါလိမ့်မည်။



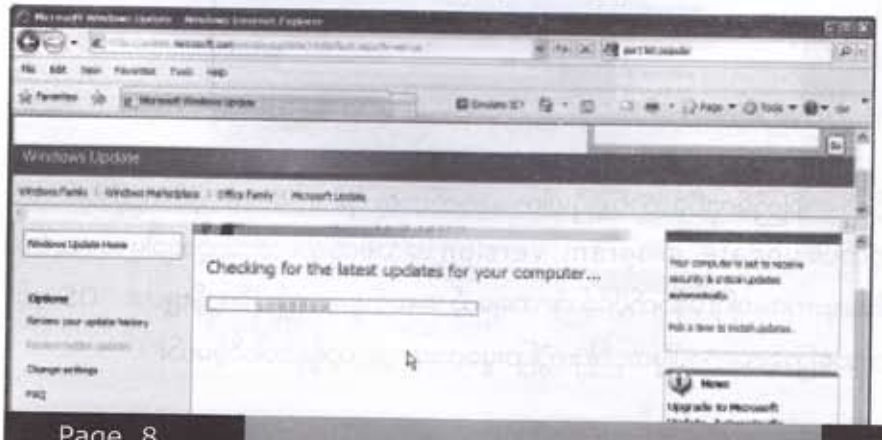
ဤအဆင့်ကို တစ်ကြိမ်လုပ်ဆောင်ခဲ့ပြီးပါက နောက်တစ်ကြိမ် update လုပ်သည့်အခါတွင် တွေ့ရလိမ့်မည်မဟုတ်ပါ။ update program version အသစ်ထွက်လာသည့်အခါမှသာ ထပ်မံတွေ့ရနိုင်ပါတယ်။ဒီနေရာကနေစပြီး နောက်ပိုင်းကြုံလာရမယ့် အဆင့်များသည် မိမိကွန်ပျူတာ OS နှင့် Microsoft ဘက်ကအပြောင်းအလဲပေါ်မူတည်ပြီး ကွဲပြားမှုလေးတွေတော့ရှိနိုင်ပါလိမ့်မယ်။

Step 3) Type of Installation

Windows Update Program ကို install လုပ်ပြီးသွားတဲ့အခါ မိမိရဲ့ကွန်ပျူတာမှာ ဘယ် update တွေလိုနေသလဲဆိုတာကို စစ်ဆေးဖို့ရန် အဆင်သင့်ဖြစ်သွားပြီး အဲဒီလိုစစ်ဆေးဖို့ရန်အတွက် express နှင့် custom install ဟူ၍ ရွေးချယ်စရာ option ၂ခုထဲမှ တစ်ခုကို ရွေးချယ်ပေးရပါမယ်။ Express install ကိုရွေးချယ်မည်ဆိုပါက မိမိကွန်ပျူတာအတွက် မရှိမဖြစ် install လုပ်ထားရမည့်အရေးကြီးသော critical update နှင့် service pack များကိုသာ ရွေးချယ်ဖေါ်ပြပြီး ထိုဖေါ်ပြသော update အားလုံးတို့ကို တန်းစီ၍ တစ်ခုပြီးတစ်ခုအလိုလျောက် install လုပ်သွားမှာဖြစ်ပါတယ်။custom install ကိုရွေးချယ်မည်ဆိုရင်တော့ critical update များသာမက အခြားသော optional update များကိုပါ တန်းစီဖေါ်ပြမှာဖြစ်ပြီး ထို update အားလုံးထဲမှ မိမိ install လုပ်လိုသော update ကိုသာလျှင် တစ်ခုချင်း ရွေးချယ် update လုပ်နိုင်ပါလိမ့်မယ်။

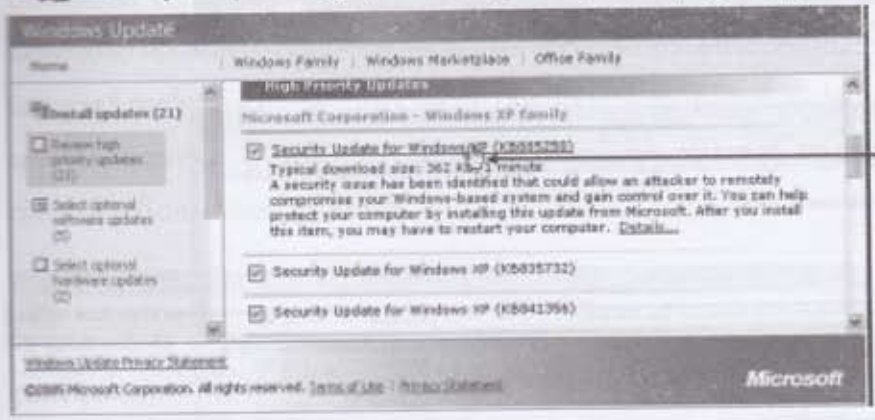


ဒီလမ်းညွှန်စာအုပ်မှာတော့ မိမိစိတ်ကြိုက် update များကိုသာ ရွေးချယ် install လုပ်ပုံကို ဖေါ်ပြမှာဖြစ်ပါတယ်။ ဒါကြောင့် **Custom** တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ မိမိကွန်ပျူတာအတွက်လိုအပ်သော update များကိုစတင်ရှာဖွေပါလိမ့်မည်။

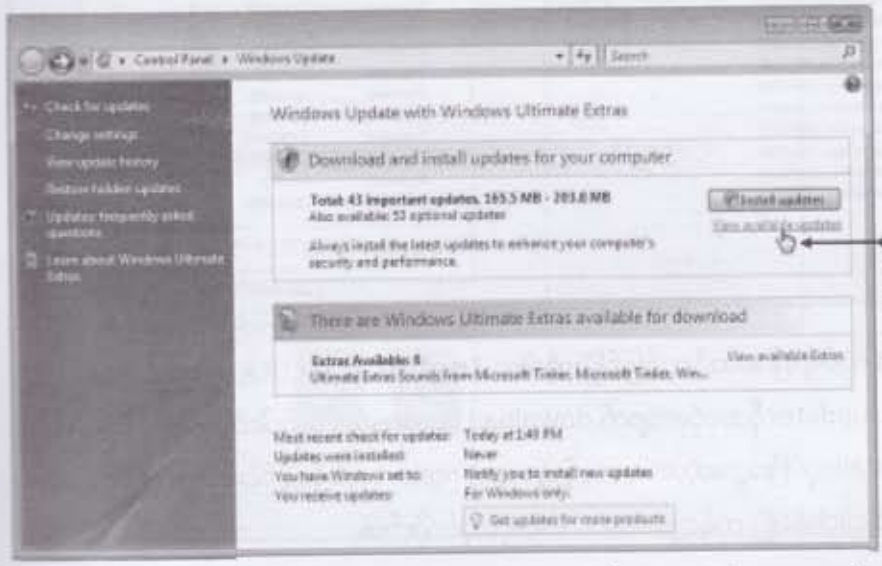


Step 4) Review and Install

စစ်ဆေးရှာဖွေပြီးသွားတဲ့အခါမှာမိမိကွန်ပျူတာအတွက် လိုအပ်သော update list ကိုထုတ်ပေးပါလိမ့်မည်။ windows updateကိုတစ်ကြိမ်တစ်ခါမျှမလုပ်ဖူးသေးပါက အနည်းဆုံးတစ်ဒါဇင်ခန့်ပါဝင်သော update များကိုတွေ့ရပါလိမ့်မည်။ ပုံမှန် default အားဖြင့် အားလုံးကို install လုပ်ရန် ရွေးချယ်ပြီးသားဖြစ်ပါလိမ့်မယ်။ ဘယ် updateတွေဟာ အရေးကြီးတဲ့ critical update တွေဖြစ်တယ်၊ ဘယ် update တွေကတော့ သိပ်အရေးမကြီးသော်လည်း တင်ထားသင့်တဲ့ optional update တွေဖြစ်တယ်ဆိုတာကို list ထဲရှိ update တစ်ခုစီပေါ်တွင် clickနှိပ်ပြီးဖတ်ရှုနိုင်ပါတယ်။



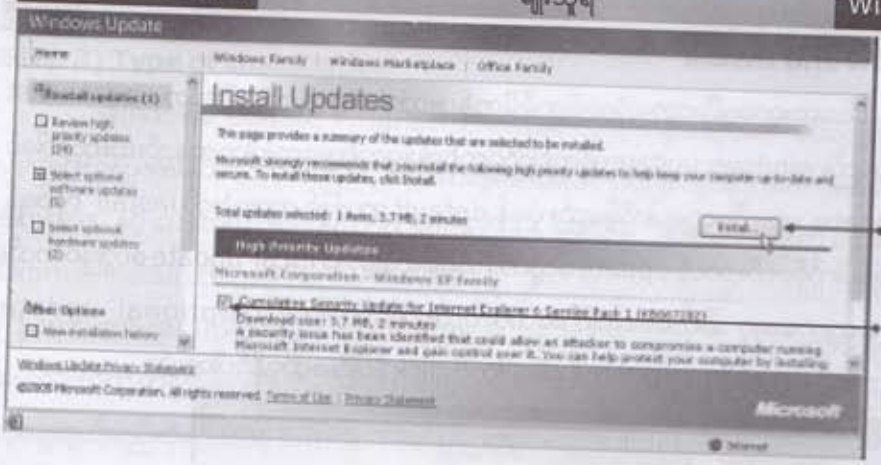
စိတ်ဝင်စားရာ update ပေါ်တွင် click နှိပ်ကြည့်နိုင်ပါတယ်။
(Windows XP)

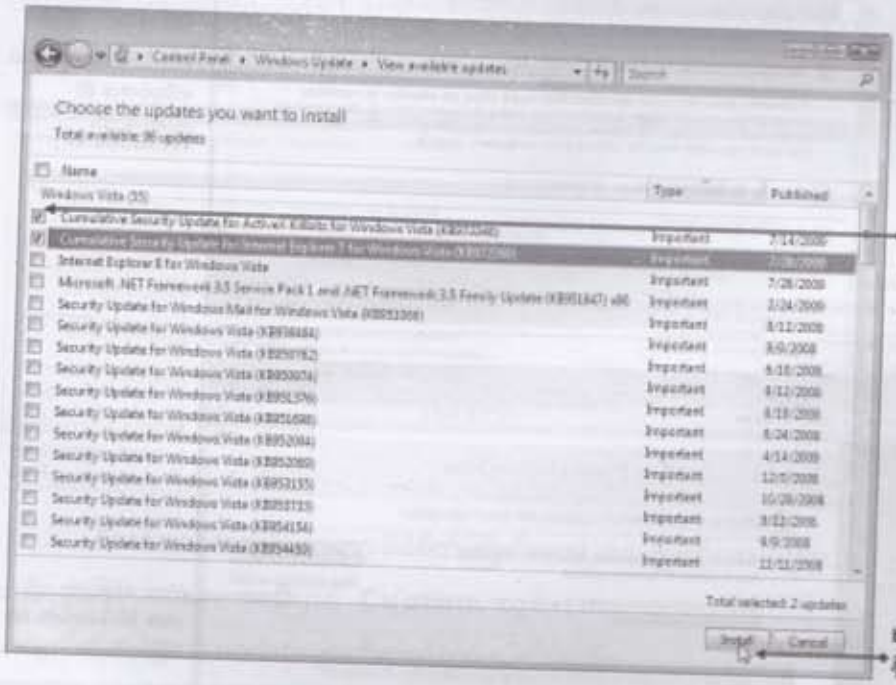


View Available တွင် click နှိပ်ပါ update list တို့ပြန်ရပါမယ်။

(Windows Vista)

အကယ်၍အရေးကြီးသော critical updateများကိုသာ ပထမဦးစွာ ရွေးချယ် installလုပ်လိုပါက အခြားသော update များဘေးရှိ select လုပ်ထားသော အမှန်ခြစ်များကို ဖြုတ်ပစ်ရပါမည်။ မိမိ install လုပ်ဖို့ရန်ရွေးချယ်ထားသော updateအရေအတွက်ကို webpageဇယားတွင် ဖေါ်ပြထားပါလိမ့်မည်။



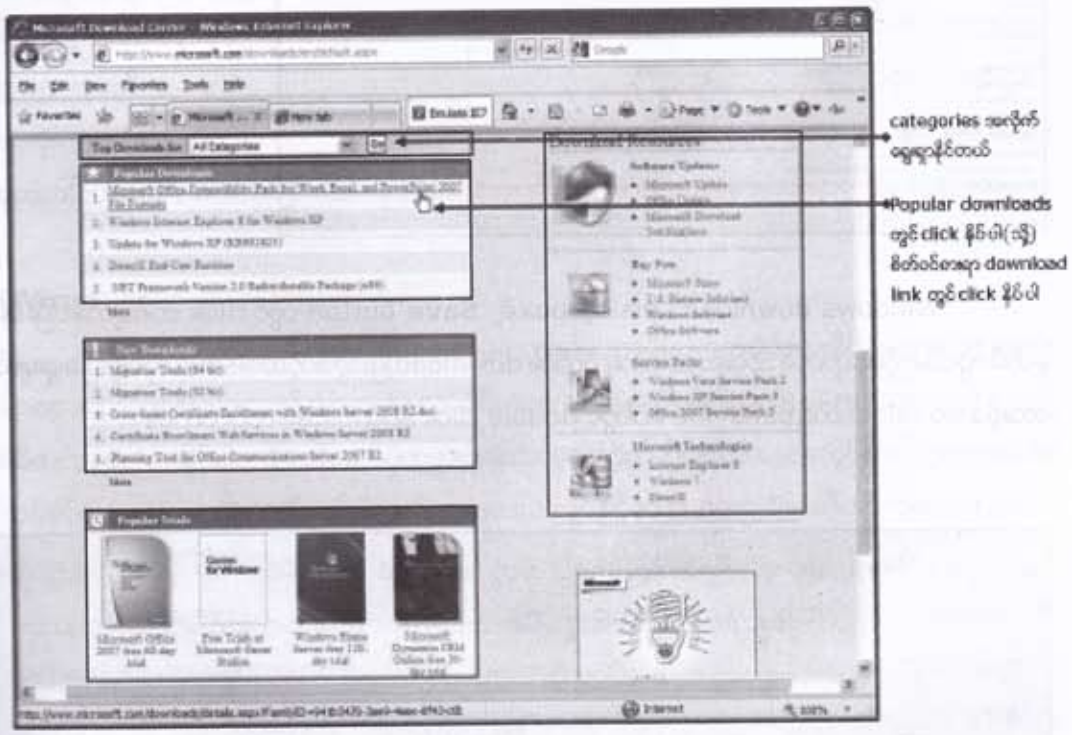


Install လုပ်ဖို့ရန်အဆင်သင့်ဖြစ်ပြီးဆိုပါက **Install** တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ မိမိရွေးချယ်ခဲ့သော update ကို အလိုလျောက် download ရယူ install လုပ်ပါလိမ့်မယ်။ အချို့သော update များအား install လုပ်ပြီးသွားတဲ့အခါမှာ ကွန်ပျူတာကို restart လုပ်ဖို့ရန် ခိုင်းစေတတ်ပါတယ်။ **Restart Now** တွင် click နှိပ်ပြီး ကွန်ပျူတာအား restart လုပ်လိုက်ပါ။

Microsoft Download Center

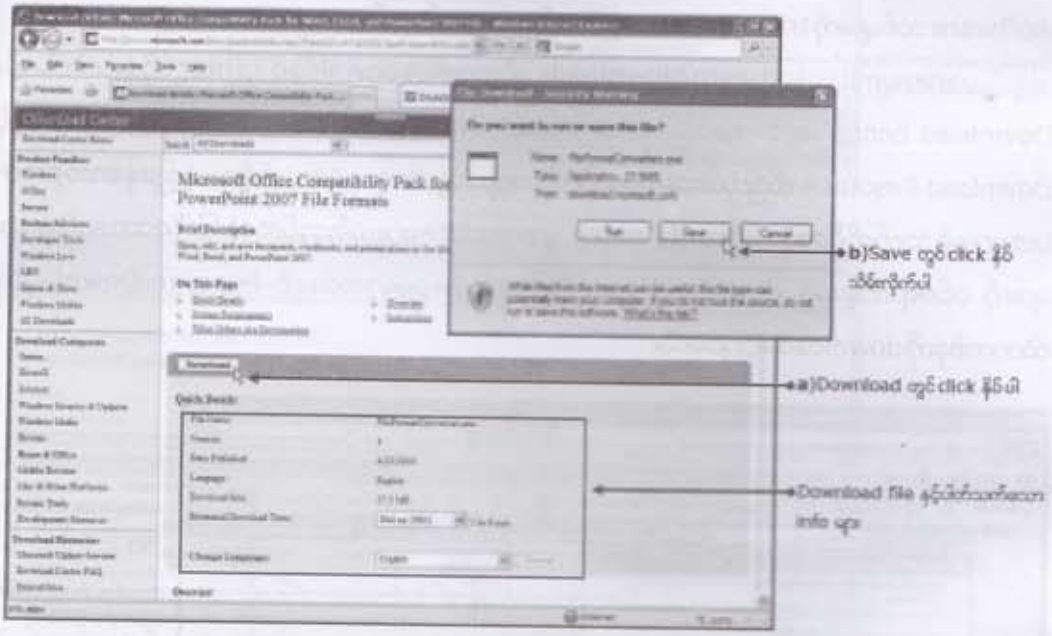
Security patch (သို့) Critical update များကို windows ရဲ့ဌာနေ site ဖြစ်သော www.microsoft.comမှာရှာဖွေ downloadရယူနိုင်ကြပါတယ်။ အဓိကအားဖြင့် microsoft မှ download center အောက်မှာ ထုတ်ဝေဖြန့်ချိထားသော productများရဲ့updateများ၊ service packများ၊ software သစ်များကိုtrial version အဖြစ်တင်ထားပေးပါတယ်။

www.microsoft.com/downloads သို့သွားပါက download center သို့ရောက်ပါမယ်။ Download center တွင် Popular Downloads ၊ New Downloads ၊ Popular Trials yနှင့် Download Resource ဆိုပြီးခွဲထားပေးတယ်။ ထိုကဏ္ဍတွေထဲကနေမိမိလက်ရှိအသုံးပြုနေသော productများနှင့် သက်ဆိုင်သော Security patch များ၊ updateများ၊ စမ်းသပ်အသုံးပြုလိုသော softwareများကို ဝင်ရောက်ရှာဖွေ download ရယူနိုင်ကြပါတယ်။ ဥပမာအနေနှင့် Popular Downloads ထဲကတစ်ခုကို download ဆွဲပြပါမယ်။



Popular downloads ပေါ်တွင် click တစ်ချက်နှိပ်ပါ။ အင်တာနက်အသုံးပြုသူများ ဆွဲယူအသုံးပြုတဲ့အကြိမ်အရေအတွက်ပေါ်မူတည်ပြီး update များ၊ software များကို တန်းစီဖော်ပြထားသော page သို့ရောက်ပါလိမ့်မယ်။

စိတ်ဝင်စားရာတစ်ခုပေါ်တွင် click တစ်ချက်နှိပ်ပါ။ information များပါသော pageကိုမြင်ရပါမယ်။ ၄င်းpage ထဲတွင် download file အမည်၊ အရွယ်အစား၊ ဘယ်အတွက်အသုံးပြုနိုင်တယ် အစရှိသဖြင့် အသေးစိတ်ဖေါ်ပြထားပါတယ်။ မိမိအတွက်လိုအပ်၍ရယူလိုပါက **Download** တွင် click နှိပ်ကာ ပေါ်လာသော ညွှန်ကြားချက်များအတိုင်းလိုက်ပါလုပ်ဆောင်ရယူနိုင်ပါတယ်။



"Windows download" dialog boxရဲ့ **Save** button တွင် click တစ်ချက်နှိပ်ပြီး မိမိ မှတ်မိ လွယ်မည့်နေရာတွင် သိမ်းဆည်းထားလိုက်ပါ။ download ပြီးသွားတဲ့အခါ save လုပ်ဖို့ရန်ရွေးချယ် ထားခဲ့သော folderထဲရှိpatch file ပေါ်တွင် double click နှိပ်၍ install လုပ်လိုက်ပါ။

မှတ်ချက် - Microsoft ရဲ့အချို့သော product တွေ၊ update တွေ၊ security patch တွေကို လွယ်လွယ် download မပေးပါဘူး။ Genuine Test စစ်ဆေးအောင်မြင်ပြီးမှသာ အသုံး ပြုခွင့်ပေးခြင်းမျိုးတွေလည်းရှိပါတယ်။ Genuine Testဆိုတာကွန်ပျူတာရှိwindow OS သည် တရားမဝင် copy ကူးယူ အသုံးပြုထား ခြင်းလား၊ တကယ့်အစစ်အမှန် ဝယ်ယူအသုံး ပြုထားခြင်းလားဆိုတာကို စစ်ဆေးခြင်းဖြစ်ပါတယ်။ အကယ်၍ တရားမဝင် copy ကူးယူ အသုံးပြုထားပါက ရှေ့ဆက် download လုပ်ခွင့်ရမည်မဟုတ်ပါ။

Using Anti-Virus Software

ယနေ့ခေတ်ကွန်ပျူတာအသုံးပြုသူများအတွက် မလွဲမသွေကြုံတွေ့နိုင်သည့်ကြီးမားသည့်အန္တရာယ်တစ်ခုမှာ virus အန္တရာယ်ပင်ဖြစ်သည်။ virus ဆိုသည်မှာ program ငယ်လေးတစ်ခုပင်ဖြစ်ပြီး အသုံးပြုသူ user များကို စိတ်အနှောင့်အယှက်ဖြစ်ရုံလုပ်ဆောင်နိုင်သော virus များမှသည် program များ၊ data များနှင့် system ပိုင်းအထိကိုပါ ဖျက်ဆီးပစ်နိုင်သော အဖျက်စွမ်းအားကြီး သည့် virus များအထိ ရှိပါတယ်။

virus များကူးစက်ပြန့်နှံ့ပုံမှာ လူများတွင်ကူးစက်ပြန့်ပွားတတ်သော biological virus တို့ကူးစက်ပြန့်ပွားပုံနှင့်များစွာ ဆင်တူပါတယ်။ အကယ်၍မိမိကွန်ပျူတာတွင် virus ကူးစက်နေပြီဆိုပါက file တစ်ခုမှ တစ်ခုသို့ကူးစက်ခြင်း၊ virus စွဲကပ်နေသော file များကိုအခြားကွန်ပျူတာတစ်လုံးတွင် သွားရောက်အသုံးပြုခြင်းဖြင့် ကူးစက်ခြင်း၊ မိမိကွန်ပျူတာနှင့် ချိတ်ဆက်ထားသော network အတွင်းရှိအခြားကွန်ပျူတာများသို့ကူးစက်ပြန့်နှံ့ခြင်း စသည်ဖြင့် virus များပြန့်နှံ့ပုံမှာအမျိုးမျိုးရှိပါတယ်။

ယခုအခါအင်တာနက်အသုံးပြုမှုများပိုမိုကျယ်ပြန့်လာရာမှအင်တာနက်အသုံးပြုခြင်း၊ Email အသုံးပြုခြင်းများမှတဆင့် virus ကူးစက်မှုများလည်းပိုမိုများပြားလာနေပြီဖြစ်ပါတယ်။ထိုမလိုလားအပ်သော program များကိုလူအများက virus ဟူ၍သိမ်းကြုံးခေါ်ဝေါ်သုံးစွဲနေကြသော်လည်း တစ်ခုနှင့်တစ်ခု အန္တရာယ်ပေးပုံ၊ကူးစက်ပြန့်နှံ့ပုံများသည်လည်းမတူညီကြပါ။ ဒါကြောင့်ကူးစက်ပြန့်နှံ့ပုံ (သို့) အလုပ်လုပ်ပုံများအပေါ်မူတည်ပြီး Virus ၊ Worm ၊ Trojan နှင့် Hoax အစရှိသဖြင့် virus အမျိုးအစားများ ကွဲပြားကြပါတယ်။

❑Virus

Virus ဆိုတာ self-replicating code ဟုခေါ်သော မိမိဖာသာပုံတူပွားနိုင်သော virus code များအားထည့်သွင်းထားသည့် execute လုပ်နိုင်သော file များပဲဖြစ်ပါတယ်။ Virus code များသည် မိမိဖာသာပုံတူပွားနိုင်ပါတယ်။ သို့သော်ပုံတူပွားဖို့ရန်အတွက် ကိုယ်တိုင် execute မလုပ်နိုင်ပါဘူး။ execute လုပ်နိုင်သော host file တစ်ခုလိုပါတယ်။ execute လုပ်နိုင်သော host file ဆိုတာကတော့ (.exe ၊ .com ၊ .bat) တို့ဖြင့် အဆုံးသတ်လေ့ရှိသော file များပဲဖြစ်ပါတယ်။

အဲဒီ host file များကို execute လုပ်သော အခါမှသာလျှင် virus code များလည်းစတင် execute လုပ်ပြီး virus များကူးစက်ပြန့်နှံ့ပါတော့တယ်။ဒါကြောင့် virus ပါလာတဲ့ file တစ်ခုမိမိကွန်ပျူတာထဲသို့စတင်ရောက်ရှိလာသော်လည်း ချက်ချင်းအန္တရာယ်မပေးနိုင်သေးပါဘူး။ ထိုဖိုင်ကို double click နှိပ်ပြီးဖွင့်ကြည့်မိတဲ့အခါမှသာလျှင် ထို virus မှစတင်အလုပ်လုပ်၍ အန္တရာယ်ပေးနိုင်ပါတယ်။

❑ Worm

Worm များသည်လည်း virus ကဲ့သို့ပင် ကိုယ်တိုင်ပုံတူပွားနိုင်သော program များပင်ဖြစ်ပါတယ်။ သို့သော် virus များကဲ့သို့ပင် execute လုပ်နိုင်သော host file များမလိုပါဘူး။ မိမိဖာသာ execute လုပ်ပြီးပြန့်နှံနိုင်ပါတယ်။ email များသည့်worm များအနှစ်သက်ဆုံးကူးသန်းသွားလာရေးလမ်းကြောင်းကြီးပင်ဖြစ်ပါတယ်။အများအားဖြင့် outlook express ကဲ့သို့ email client program များကိုဝင်ရောက်ထိန်းချုပ်ပြီး address book ထဲတွင်ရှိသော လိပ်စာများ ဆီသို့ attachment များတွင်ကွယ်ဝှက်လိုက်ပါ၍ messageများအလိုအလျောက်ပို့လွှတ်လေ့ရှိပါတယ်။ လက်ခံရရှိသော သူများမှာလည်း မိမိ၏အပေါင်းသင်းသူငယ်ချင်းများလည်းဖြစ်၊ စီးပွားဖက်များ ထံမှလာသော message များဖြစ်သောကြောင့် နှစ်ခါစဉ်းစားနေစရာမလိုပဲ ယုံယုံကြည်ကြည်ဖွင့်ပင် attachment များကိုဖွင့်ဖတ်ကြမှာဖြစ်ပါတယ်။ အချို့သော worm များသည် attachment များကိုပင်ဖွင့်ကြည့်စရာမလိုဘဲ preview pane တွင်ကြည့်ရုံမျှဖြင့်ပင်ကူးစက်ခံရနိုင်ပါတယ်။

❑Trojans

Trojan horse များသည် virus များကဲ့သို့ ပုံတူမပွားနိုင်တာကလွဲ၍ကျန်သော လက္ခဏာများမှာအတူတူပင်ဖြစ်ပါတယ်။ Trojan များဟာ vjrus များနှင့် အလားသဏ္ဌာန် တူသော်လည်း၊ တိတ်တခိုးဝင်ရောက်နိုင်အောင် ရည်ရွယ်ပြီး ရေးထားသောကြောင့် anti-virus program များဟာ တစ်ခါတစ်လေမှာ Trojan များကိုမမြင်နိုင်ဘဲဖြစ်တဲ့အတွက် pass လုပ်ပေးနိုင်ပါတယ်။ Trojan တွေဟာ အသုံးပြုသူ၏ personal security ကိုသာမက computer system ပိုင်းကိုပါ နည်းလမ်းအသွယ်သွယ်နှင့် အန္တရာယ်ပေးနိုင်ပါတယ်။ Trojan များဟာ နည်းလမ်းအမျိုးမျိုးဖြင့်မိမိရဲ့ကွန်ပျူတာထဲသို့ဝင်ရောက်လာ နိုင်ပါတယ်။ ဆိုရရင် email မှာပါလာတဲ့ attachment file ကိုဖွင့်လိုက်တဲ့အခါမျိုးမှာဖြစ်စေ Website တစ်ခုခုကိုသွားရောက်ကြည့်ရှုတာမှဖြစ်စေ ပါလာနိုင်ပါတယ်။ အဲဒီလိုပါလာတဲ့ Trojan များဟာ ကွန်ပျူတာ၏ registry နှင့် start up area ထဲမှာ သူဘာသာသူဝင်ရောပြီးနေရာဝင်ယူတတ်ပါတယ်။

Trojan တွေဟာ install လုပ်ပြီး နေရာဝင်ယူသွားပြီဆိုရင် သူတို့ကို remove လုပ်ဖို့ရန်အလွန်ခက်ပါတယ်။ အကောင်းဆုံး Anti-virus software တွေတောင်မှ အမြဲတမ်း detect မလုပ်နိုင်ပါဘူး။ တကယ်လို့ရှာတွေ့ခဲ့ရင်လည်း remove လုပ်ဖို့အလွန်ခက်ပါတယ်။ Registry ထဲတွင်နေရာဝင်ယူထားတတ်သောကြောင့် Trojan များကိုဖျက်ထုတ်ရင်းregistry data များကိုပါမှားဖျက်မိပါက ကွန်ပျူတာ၏ operation ပိုင်းကိုထိခိုက်နိုင်ပါတယ်။ အကယ်၍ Trojan ကို complete မဖျက်နိုင်ဘဲ တစ်စိတ်တစ်ပိုင်းသာဖျက်ခဲ့ပြန်ရင်လည်း သူရဲ့အန္တရာယ်က မကင်းနိုင်ပါဘူး။ ကွန်ပျူတာကို Restart လုပ်တာနှင့် သူဘာသာ reload ပြန်လုပ်ပြီးနေနိုင်ပါသေးတယ်။

Trojan အမျိုးမျိုးရှိသည့်အနက် hacker များဟာ Remote Administration Trojan လို့ ခေါ်တဲ့ Trojan အမျိုးအစားကို အသုံးပြု၍ အခြားသူတို့၏ ကွန်ပျူတာထဲသို့ ဝင်ရောက်နိုင်ရန် အသုံးပြုလေ့ရှိပါတယ်။ အဲဒီအထဲကမှ နာမည်ဆိုးနှင့်အကျော်ကြားဆုံး Remote administration Trojanကတော့ SubSeven ပဲဖြစ်ပါတယ်။ SubSeven သာသင့်ကွန်ပျူတာထဲသို့ဝင်ရောက်နေနိုင်ပြီဆိုလျှင် အင်တာနက်နှင့် ချိတ်ဆက်ပြီး onlineဖြစ်သွားတဲ့အခါမှာ hackerတွေဟာအဝေးကနေပြီး သင့်ကွန်ပျူတာထဲမှာရှိသမျှ dataအားလုံးကို access လုပ်နိုင်ပြီး သူအလိုရှိရာ information မှန်သမျှကို ခိုးယူသွားနိုင်စွမ်းရှိပါတယ်။

အဲဒီလို Trojan မျိုးကိုအသုံးပြုပြီး ထောက်လှမ်းနိုင်တဲ့ Spyware များလည်းရှိပါတယ်။ နာမည်ကျော်ကြားတဲ့ တစ်ခုကတော့ "Catch Cheat" ပဲဖြစ်ပါတယ်။ Survillence Tool တစ်ခုဖြစ်တဲ့ **Golden Eye** လိုမျိုး မိမိထောက်လှမ်းလိုတဲ့ ကွန်ပျူတာမှာသွားရောက် install လုပ်စရာမလိုပါဘူး။ မိမိထောက်လှမ်းလိုတဲ့ ကွန်ပျူတာထဲရောက်အောင် email ပို့လွှတ် လိုက်ရုံပါပဲ။

❑ Virus Hoaxes

Virus hoaxes ဆိုတာကတော့ virus များကဲ့သို့ ပွားပြီး (replicate) ကူးစက် စေနိုင်သော program များမဟုတ်ဘဲ virusများအကြောင်းနှင့် ဆက်နွယ်ပြီး မမှန်ကန်သော သတိပေးချက်များပါဝင်သော messageများပဲဖြစ်ပါတယ်။ အများအားဖြင့် တစ်ယောက်မှ တစ်ယောက်သို့ email များ forward လုပ်ခြင်းဖြင့်ပျံ့နှံ့စေပါတယ်။ အနီးစပ်ဆုံးမြန်မာမှုပြုရရင် ရွှေပေလွှာ သဘောမျိုးဖြစ်ပါလိမ့်မယ်။

hoax တွေထဲမှာ technical နှင့်ဆက်နွယ်သော အကြောင်းအရာများကို နားလည်ရန်ခက်ခဲသော စကားလုံးများဖြင့် ရေးသားဖော်ပြထားပြီး အခြားသူများဆီသို့ ဆက်လက်ပို့လွှတ်ရန် request လုပ်လေ့ရှိပါတယ်။ hoax message များဟာ ကွန်ပျူတာများကိုတိုက်ရိုက်အန္တရာယ်မပေးနိုင် ပါဘူး။ သို့သော် အချို့သော hoax များကတော့ virus များကဲ့သို့ အန္တရာယ်ကြီးပါတယ်။ hoax တစ်ခုမှာဆိုရင် ကွန်ပျူတာထဲမှာ သေချာပေါက်ရှိနေသော file တစ်ခုကို virus ပါသော file တစ်ခုအဖြစ်သတိပေးရာမှခိုင်းပြီး တွေ့ရှိပါက ဖျက်ပစ်ဖို့ရန်အကြံပေးပါတယ်။ ထို file ဟာမိမိကွန်ပျူတာ အလုပ်လုပ်စေရန်အတွက် မရှိမဖြစ် လိုအပ်သော system file တစ်ခုပင်ဖြစ်ပါတယ်။ ဒါကြောင့် hoax များဟာ virus များကဲ့သို့တိုက်ရိုက် အန္တရာယ်မပေးနိုင်သော်လည်း လက်ခံရရှိသူများကို စိတ်ရှုပ်ထွေးဝေခွဲမရဖြစ်စေပြီး ထို message များကိုဖတ်နေရခြင်းအားဖြင့် အချိန်ကုန် အကျိုးမရှိဖြစ်စေပါတယ်။

လက်ခံရရှိသော email အား hoax ဟုတ်မဟုတ် ဝေခွဲမရဖြစ်နေတဲ့အခါမျိုးနှင့် ကြုံလာပြီဆိုရင် www.hoax-slayer.com တို့လို website မျိုးတွေသွားရောက်၍ email title တွင်းပါစာသားများ ထည့်သွင်းကာရှာဖွေခြင်းဖြင့် hoax ဟုတ်မဟုတ်ကို ခွဲခြားနိုင်ပါတယ်။ အင်ပြီးဟ်နှင့်ပတ်သက်သော hoax တစ်ခုကို ဥပမာအနေနှင့် ဖော်ပြလိုက်ပါတယ်။

Read more information about this hoax

An example of the hoax email:

Subject: 2 MOONS ON 27 AUGUST 2007

27th August 2007, a Monday the Whole World is waiting for.....2 moons on 27th August 2007

Planet Mars will be the brightest in the night sky starting August. It will look as large as the full moon to the naked eye. This will cultivate on Aug. 27, 2007 when Mars comes within 34.65M miles of earth. Be sure to watch the sky on Aug. 27 12:30 am. It will look like the earth has 2 moons.

The next time Mars may come the close is in 2287.

Share this with your friends as NO ONE ALIVE TODAY will ever see it again.

virus များ၏အန္တရာယ်မှာကြီးမားသော်လည်းယင်းတို့ကိုကာကွယ်နိုင်ရန် နည်းလမ်းများလည်း ရှိပါတယ်။ Anti-virus Program များကိုထုတ်လုပ်သော Company များအနေဖြင့် နေ့စဉ်နှင့်အမျှဆိုသလို virusများအသစ်အသစ်ထွက်ပေါ်နေမှုကိုမျက်ခြေမပြတ်စောင့်ကြပ်ကြည့်ရှုလျက်ရှိပါတယ်။ဒါ့ကြောင့်လည်း virus အသစ်ထွက်ပေါ်လာသည်နှင့် မရွေးမနောင်းပင် ယင်း virusကိုမည်သို့မည်ပုံ ကာကွယ်နိုင်းရမည်ဆိုတဲ့နည်းလမ်းများကို ဖေါ်ထုတ်တင်ပြနိုင်စွမ်းရှိကြပါတယ်။

ဆိုရရင် အသစ်သစ်ထွက်ပေါ်လျက်ရှိသော virusများ၊ ထွက်ပေါ်ခဲ့ပြီးသော virus များနှင့် ပါတ်သက်သော သတိပေးချက်များ၊ ၄င်း virus တို့မည်သို့မည်ပုံ အလုပ်လုပ်ကြသလဲ၊ မည်သည့် အတိုင်းအတာထိ အန္တရာယ်ပေးဖျက်ဆီးနိုင်ပုံ အစရှိသည့် ကာကွယ်နိုင်မည့် နည်းလမ်းများ နှင့် ရှာဖွေရှင်းလင်း ဖယ်ရှားပေးနိုင်သော Removal Tools များကို Anti-virus Company ကြီးများ၏ website များတွင် အမြဲတစေ update လုပ်၍တင်ထားပေးပါတယ်။

ဒါကြောင့် Internetအသုံးပြုသူများအနေနှင့် Anti-virus websiteများကိုမကြာခဏဆိုသလို ဝင်ရောက်ကြည့်ရှု၍ virus အန္တရာယ်ကြုံတင်ကာကွယ်ခြင်း၊ နှိမ်နင်းခြင်းများပြုလုပ် နိုင်ကြပါတယ်။ အသုံးပြုသူ userများအနေနှင့်ဝင်ရောက်ကြည့်ရှုသင့်သော Anti-virus websiteများအနက်မှအချို့မှာ

- ➲http://securityresponse.symantec.com
- ➲http://home.mcafee.com/VirusInfo
- ➲http://threatinfo.trendmicro.com/vinfo/
- ➲http://www.f-secure.com/v-descs ..... တို့ပဲဖြစ်ပါတယ်။

Antivirus Software

virus များ နေ့စဉ်နှင့်အမျှဆိုသလိုပင် တစ်မျိုးပြီးတစ်မျိုး ပေါ်လာလျက်ရှိနေပါတယ်။ ယနေ့မှာတော့ မိမိတို့ကွန်ပျူတာထဲသို့ Virusများအများဆုံးဝင်ရောက်လေ့ရှိသည့် လမ်းကြောင်းတွေကတော့ email attachment များမှတစ်ဆင့် ဝင်ရောက်ကူးစက်ခြင်းနှင့် Removable disk လို့ခေါ်သည့် memory stick၊ external hard driveတို့မှတစ်ဆင့် ဝင်ရောက်ကူးစက်ခြင်းတို့ဖြစ်ပါတယ်။ အလားတူနောင်အနာဂတ်ကာလတွေမှာလည်း အခြားဝင်ပေါက်များမှနေ၍ Virus များအန္တရာယ်ကိုကြုံရနိုင်ပါသေးတယ်။ ဆိုရရင် ယနေ့အချိန်မှာတောင် အချို့သော website များကို သွားတက်ကြည့်နေမိတဲ့အခါမျိုးမှာပင် trojan များ၊ worm များ၏ အန္တရာယ်ကိုကြုံတွေ့လာရပြီဖြစ်ပါတယ်။

ယခုလို ကွန်ပျူတာကိုဒုက္ခပေးနိုင်တဲ့ Virus အမျိုးအစားတွေကလည်းများလာတယ်။ ဝင်ရောက်ကူးစက်ခံရနိုင်တဲ့ အခွင့်အလမ်းတွေကလည်း များလာတဲ့အတွက် များစွာစိုးရိမ်ကြောက်လန့် နေဖို့လည်းမလိုပါဘူး။ ကွန်ပျူတာအား Virus မဝင်နိုင်အောင် ကာကွယ်ပေးနိုင်တဲ့ Antivirus software တစ်ခုကို ထည့်သွင်း installထားမယ်။ အဲဒီ software ကိုအပြဲတမ်း updateဖြစ်အောင် လုပ်ထားမယ်ဆိုရင်များစွာစိုးရိမ်စရာမလိုဘဲစိတ်ချအသုံးပြုနိုင်မှာဖြစ်ပါတယ်။ ယနေ့အခါ Virus များအန္တရာယ်မှကာကွယ်ပေးနိုင်သော software အတော်များများပေါ်ထွက်လာလျက်ရှိပါတယ်။ Norton ၊ Kaspersky ၊ Mcafee ၊ Avira အစရှိသဖြင့် Antivirus software ရေးသားရောင်းချသည့် Vendor ပေါ်မူတည်ပြီးအမည်အမျိုးမျိုးပေါ့။

မည်သို့ပင်အမည်တွေကွဲလွဲပါစေ Antivirus program တို့၏လုပ်ဆောင်မှုများသည် အခြေခံအားဖြင့်အတူတူပင်ဖြစ်ပါတယ်။ ဆိုရရင် AVတို့သည် data တွေရဲ့ patternကိုကြည့်ပြီး virus ဟုတ်မဟုတ် virus ကပ်ငြိနေခြင်းရှိမရှိ ဆုံးဖြတ်ပါတယ်။ အကယ်၍များ file တစ်ခုမှာ virus ကပ်ငြိနေပြီဆိုရင် မူရင်းနဂို file အတိုင်း ပြန်လည်ရရှိအောင် ကပ်ငြိနေတဲ့ virus(malicious code) များကို ဖယ်ထုတ်ရှင်းလင်းပါလိမ့်မယ်။ ဒါကို repair လုပ်တယ်လို့ခေါ်တယ်။ အဲဒီလိုမှ repair လုပ်လို့မရရင် ဆက်လက်မပြန့်နှံ့နိုင်အောင် quarantine ထဲပို့မယ်။ သို့မဟုတ် လုံးဝဖျက်ထုတ်ပါလိမ့်မယ်။

အဲဒီလို virus ကပ်ငြိနေခြင်းရှိမရှိနှင့် ဖယ်ရှားရှင်းလင်းခြင်းများကို AV program တို့ရဲ့ Scan Engine ဆိုတဲ့အပိုင်းကနေ အဓိကလုပ်ဆောင်ပါတယ်။ ဒါ့ကြောင့် AV pro တစ်ခုအောင်မြင်မှုရှိမရှိဆိုတာသည် scan engine ရဲ့စွမ်းဆောင်မှုပေါ်များစွာမူတည်ပါတယ်။ ဒါက အရေးအကြီးဆုံးအခြေခံအစိတ်အပိုင်းတစ်ခုပါ။ ဒါ့အပြင်virus definition က date အောက်နေလျှင်update လုပ်ရန် အသိပေးနိုင်ခြင်း၊ အလိုအလျောက် update လုပ်ပေးနိုင်ခြင်း၊ အသုံးပြုသူတို့မေ့နေလျင်တောင်မှ အချိန်ကျလျင် အလိုအလျောက် scan လုပ်ခြင်း၊ web browser ၊ email program တို့နှင့် ပူးပေါင်း၍ realtime စစ်ဆေးကာကွယ်ပေးနိုင်ခြင်းအစရှိသည့် feature တွေပေါ်လည်းများစွာမူတည်ပါသေးတယ်။

ယနေ့ခေတ်ကွန်ပျူတာများမှာရှိတဲ့ တန်းဝင်AV programတွေမှာတူညီတဲ့ feature တွေပါရှိသည့် အတွက် install လုပ်ပုံတွေ၊setup လုပ်ပုံတွေဟာ တစ်ခုနှင့်တစ်ခု များစွာမကွာခြားလှပါဘူး။ တစ်မျိုးကိုဘဲ ကျွမ်းကျွမ်းကျင်ကျင် သုံးနိုင်ဖို့လိုတယ်။ တစ်မျိုးကိုသုံးနိုင်ပြီဆိုရင် လိုအပ်လို့နောက်တစ်ခု ပြောင်းသုံးပါက အနည်းငယ်လေ့လာလိုက်ရုံဖြင့် ကျွမ်းကျွမ်းကျင်ကျင် ကိုင်တွယ်သုံးနိုင်ပါလိမ့်မယ်။

ဒီလမ်းညွှန်စာအုပ်မှာတော့ Antivirus Program နှစ်ခုအကြောင်းကိုဖော်ပြသွားပါမယ်။ ပထမဦးစွာအခကြေးငွေပေးစရာမလိုပဲ free download ရယူသုံးနိုင်တဲ့ AV program တွေထဲက Avira Antivirဖြင့် ပြည့်ပြည့်စုံစုံ ဖော်ပြသွားပါမယ်။ ပြီးမှ စျေးကွက်အတွင်းလွယ်လွယ်ကူကူဝယ်သုံးနိုင်ပြီဖြစ်တဲ့ Kasperskyအကြောင်းကိုအကျဉ်ချုံးတင်ပြသွားမှာဖြစ်ပါတယ်။

Avira AntiVir(Free Edition)

အချို့သော အခမဲ့ဆိုတဲ့ freeware များသည် အသုံးပြုသူတို့အတွက် ဆိုးကျိုးများကိုပါ ဖြစ်စေနိုင်ခြင်းကြောင့် အသုံးမပြုခင်မှာလွန်စွာသတိထားဖို့လိုပါတယ်။ သို့သော် ယခုဖော်ပြမည့် Avira Antivir freeware ကတော့စိတ်ချလက်ချအသုံးပြုနိုင်သော Antivirus programတစ်ခုပင်ဖြစ်ပါတယ်။ Avira ကို Install ပြုလုပ်သုံးမည်ဆိုပါက Virus များ၊ Worm များ၊ trojan များ၏ အန္တရာယ်မှ အပြည့်အဝကာကွယ်ပေးနိုင်အောင် မိမိတို့ရဲ့ကွန်ပျူတာမှာအောက်ဖော်ပြပါ Service များကို လုပ်ဆောင်ပါလိမ့်မယ်။

- ➲Resident Protection
- ➲On-Demand Scanner
- ➲Virus database Update
- ➲Automatic Update feature
- ➲AntiSpyware protection

➤Resident Protection သည် နောက်ကွယ်မှနေ၍ကွန်ပျူတာတွင်းရှိ fileများအား (CD၊ Memory stickအပါအဝင်) Virus ကြောင့်တစုံတရာအပြောင်းအလဲဖြစ်မှုများကိုစောင့်ကြည့်စစ်ဆေးပေးနိုင်ပါတယ်။

➤Automatic Update featureသည် Virus definition ကိုအမြဲတမ်း update ဖြစ်နေရန် အတွက် အလိုအလျောက် Update လုပ်ပေးနိုင်ပါတယ်။

➤AntiSpyware protection သည်spyware၊ adware များအားစောင့်ကြည့်စစ်ဆေးပေးနိုင်စွမ်းပြီး အန္တရာယ်ကင်းရှင်းကြောင်းကိုအာမခံပေးနိုင်ပါတယ်။

Download Avira Antivir(Free edition)

Avira အား download ရယူနိုင်တဲ့ မူရင်းဌာနေ Site ကတော့ **www.free-av.com** ပဲဖြစ်ပါတယ်။ ဌာနေ Site ကနေ download ရယူနိုင်သလို www.download.com၊ www.tucows.com အစရှိတဲ့ download siteများကနေလည်း အလွယ်တကူရှာဖွေရယူနိုင်ပါတယ်။ ဒီလမ်းညွှန်မှာတော့ ဌာနေ site ကနေdownload ရယူပုံများကို ဖော်ပြသွားပါမယ်။

1) Avira အား downloadရယူရန် **www.free-av.com** သို့သွားပါ။ **Download free Antivir** တွင် clickနှိပ်ပါက Antivir installer အား download ရယူနိုင်သော pageသို့ရောက်ပါမည်။

2) Download nowတွင် click နှိပ်ပါ။ www.download.comသို့ရောက်သွားပြီး downloadရယူရမည့် linkကိုတွေ့ရပါမယ်။

3)Download now တွင်ထပ်မံ clickနှိပ်လိုက်ပါ။ ပုံမှန်အားဖြင့် ဆိုရင် download dialogbox ကျလာပြီး installer fileကိုစတင် downloadရယူနိုင်ရမှာဖြစ်ပါတယ်။ ဒါပေမယ့်အချို့သော ကွန်ပျူတာတွေမှာဆိုရင် download dialogbox ကျမလာဘဲ security အရ block လုပ်ထားကြောင်းဖော်ပြသော barတစ်ခု ကိုသာ IE ရဲ့အပေါ်ဘက်မှာတွေ့ရပါမယ်။

4)security warning barပေါ်တွင် clickနှိပ်ပါက menu တစ်ခုကျလာပါမည်။ menu ထဲရှိ **Download file**တွင် clickနှိပ်လိုက်ပါ။ download dialogboxပွင့်လာပါလိမ့်မယ်။ **Save**တွင် clickနှိပ်၍မိမိ မှတ်မိလွယ်မည့်နေရာတွင် downloadရယူသိမ်းဆည်းထားလိုက်ပါ။

Installing Avira(Free edition)

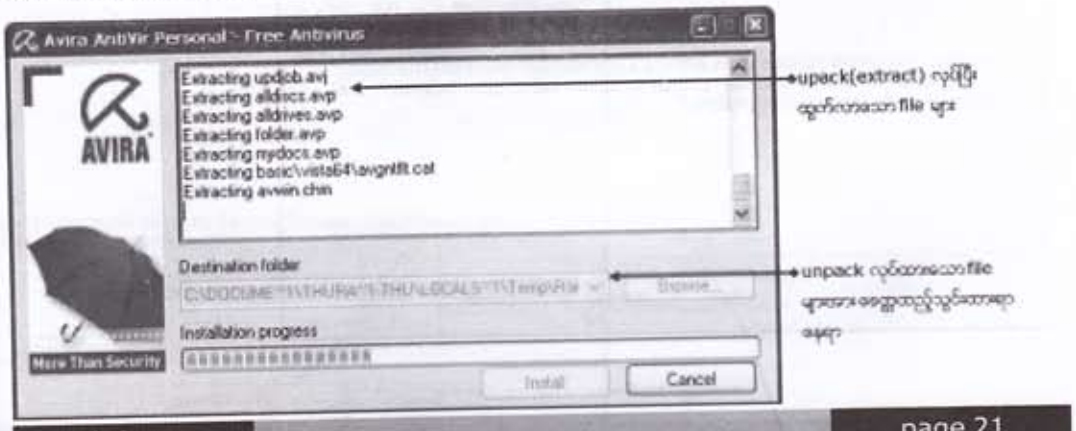
ကွန်ပျူတာများကို အင်တာနက်နှင့် online ချိတ်ဆက်ပြီး file များကို share လုပ်၍ ကွန်ပျူတာ တစ်လုံးမှ တစ်လုံးသို့ပို့လွှတ်ခြင်း၊ download ရယူခြင်းတို့ဟာ ယနေ့အချိန်မှာတော့ အသုံးများတွင်ကျယ် နေပြီ။ အဲဒီလိုအသုံးပြုကြရာမှာ file များ (သို့) program များရဲ့အရွယ်အစားပေါ်များစွာမူတည်နေပါတယ်။ ဆိုရင် file size ကြီးနေရင်ကြာမယ်၊ ဖွင့်ရင်မြန်မယ်ပေါ့။ ဒါကြောင့် အင်တာနက်ပေါ်မှာ website အတော် များများဟာ fileများကိုမူလနဂိုအရွယ်ထက်ငယ်အောင် compressလုပ်ပြီး download ရယူနိုင်ရန်တင်ထား လေ့ရှိပါတယ်။

ယနေ့အခါအင်တာနက်ကနေ download ရတဲ့ software installer အများစုတို့သည် pack လုပ်ထားသော file များဖြစ်ပါတယ်။ pack လုပ်တယ်ဆိုတာက install လုပ်ဖို့ရန်လိုအပ်သော နဂိုမူလ data file တွေ၊ DLL file တွေကိုစုပေါင်းပြီး exe file တစ်ခုတည်းဖြစ်အောင် လုပ်ထားခြင်းဖြစ်ပါတယ်။ သဘောက အမယ်တွေအများကြီးကိုပုံးတစ်ပုံးထဲစုပေါင်းထည့်သွင်း၍ ကျစ်ကျစ်လစ်လစ်ဖြစ်အောင် ထုပ်ပိုးပြီး ပေးသလိုမျိုးပေါ့။ နောက်ပိုင်းမှာဖော်ပြမယ့် Kaspersky installer file သည်လည်းယခုလို pack လုပ်ထား သော exe file ဖြစ်ပါတယ်။

ဒီလို pack လုပ်ထားသည့် file တို့ကိုသုံးမယ်ဆိုရင် ဦးစွာပထမ unpack လုပ်ရတယ်။ ပြီးမှ သုံးလို့ရတယ်။ သို့သော် pack လုပ်ထားသော exe file တို့ကို unpack(extract) လုပ်ရန်သီးခြား soft-ware မလိုပါဘူး။ self extracter ပါပြီးသားဖြစ်တဲ့အတွက်ကြောင့် double click နှိပ်ရုံဖြင့် သူဘာသာ အလိုလျောက် unpack လုပ်ပေးပါတယ်။ ပြီးမှ စတင် install ကြရပါတယ်။ ဒါက Avira မှ မဟုတ်ပါဘူး။ အင်တာနက်က download ဆွဲယူ install တဲ့အခါမှာကြုံရနိုင်တာတွေဖြစ်ပါတယ်။

Step1) Unpacking

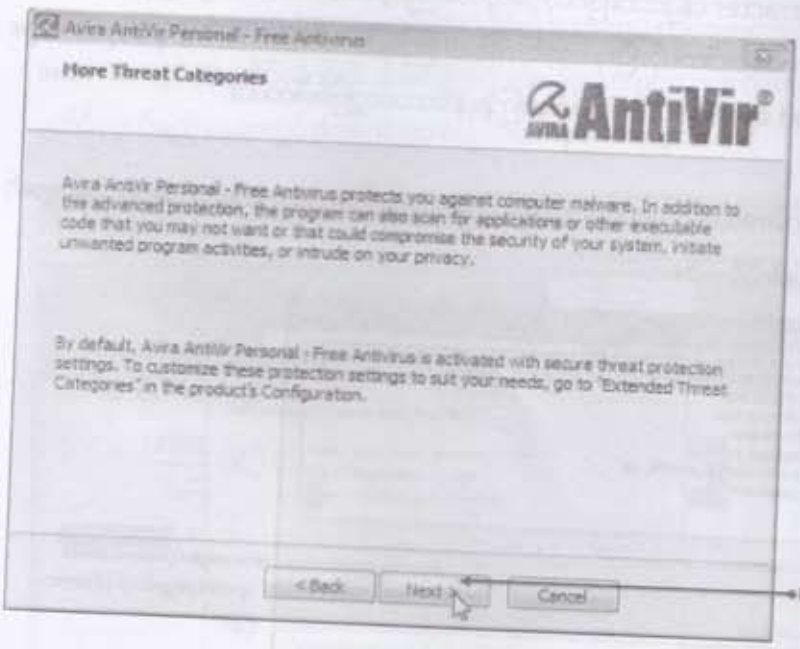
အင်တာနက်မှ download ရယူထားသော file ပေါ်တွင် double click နှိပ်လိုက်ပါ။ အလိုလျောက် unpack(extract) လုပ်ပါလိမ့်မယ်။



step 2) Welcome

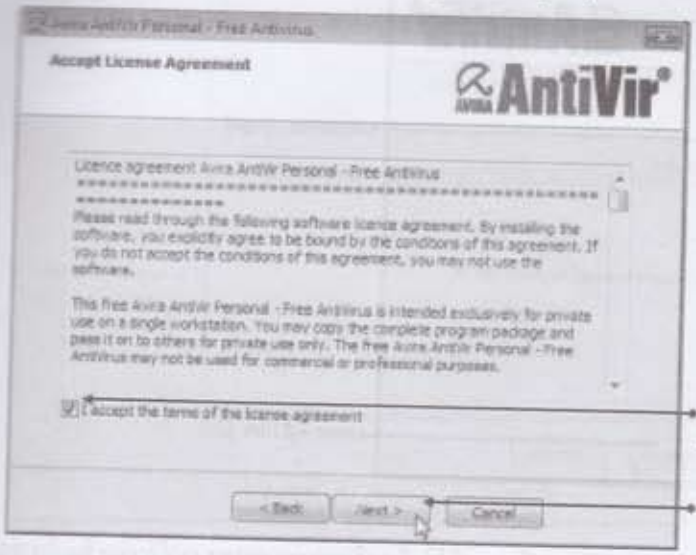
Unpack လုပ်ပြီးတဲ့အခါ install လုပ်ဖို့ရန် အဆင်သင့် ဖြစ်သွားပြီး Welcome Wizardကို မြင်ရပါမယ်။ **Next** တွင် clickနှိပ်လိုက်ပါ။

Step 2) More threat Categories



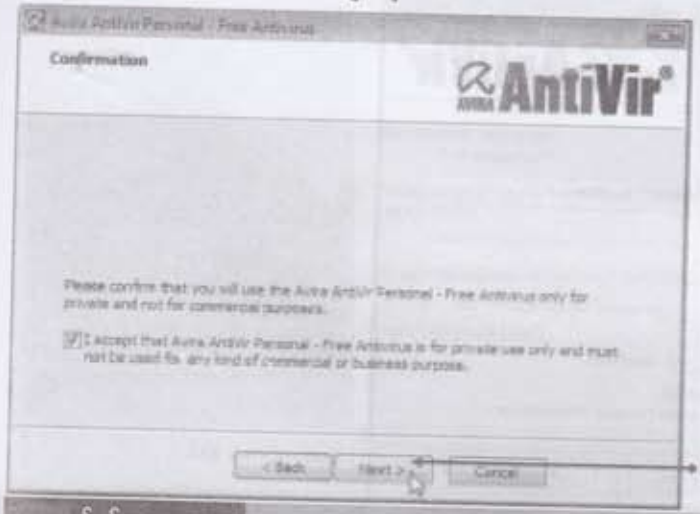
Step3) License Agreement

License Agreement ထဲမှာဆိုရင် အဓိကအားဖြင့် program ကို copy ကူးယူပြီး အခြားသူ တို့အား ဖြန့်ဝေခြင်းမလုပ်ပါဘူးဆိုတာကို အာမခံခိုင်းတာမျိုးပါလေ့ရှိပါတယ်။ မည်သည့်နည်းနှင့်မဆို သဘောတူလက်ခံမှသာ ရှေ့ဆက် installလုပ်ခွင့်ရမှာဖြစ်ပါတယ်။ **I accept**တွင် ☑ အမှန်ခြစ်ပေါ်အောင် click တစ်ချက်နှိပ်ပါ။ ထို့နောက် **Next** တွင် Clickနှိပ်လိုက်ပါ။



Step 4) Confirmation

License Agreement ကို သဘောတူကြောင်းထပ်မံအတည်ပြုချက်တောင်းသော Confirmation Wizard ကိုမြင်ရပါမယ်။ I acceptဘေးရှိ checkboxတွင် ☑ အမှန်ခြစ်ပေါ်အောင် select မှတ်ပြီး **Next** တွင် Click တစ်ချက်နှိပ်ပါ။

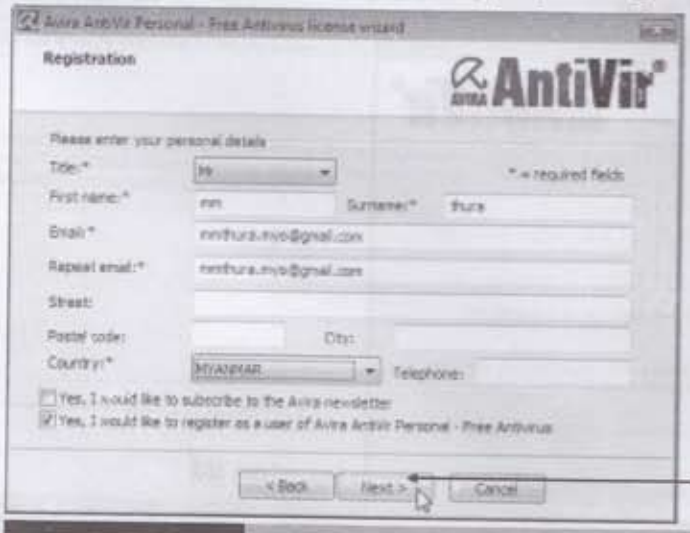


Step 5) Choose Installation Type

Installation typeကို ရွေးချယ်ပေးရပါမယ်။ customကိုရွေးချယ်မည်ဆိုပါက programရဲ့ ဘယ်အစိတ်အပိုင်းတွေကို install လုပ်မယ်။ ဘယ်ဟာတွေကိုတော့ installမလုပ်ဘူး အစရှိသဖြင့် ကိုယ်တိုင်စဉ်းစားပြီးရွေးချယ်ကြရပါလိမ့်မယ်။ **Complete** တွင်ရွေးချယ်ပြီး **Next**တွင် clickနှိပ်ပါ။

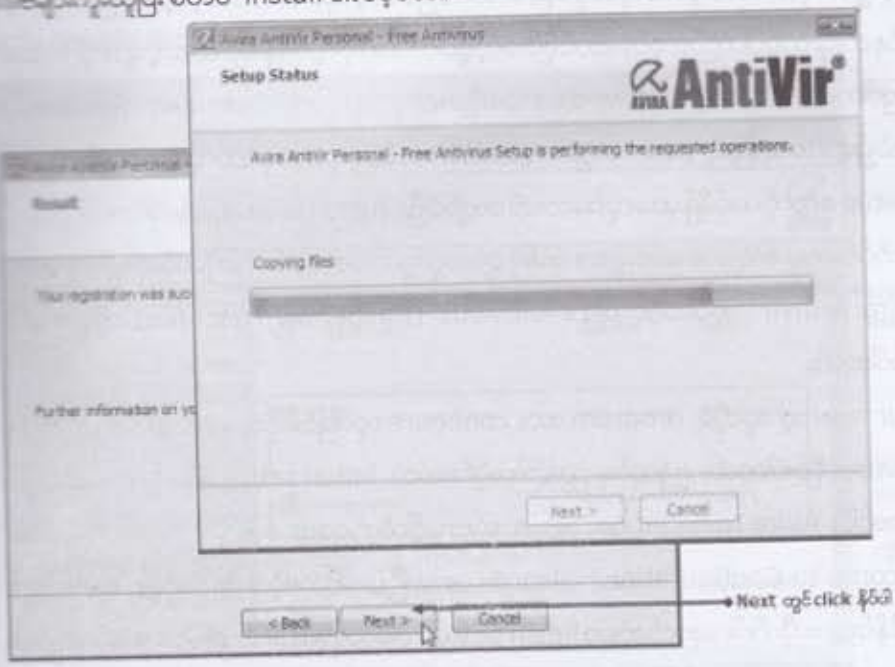
Step 6) Registration

Antivirမှတောင်းဆိုသော အချက်အလက်များကို ဖြည့်စွက်ကာ register လုပ်ကြရပါမယ်။ asterisk (*) ပြထားသောနေရာသည် မဖြစ်မနေ ဖြည့်စွက်ရမည့်နေရာများဖြစ်ပြီး ကျန်တာတွေကတော့ ဖြည့်လိုကဖြည့်၊ မဖြည့်ချင်ကဒီအတိုင်းကွက်လပ်ထားလည်းရပါတယ်။ ဖြည့်စွက်ပြီးပါက **Next**တွင် click နှိပ်ပါ။ အင်တာနက်ပေါ်ရှိ Antivirမှ serverတို့နှင့်ချိတ်ဆက်ပြီး register လုပ်ပါလိမ့်မယ်။



Step 7) Result

Registerလုပ်ပြီးကြောင်းဖော်ပြသော wizard ရှိ **Next**တွင် click နှိပ်လိုက်ပါ။ လိုအပ်သော fileများကူးယူပြီး စတင် install ပါလိမ့်မယ်။



Step 8) Installation complete

Antivir ကိုအောင်မြင်စွာ installလုပ်ပြီးကြောင်း ဖော်ပြသော wizard ပဲဖြစ်ပါတယ်။ **Finish** တွင် click နှိပ်လိုက်ပါ။ ဒါဆိုရင် Antivirအားကွန်ပျူတာမှာ installလုပ်ပြီးသွားပြီ။

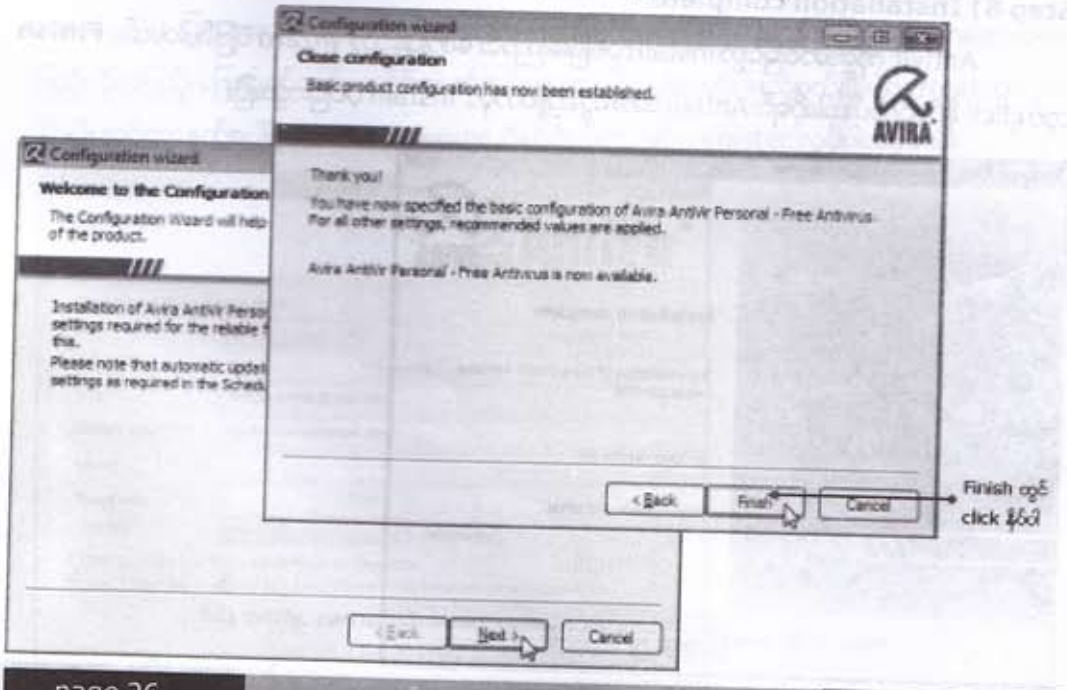
Initial Setup

အထူးသဖြင့် security ပိုင်းနှင့်ဆိုင်တဲ့ softwareတစ်ခုကိုလုပ်ပြီးတိုင်း အဲဒီ software program သည်ကွန်ပျူတာမှာကောင်းစွာအလုပ်လုပ်နိုင်အောင်မဖြစ်မနေလုပ်ဆောင်သင့်တဲ့အခြေခံလုပ်ငန်းစဉ်တွေကိုထုတ်နှတ်ပြီးတစ်ပါတည်းလုပ်ဆောင်ခိုင်းလေ့ရှိပါတယ်။ ထိုလုပ်ငန်းစဉ်အဆင့်များကို initial setup လို့ခေါ်ကြပါတယ်။ Activationတို့၊ Updating တို့၊ Registeringတို့၊ Scanningတို့ဖြစ်ပါတယ်။

အကယ်၍များအသုံးပြုသူ user ကကျွမ်းကျင်တယ်။ ဘယ်နေရာကနေဘာလုပ်ရမယ်ဆိုတာတွေသိရင် initial setup တွေကိုယခုချိန်မှာမလုပ်သေးဘဲကျော်ခဲ့ပြီး Installation ကို အဆုံးသတ်လိုက်လို့ရပါတယ်။ နောက်ပိုင်းကျမှ အေးအေးဆေးဆေး တစ်ခုချင်းရွေးချယ် setup လုပ်ကြမယ်ဆိုရင်လည်းရပါတယ်။ဒါက Avira Antivir အပါအဝင်အခြား Antivirus (Kaspersky ၊ McAfee) တို့မှာလည်းဒီအတိုင်းပင်ဖြစ်ပါတယ်။

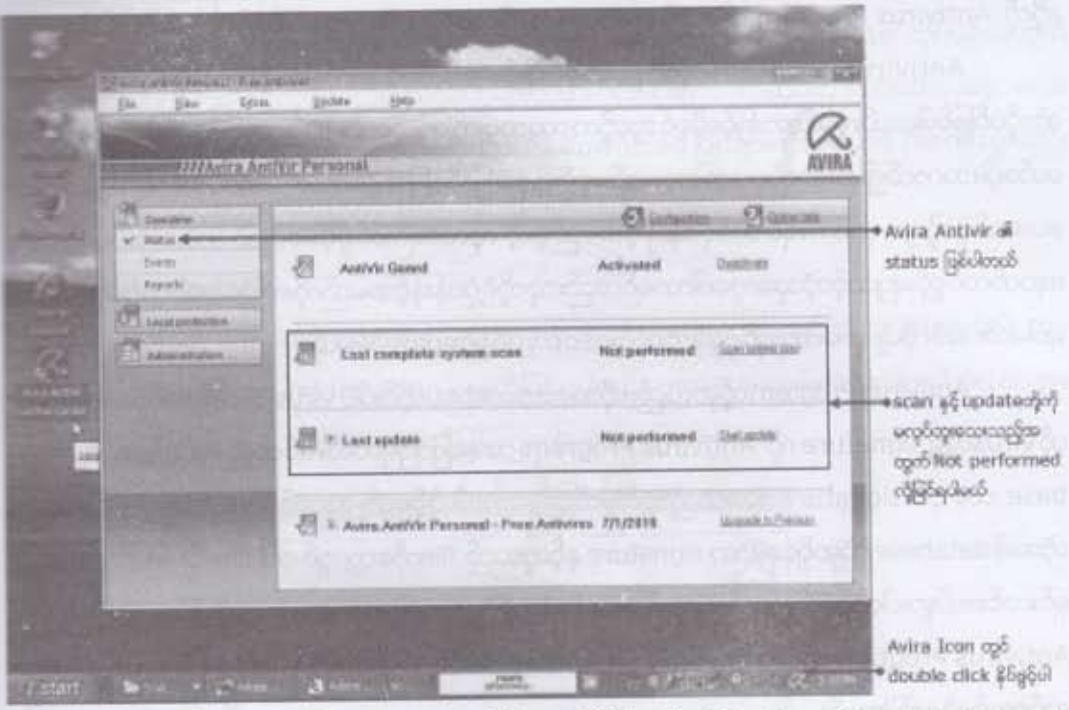
Antivir ကတော့ သူတို့ရဲ့ program အား configure လုပ်ခြင်းကိုသာ initial setup အနေနှင့် အဓိကလုပ်ဆောင်ခိုင်းပါတယ်။ ဤတွင်မှ ညွှန်ကြားခိုင်းစေတဲ့ initial setup များကို တစ်ဆင့်ချင်းလိုက်ပါလုပ်ဆောင်ပြီး Avira Installation အားအဆုံးသတ်လိုက်ရအောင်။

"Welcome to Configuration" wizard ကနေစပြီးပေါ်လာတဲ့အဆင့်တိုင်းမှ Next တွင် click တစ်ချက်စီနှိပ်သွားလိုက်ပါ။ နောက်ဆုံးမှာ finish button ပါသော wizard ကိုမြင်ရပါမယ်။ **Finish** တွင် click နှိပ်ပြီး initial setup လုပ်ခြင်းအားအဆုံးသတ်လိုက်ပါ။



Open Avira

Avira Antivirusအားဖွင့်ရန် desktopပေါ်တွင်ရှိသော iconပေါ်တွင် double click နှိပ်၍ဖွင့်ပါ။ အလားတူပင် ကွန်ပျူတာ Screen ၏ညာဘက်ထောင့်အောက်ခြေတွင်ရှိသော Taskbarထဲရှိ iconတွင်လည်း double click နှိပ်၍ဖွင့်နိုင်ပါတယ်။



Avira ပွင့်လာတဲ့အခါ statusကနေစမြင်ရမှာဖြစ်ပါတယ်။အဲဒီ statusထဲမှာ Antivir Guard သည် activate ဖြစ်မဖြစ်၊ကွန်ပျူတာတွင် virusများရှိမရှိ၊နောက်ဆုံးအကြိမ်ရှာဖွေစစ်ဆေးခဲ့သောရက်စွဲ၊ နောက်ဆုံးအကြိမ် update လုပ်ခဲ့သော virus definition ရက်စွဲတို့ကိုတွေ့ရပါမယ်။ မိမိရဲ့ကွန်ပျူတာကို virusများအန္တရာယ်မှကာကွယ်တားဆီးနိုင်ရန်အရေးကြီးဆုံးက updateလုပ်ရမယ်။ scan လုပ်ရမယ်။ (ဒီ update နှင့် scanning ဆိုတာတွေက ဘယ် Antivirus programကိုပဲသုံးသုံးမဖြစ်မနေ လုပ်ဆောင်ရမယ့်လုပ်ငန်းစဉ်များဖြစ်သည့်အတွက် ဘာကြောင့် updateလုပ်ရမယ်။ဘယ်လိုscan လုပ်ရမလဲဆိုတာတွေကို အဝိုင်းလိုက်ခွဲပြီးတတ်နိုင်သမျှအပြည့်အစုံဆုံးဖြစ်အောင် ဖော်ပြသွားပါမယ်။)

မှတ်ချက် - "Auto protect"featureဖြစ်တဲ့ Antivir Guard သည် အမြဲတမ်း activated ဖြစ်နေဖို့လိုပါတယ်။သို့မှသာ real timeကာကွယ်ပေးနိုင်မှာဖြစ်ပါတယ်။အကြောင်းတစ်ခုခုကြောင့် ထီးကလေးပိတ်ပြီးDeactivated ဖြစ်နေပါက activate တွင် click နှိပ်ကာ ထီးပြန်ဖွင့်ပေးဖို့လိုပါတယ်။

Virus Update

Antivirus Programတစ်ခုကို ကွန်ပျူတာမှာ Install ပြီးရုံဖြင့် virus တို့ရန်မှ ကင်းဝေးသွားပြီး virus တွေမဝင်ရောက်နိုင်တော့ဘူးလို့ယူဆ၍မရပါ။ Antivirus တွေဆိုတာက သူတို့သိတဲ့ virus မျိုးတွေရဲ့ ရန်ကသာ ကာကွယ်ပေးနိုင်ပါတယ်။ နေ့စဉ်နှင့်အမျှထွက်ပေါ်ပျံနှံ့လျက်ရှိသည့် အသစ်အသစ်သော virus တို့ကို Antivirus Program တို့သည် သူဖာသာအလိုအလျောက်တော့ မမြင်နိုင် မတားဆီးနိုင်ပါဘူး။

Antivirus Program တို့ကို ဥပမာခိုင်းနှိုင်းရရင် ဂိတ်ပေါက်စောင့်တဲ့လုံခြုံရေး ဝန်ထမ်းများကဲ့သို့ပင်ဖြစ်ပါတယ်။ ပုံမှန်အားဖြင့်ဆိုရင် သူတို့က လာသမျှကိုကြည့်မယ်။ ID တောင်းယူစစ်ဆေးဝင်ခွင့်ပေးမယ်ပေါ့။ အကယ်၍များအရပ်ပုပု၊ အသားမည်းမည်း၊ နဖူးပြောင်ပြောင်နဲ့ကောင် "အောင်အောင်" လို့ခေါ်တယ် ပေးမဝင်နဲ့လို့များ မှာထားရင် အဲဒီပုံပန်းနှင့်အမည်ရှိတဲ့ လူလာရင် ဝင်ခွင့်မပေးဘဲ တားထားပါလိမ့်မယ်။ နောက်ထပ်ခွင့်မပြုသင့်တဲ့သူတွေပေါ်လာရင်လည်း သူတို့ရဲ့ပုံပန်းနှင့်အမည်ကို လုံခြုံရေးဆီထပ်မံပို့ပေးထားရပါမယ်။ အဲဒီလိုမျိုးမှာမထားရင် ပုံမှန်အတိုင်းစစ်ဆေးဝင်ခွင့်ပေးပါလိမ့်မယ်။

Antivirus Programတို့မှာလည်းထိုသဘောတရားအတိုင်းပါပဲ virus အသစ်တစ်ခုပေါ်လာတိုင်း ထို virusတို့ရဲ့ signature ကို Antivirus Program အားပြောပြရတယ်။ ဒီတော့မှ Program ရဲ့ data-base ထဲမှ ၄င်း signature အားထည့်သွင်းမှတ်သားထားပါလိမ့်မယ်။ နောက်ပိုင်းကွန်ပျူတာကို စစ်ဆေးတဲ့အခါ database ထဲမှာရှိနေသော signature နှင့်တူသည့် fileကိုတွေ့လျှင် ၄င်း fileကို virus ဟုသိရှိပြီး ရှင်းလင်းဖယ်ရှားပါလိမ့်မယ်။ သည့်အတွက် အသစ်အသစ်ထွက်ပေါ်လာသော virusတို့၏ signature အား Antivirus Program တို့အားပြောပြရန်ဖြစ်ပါတယ်။ အဲဒီလိုပြောပြခြင်းကို virus definition update လုပ်တယ်လို့ခေါ်ပါတယ်။

virus အသစ်တစ်မျိုးပေါ်လာတိုင်း Antivirus ထုတ်လုပ်ရောင်းချသူများ(Vendor)သည် သူတို့ရဲ့ website ၊ သူတို့ရဲ့ update server တွေမှာ virus definition(ဝါ) virus signature fileတွေကို တင်ထားပေးလေ့ရှိပါတယ်။ အသုံးပြုသူတွေကလည်း virus definition တစ်ခုထွက်လာတိုင်းအဲဒီ file ကိုရယူပြီးမိမိကွန်ပျူတာ Antivirus Program ကိုအမြဲတမ်း update ဖြစ်အောင်လုပ်ပေးဖို့လိုပါတယ်။ သို့မှသာ အသစ်အသစ်ထွက်ပေါ်လာသော virusတို့ကိုမြင်နိုင်တားဆီးနိုင်မှာဖြစ်ပါတယ်။

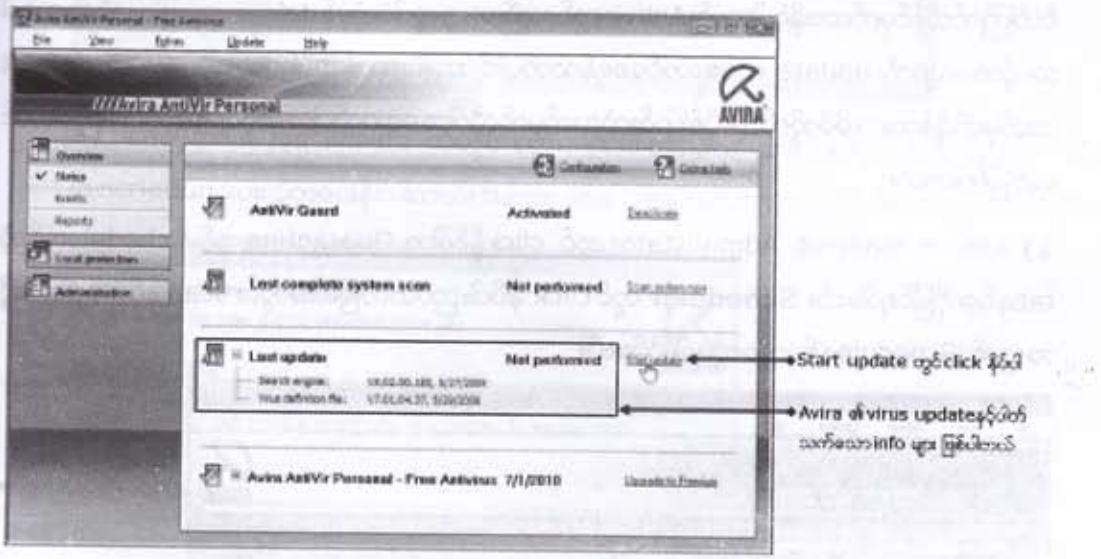
Update မှာမှ ၂မျိုးရှိတယ်။ Online Update နှင့် Offline Update ။ Online Update ဆိုတာက အင်တာနက်ချိတ်ဆက်ပြီး updateလုပ်ခြင်းဖြစ်ပါတယ်။ အလွယ်ကူဆုံး update လုပ်ခြင်းလည်းဖြစ်ပါတယ်။ အများအားဖြင့် program ထဲကနေ Start update လို့နှိပ်လိုက်တာနှင့် update server ဖြင့်ချိတ်ဆက်ကာ virus definition file အား download ရယူပြီးအလိုအလျောက် install လုပ်သွားမှာဖြစ်ပါတယ်။

အဲဒီထက်ပိုလွယ်ချင်သေးရင် ဘယ်နေ့ဘယ်အချိန်မှာ update လုပ်ပါဆိုပြီး program မှာ setting တွေထည့်ခိုင်းထားလို့ရပါတယ်။ ခိုင်းထားတဲ့နေ့ အချိန်ရောက်တာနှင့် သူဖာသာ အလိုအလျောက် update ရယူ install ပါလိမ့်မယ်။ ဒီနည်းဟာ အင်တာနက်ချိတ်ဆက်ထားသော ကွန်ပျူတာကနေ online update လုပ်ခြင်းဖြစ်ပါတယ်။

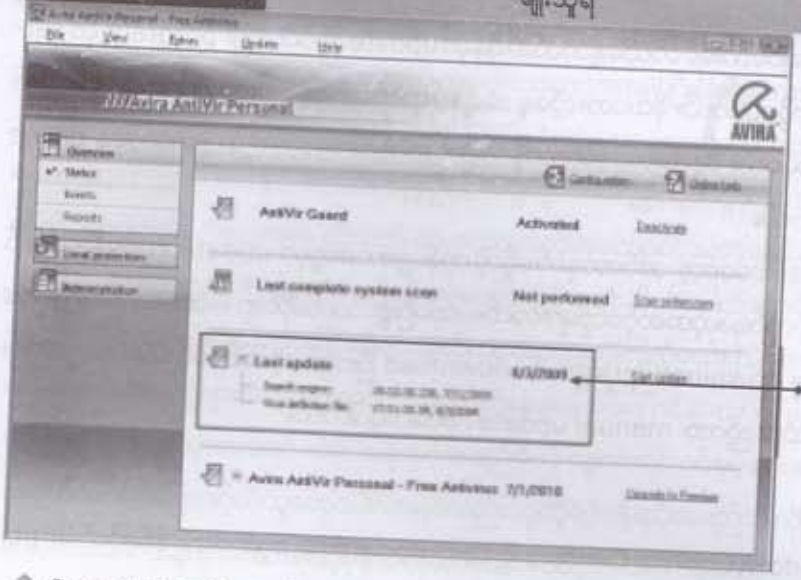
Offline Update ကတော့ အင်တာနက်မရှိတဲ့ ကွန်ပျူတာတွေမှာ update လုပ်ရန်အတွက် ဖြစ်ပါတယ်။ သူကကျတော့ လုပ်ရမယ့်အဆင့်တွေများတယ်။ ပထမဦးစွာ သက်ဆိုင်ရာ websiteကနေ virus definition fileကိုရှာဖွေ download ရယူရတယ်။ download ပြီးသွားတဲ့အခါ အဲဒီ fileကို ကူးယူပြီး updateလုပ်လိုတဲ့စက်ထဲထည့်ကာ manual update လုပ်ပေးရပါတယ်။

Online Update

1) Avira Main Window(Control Center) ရှိ Last update တွင် click နှိပ်လိုက်ပါ။ update နှင့်ပတ်သက်သော information များကိုမြင်ရပါမယ်။ updateမလုပ်ရသေးပါက "database status" နေရာတွင် Not Performed လို့မြင်ကြရပါမယ်။



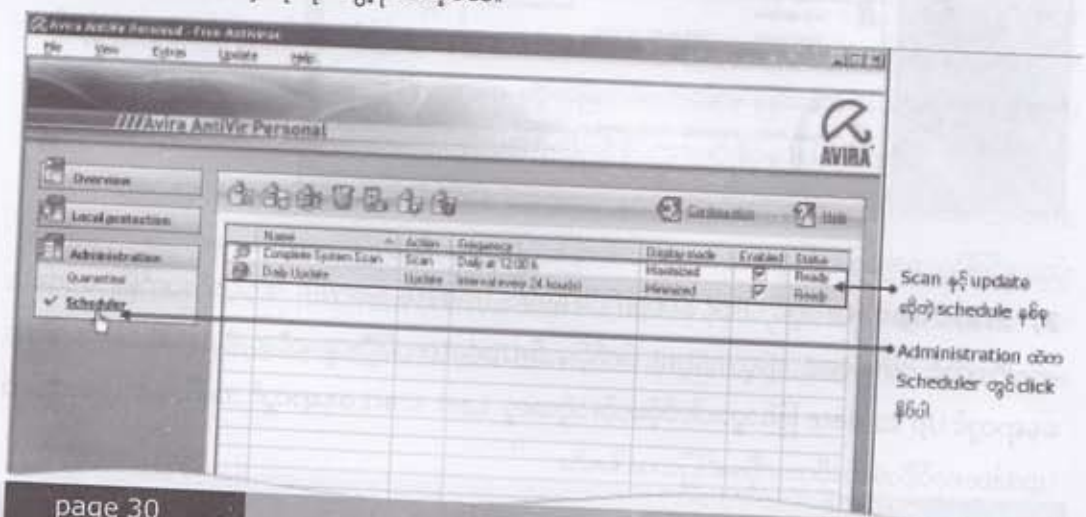
2) Start update တွင် click နှိပ်လိုက်ပါ။ Avira Update Server နှင့်ချိတ်ဆက်ပြီး update များကို စတင် dowload ရယူ install ပါလိမ့်မယ်။Updateလုပ်ပြီးသွားတဲ့အခါ database status နေရာတွင် Up to date ဖြစ်သွားပါလိမ့်မယ်။ ထို့အတူ Last start နေရာတွင် ဘယ်နေ့ဘယ်အချိန်က update လုပ်ခဲ့တယ်ဆိုတာကိုဖော်ပြထားပါမယ်။



Automatic Virus Update

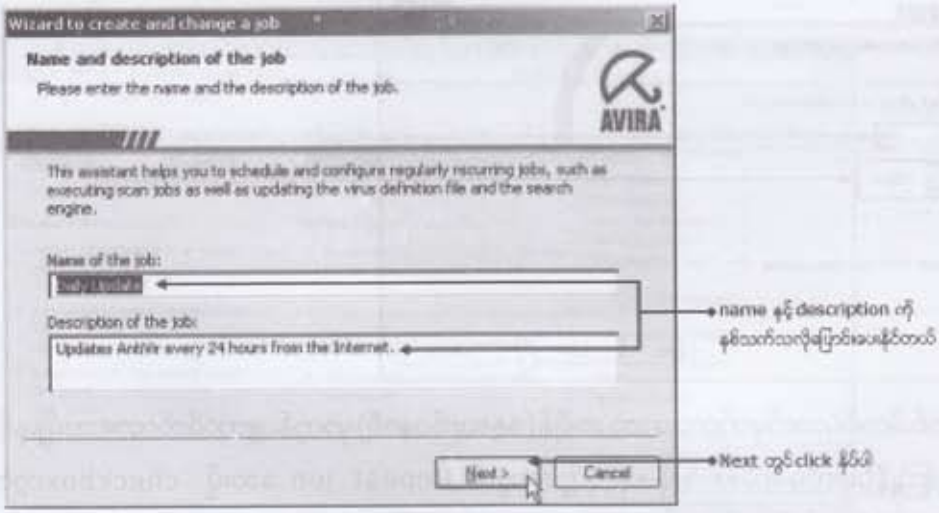
Antivirus programများတွင် Virus update လုပ်စေလိုသော အချိန်များကို မိမိတို့စိတ်ကြိုက်သတ်မှတ်ထားနိုင်ပါတယ်။ Antivirတွင်လည်းအတူတူပါပဲ။ ပုံမှန် default အားဖြင့် တစ်နေ့တစ်ခါ အလိုအလျောက် update လုပ်ဆောင်စေရန်သတ်မှတ်ထားပြီးသားဖြစ်ပါတယ်။သို့သော် ထို default သတ်မှတ်ချိန်အစား မိမိတို့လိုသလိုပြောင်းလဲသတ်မှတ်လိုပါက အောက်ပါအဆင့်များအတိုင်းလုပ်ဆောင်ရမှာဖြစ်ပါတယ်။

1) Antivir windowရှိ Administatorတွင် clickနိပ်ပါက Quarantine နှင့် Schedulerဆိုတဲ့ tabနှစ်ခုကိုမြင်ရပါမယ်။ **Scheduler** တွင် click နိပ်ပါ။ ညာဘက်ခြမ်းအတွင်း Scan နှင့် updateတို့အတွက် Scheduleနှစ်ခုကိုတွေ့ရပါလိမ့်မယ်။

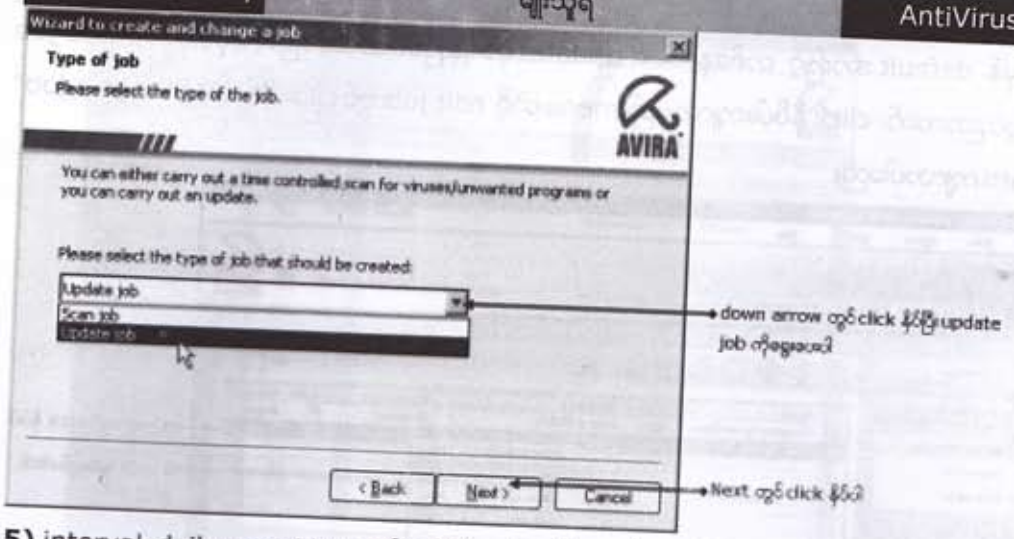


2) ပုံမှန် default အားဖြင့် တစ်နေ့တစ်ခါ update လုပ်ရန် ဖြစ်ပါတယ်။ ပြောင်းလိုပါက update job ပေါ်တွင် ညာဘက် click နှိပ်ပါ။ကျလာမည့် menu ထဲရှိ edit jobတွင် click နှိပ်ပါ။ "change a job" wizard ကျလာပါမည်။

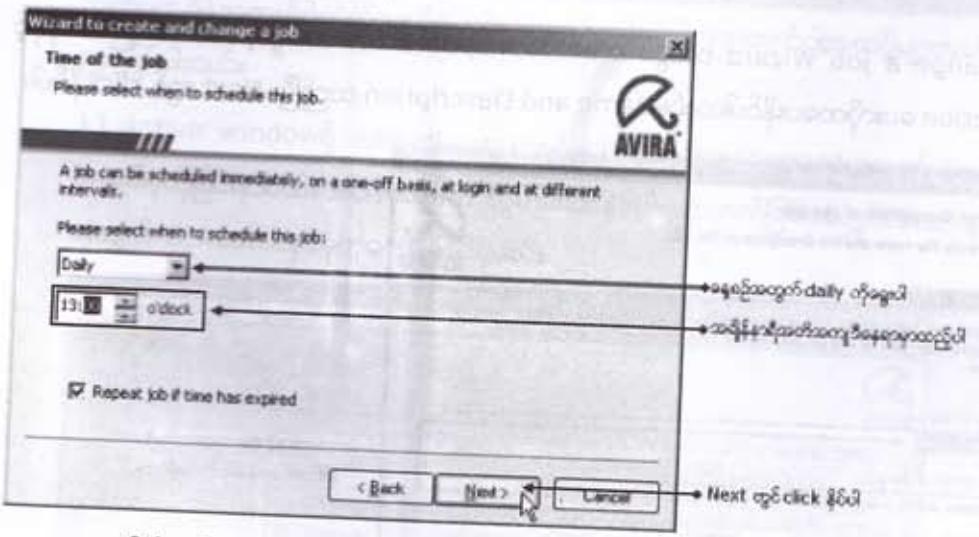
3) "change a job"Wizard ထဲတွင် scan လား update လား အစရှိတဲ့ Job အမည်တစ်ခုနှင့် description ပေးလိုကပေးနိုင်ပါတယ်။ Name and Description ထည့်ပြီး Next တွင် clickနှိပ်ပါ။



4) scan jobကိုပြင်မှာလား update job ကိုပြင်မှာလားဆိုတာကိုရွေးချယ်ပေးရပါမယ်။ယခု update ကိုပြင်မှာဖြစ်သည့်အတွက် update jobကိုရွေးချယ်ပြီး **Next** တွင် နှိပ်ပါ။

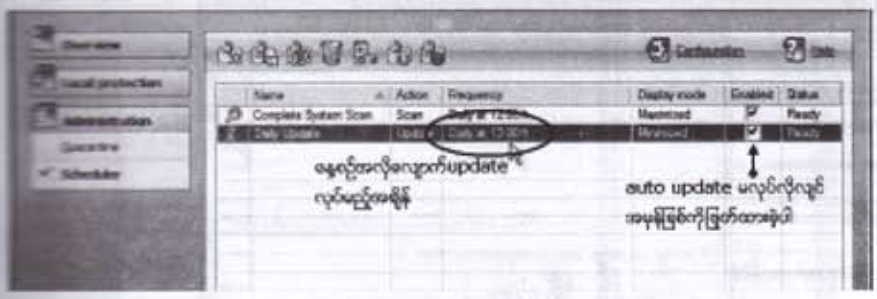


5) interval၊ daily ၊ weekly အစရှိသဖြင့် schedule လုပ်ထားနိုင်ပါတယ်။ ပုံမှန် default အားဖြင့် Interval နှင့် schedule လုပ်ထားပါတယ်။ အကယ်၍များနေ့စဉ်ဘယ်နှစ်နာရီထိုး(ဥပမာ နေ့လည်၁နာရီ) တွင် အလိုလျောက် update လုပ်ပါဆိုတာမျိုးအချိန်အတိုအကျနှင့်လုပ်လိုလျှင် dailyကိုရွေးပါ။ O'clock နေရာတွင် နေ့လည်၁နာရီအတွက် 13:00 ဖြစ်အောင်ထည့်ပါ။ ဒါဆိုရင်နေ့စဉ်နေ့လည်၁နာရီထိုးတာနှင့် အလိုအလျောက် updateလုပ်ပါလိမ့်မယ်။



တစ်ခါတစ်ရံသတ်မှတ်ထားသော အချိန်(နေ့လည်၁နာရီ)မှာကွန်ပျူတာပိတ်ထားတာမျိုးနှင့် ကြုံကောင်းကြုံနိုင်ပါလိမ့်မယ်။ အဲဒီလိုအခြေခံမျိုးအတွက် Repeat job ဘေးရှိ checkboxတွင် အမှန်ခြစ်ဖြစ်အောင်ရွေးခဲ့ပါက သတ်မှတ်ချိန်ကျော်သွားသော်လည်းကွန်ပျူတာဖွင့်တာနှင့်အလိုအလျောက် သူဖာသာ updateလုပ်ပေးပါလိမ့်မယ်။ စိတ်ဝိုင်းကျပြင်ဆင်သတ်မှတ်ပြီးပါက Next တို့တွင် clickနှိပ်ပြီး

ရွေးထက်သွားပါ။နောက်ဆုံးမှာတော့ scheduler ထဲတွင် update job အတွက်အချိန် (နေ့လည်၁နာရီသို့) ပြောင်းသွားတာ ကိုတွေ့ရပါမယ်။ (မှတ်ချက် - ဤအဆင့်များအတိုင်းပင် Scan job ကိုလည်းမိမိတို့ လိုသလိုပြောင်းလဲကာ schedule လုပ်ထားနိုင်ပါတယ်။)

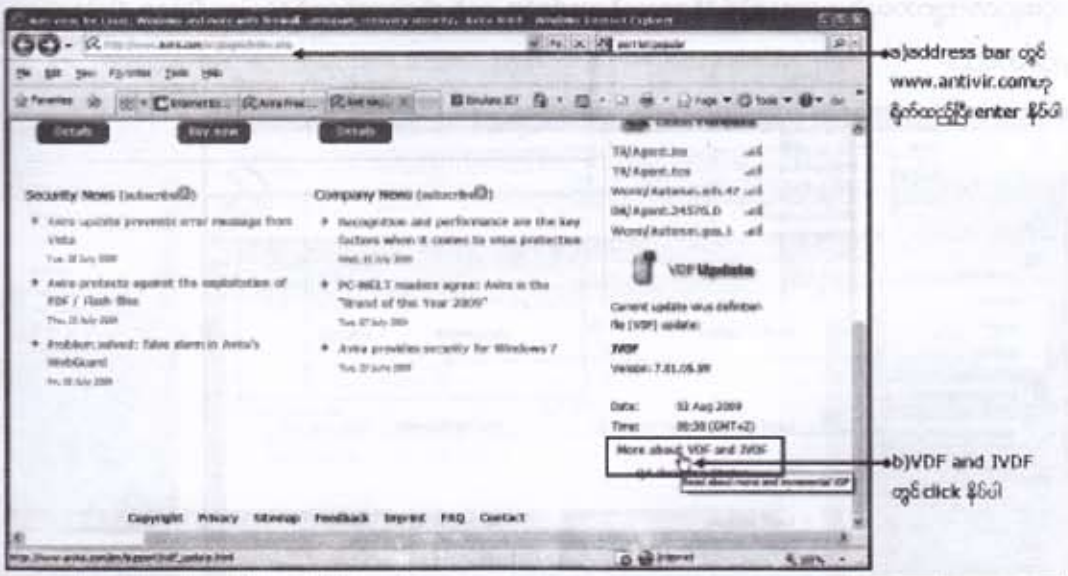


Antivir Manual Update

ရှေ့မှာဖေါ်ပြခဲ့တဲ့ virus update သည်အင်တာနက်မှတစ်ဆင့် Antivir server နှင့်ချိတ်ဆက်ပြီး online update လုပ်ပုံများပဲဖြစ်ပါတယ်။ယခုဖေါ်ပြမယ့် update လုပ်ပုံကတော့ virus definition file ကို manual download ရယူပြီးမှ update လုပ်ပုံများပဲဖြစ်ပါတယ်။အင်တာနက်နှင့် ချိတ်ဆက်ထားခြင်းမရှိသောကွန်ပျူတာများမှာ update လုပ်နိုင်စေရန်အတွက်ဖြစ်ပါတယ်။

❑Download virus definition update file

1) Avira virus update အား download ရယူရန် **www.antivir.com** သို့သွားပါ။ **"VDF and IVDF"** တွင် click နှိပ်ပါ။ download ရယူနိုင်သော update file ပါဝင်သည့် page ကိုတွေ့ရပါမည်။

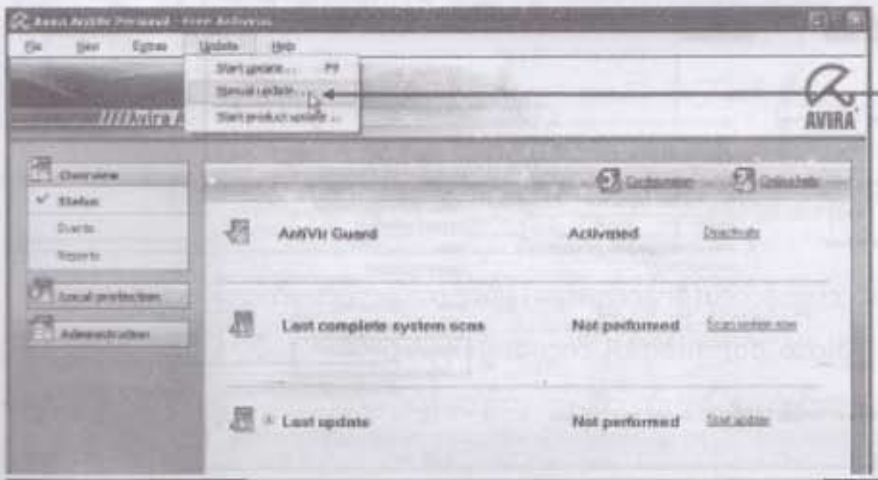


2) သက်ဆိုင်ရာ update file ပေါ်တွင် click တစ်ချက်နှိပ်ပါက "file download" dialogue box ကျလာပါလိမ့်မည်။ save တွင် click နှိပ်ပြီး မိမိမှတ်မိလွယ်မည့် folder တစ်ခုအောက်တွင် သိမ်းဆည်းထားလိုက်ပါ။

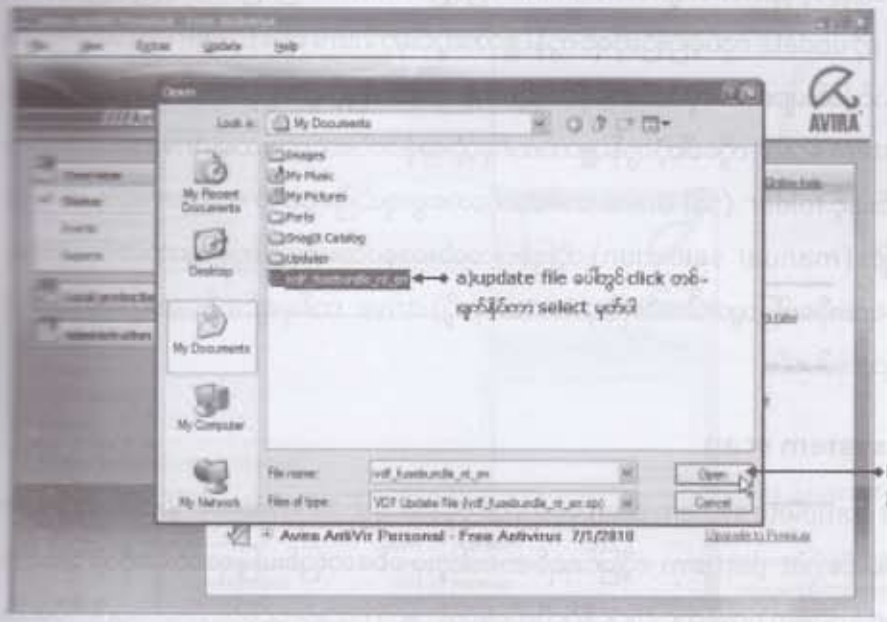
❑Updating Avira Virus Definition

virus definition file မိမိစက်ထဲရှိပြီဆိုရင် စတင် update လုပ်လို့ရပါပြီ။ အရေးကြီးတာက ကွန်ပျူတာထဲက ဘယ်နေရာမှာရှိသလဲ ဆိုတာလောက်တော့ သိထားရပါမယ်။

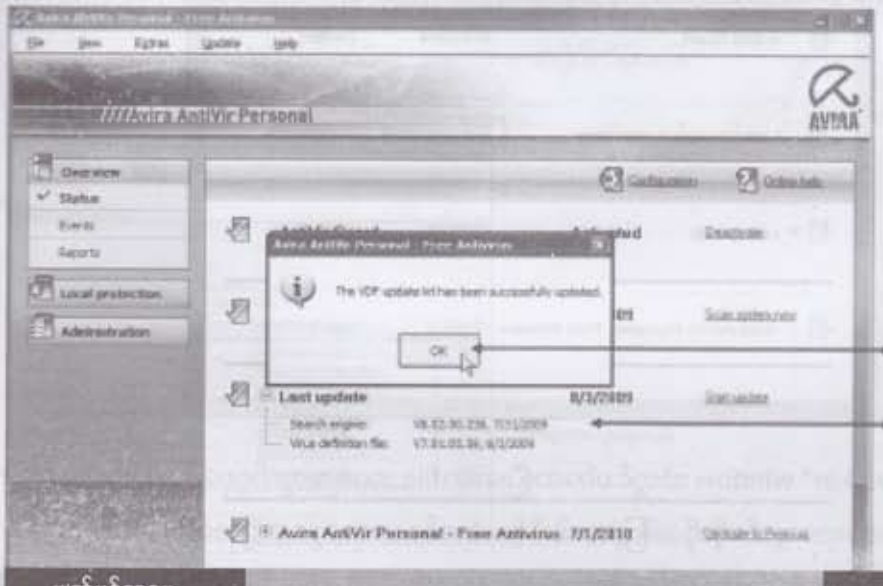
1) Virus updateပြုလုပ်ရန်အတွက် Avira main windowရှိ **Update** တွင် click တစ်ချက်နှိပ်ပါ။ ထို့နောက်ကျလာမည့် menu ထဲရှိ **Manual update** တွင် click တစ်ချက်နှိပ်ပါက Open dialogbox ကျလာမည်။



2) Open dialogbox ထဲတွင် မိမိ download ရယူထားခဲ့သော Avira update file ကို ရွေးချယ်ပေးရပါမည်။



update file ရှိရာကို ရွေးချယ်ခဲ့ပြီးပါက **Open** button တွင် click တစ်ချက် နှိပ်ပါ။ မိမိညွှန်ပြခဲ့သော file ထဲတွင် သွားရောက်ရှာဖွေပြီး၊ တွေ့ရှိပါက virus update စတင်လုပ်ဆောင်ပါလိမ့်မည်။ update လုပ်ပြီးတဲ့အခါအောင်မြင်စွာပြီးစီးကြောင်း ဖော်ပြတဲ့ message ကိုမြင်ရပြီဆိုရင် last update နေ့ရာ မှာပါရက်စွဲပြောင်းသွားတာကိုတွေ့ရပါမယ်။

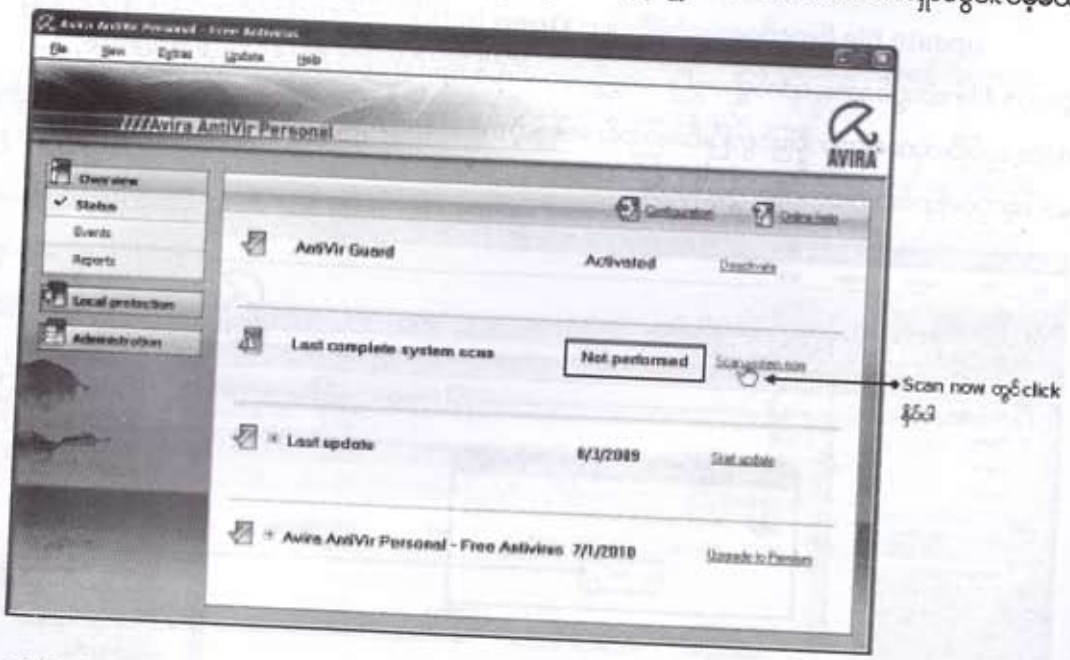


◈ Virus များအားရှာဖွေရှင်းလင်းခြင်း

ရွေမှာဖေါ်ပြခဲ့တဲ့ နည်းလမ်းများထဲက online ပဲဖြစ်ဖြစ်၊ offline ပဲဖြစ်ဖြစ် တစ်နည်းနည်းနှင့် virus definition ကို update လုပ်ခဲ့ပြီးပြီဆိုရင် ကွန်ပျူတာတွင်းမှာ viurs များ၊ trojan များ၊ worm များ ရှိမရှိ ရှာဖွေရှင်းလင်းခြင်းများ အားလုပ်ဆောင်နိုင်ပါပြီ။ အကြမ်းအားဖြင့် ရှာဖွေရှင်းလင်းပုံ နှစ်မျိုးရှိတယ်။ "complete system scan" လို့ခေါ်တဲ့ကွန်ပျူတာတစ်ခုလုံးအနှံ့ တပ်ဆင်ထားသမျှ drive အားလုံးထဲမှာ ရှာဖွေစစ်ဆေးခြင်း နှင့် folder (သို့) drive တစ်ခုခုကိုသာရွေးချယ်ပြီး(ဥပမာ - removable drive) စစ်ဆေး ရှာဖွေခြင်း (manual selection) တို့ဖြစ်ပါတယ်။ယခုပထမဦးစွာ ကွန်ပျူတာတစ်ခုလုံးအနှံ့ ရှာဖွေရှင်းလင်းပုံများကိုဖေါ်ပြသွားပါမယ်။ ပြီးမှ folder (သို့) drive တစ်ခုချင်းစစ်ဆေးရှာဖွေပုံများကို ဆက်လက်ဖေါ်ပြသွားပါမယ်။

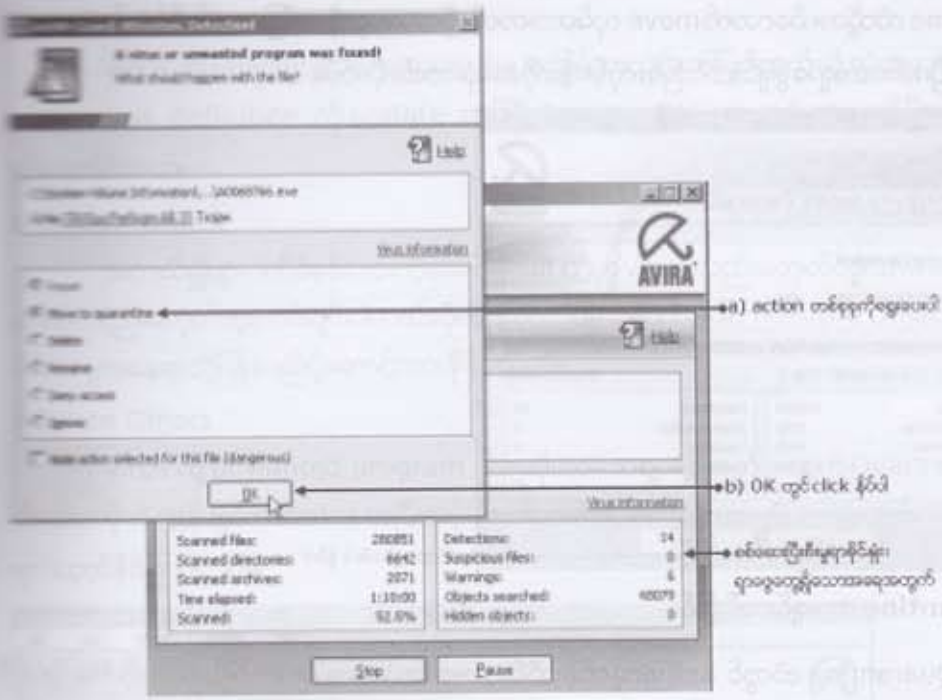
❑complete system scan

1) Avira ရဲ့ last complete system scan နေရာတွင် ပုံမှန်အားဖြင့် နောက်ဆုံးအကြိမ်စစ်ဆေးခဲ့သောရက်စွဲကိုတွေ့ရပါမယ်။ not perform လို့မြင်ရရင် တစ်ခါဘူးမှ စစ်ဆေးခြင်းမပြုရသေးပါဆိုတဲ့ သဘောဖြစ်ပါတယ်။ Scan system now တွင် click နှိပ်လိုက်ပါ။ ကွန်ပျူတာအားစတင်စစ်ဆေးရှာဖွေပါလိမ့်မယ်။

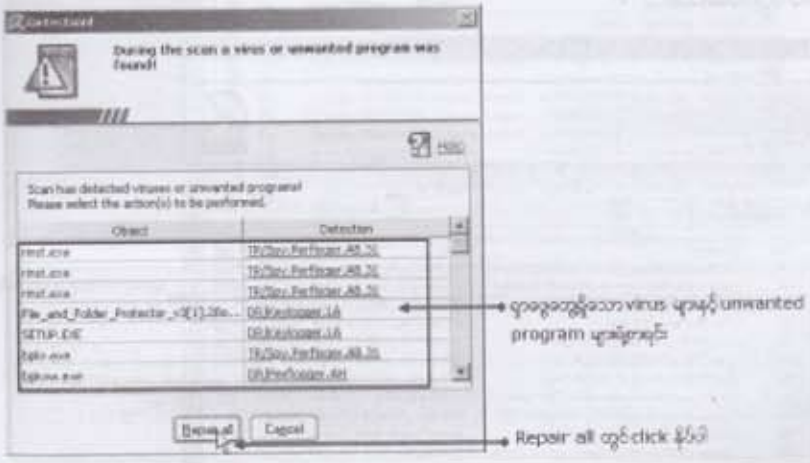


2) "Luke filewalker" window ထဲတွင် စစ်ဆေးပြီးသော file အရေအတွက်စုစုပေါင်း၊ ပြီးစီးမှုရာခိုင်နှုန်း၊ ရှာဖွေတွေ့သောအရေအတွက် တို့ကို ဖေါ်ပြထားပါလိမ့်မယ်။ စစ်ဆေးရှာဖွေနေစဉ်အတွင်း virus (သို့)

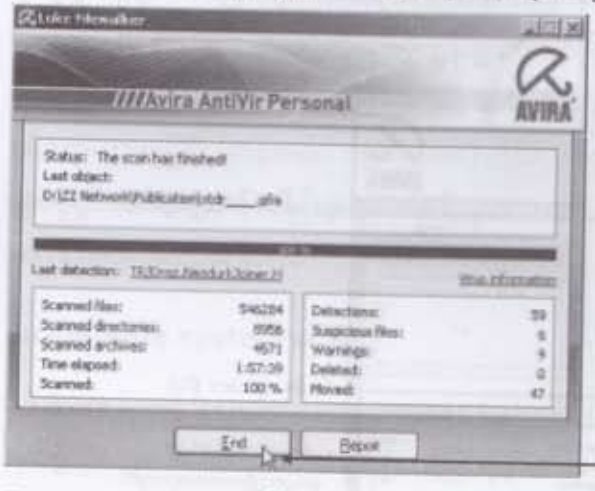
unwanted program တစ်ခုခုကိုတွေ့ရှိပါက Alert များဖြင့် အသိပေးလေ့ရှိပြီး delete ၊ repair ၊ quarantine အစရှိသည့် action များထဲကတစ်ခုခုကိုရွေးချယ်အတည်ပြုပေးရပါတယ်။



3)ကွန်ပျူတာတစ်ခုလုံး စစ်ဆေးပြီးသွားတဲ့အခါ ရှာဖွေတွေ့ရှိသော virus နှင့် unwanted program များအားဖော်ပြထားပါလိမ့်မယ်။ repair all တွင် click နှိပ်လိုက်ပါ။ မူရင်းနဂို file အတိုင်းပြန်လည်ရရှိအောင် ကပ်ညှိနေတဲ့ virus(malicious code) များကို ဖယ်ထုတ်ရှင်းလင်းပါလိမ့်မယ်။ အဲဒီလိုမှ repair လုပ်လို့မရရင် ဆက်လက်မပျံနှံနိုင်အောင် quarantine ထဲပို့ပါလိမ့်မယ်။



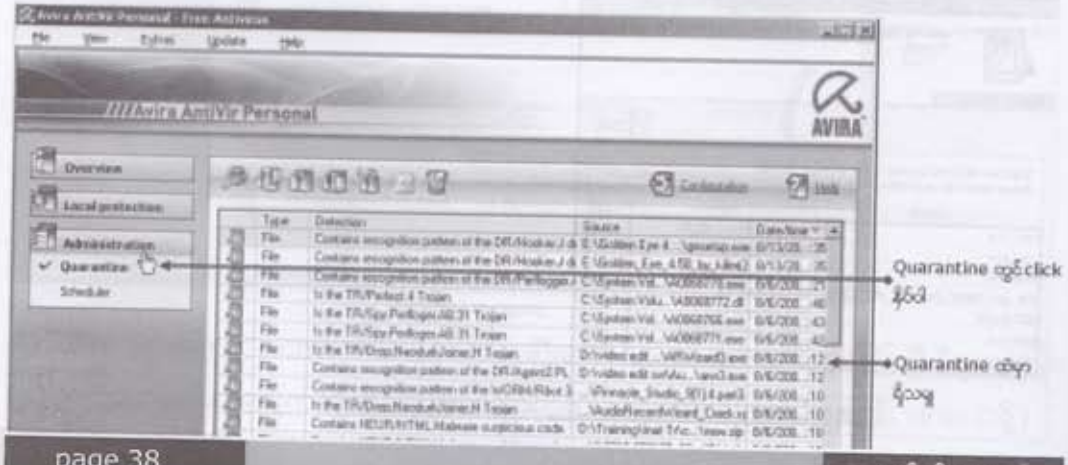
4)repair လုပ်လို့ရနိုင်တာတွေ repair လုပ်၊ လုပ်လို့မရနိုင်တာတွေ quarantine ထဲရွေးပြီးတဲ့အခါ စစ်ဆေးခဲ့သော file အရေအတွက်၊ရှာဖွေတွေ့သော virus နှင့် unwanted program အရေအတွက်နှင့် quarantine ထဲသို့ဘယ်လောက် move လုပ်ထားတယ်ဆိုတာတွေကို ဖော်ပြထားပါလိမ့်မယ်။ End တွင် click နှိပ်ပြီး စစ်ဆေးရှာဖွေရှင်းလင်းခြင်းလုပ်ငန်းကို အဆုံးသတ်လိုက်ပါ။



❑Quarantine အားရှင်းလင်းခြင်း

Quarantine ထဲတွင် Antivirမှထိန်းသိမ်းထားသော Virus များကပ်ငြိနေသည့် file များကို တွေ့ရပါမယ်။ထို file များကို သေချာအောင်ထပ်မံ scan လုပ်ဖို့ရန်ကြိုးစားကြည့်နိုင်သလို အကယ်၍ ကပ်ငြိနေတာလုံးဝသေချာနေတယ်၊ repair လုပ်လို့မရနိုင်တော့တဲ့အခါမျိုးမှာ ဖျက်ပစ်လိုပါကလည်း ဒီနေရာမှာဖျက်ထုတ်နိုင်ပါတယ်။

1) control window ထဲက **Administration** တွင် click နှိပ်လိုက်ပါ။ Quarantine ထဲတွင်ထိန်းသိမ်းထားသော file များအားတွေ့ရပါမယ်။



Quarantine ထဲက file တစ်ခုခုပေါ်တွင် right-click နှိပ်ကြည့်ပါ။ Rescan Object ၊ Restore Object နှင့် Delete Object ဆိုတဲ့အဓိက option သုံးမျိုးပါသော menu တစ်ခုကျလာပါမယ်။

►Rescan Object

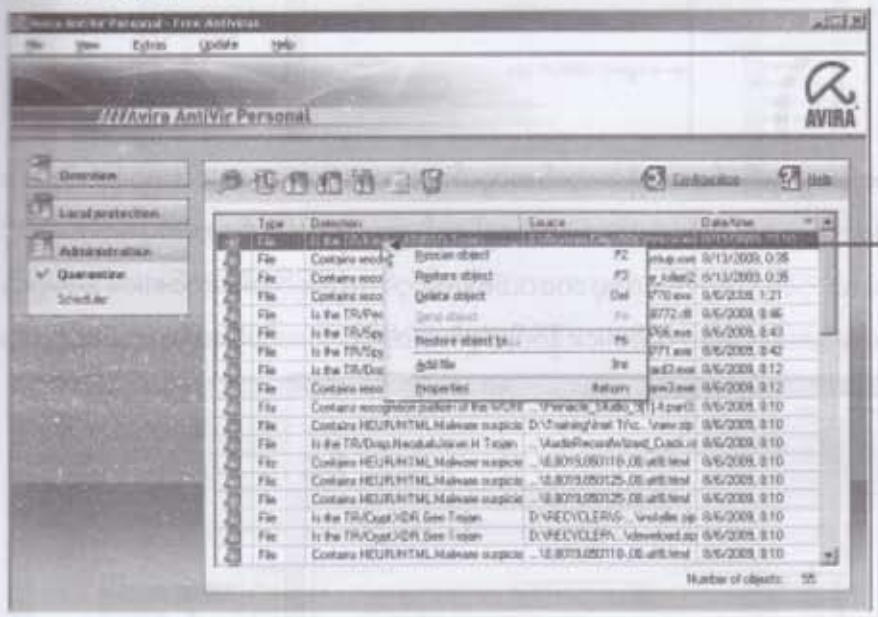
virus သို့ unwanted program file အဖြစ်မှားယွင်းဖော်ပြပါတယ်လို့ သံသယရှိတဲ့ အခါမျိုး အတွက် virus definition ကို update လုပ်ပြီး Rescan Object တွင် click နှိပ်ကာ ပြန်လည် စစ်ဆေးနိုင်တယ်။

►Restore Object

အကယ်၍များ ထပ်မံစစ်ဆေးတဲ့အခါ result ထဲမှာ virus လည်းမဟုတ်ဘူး unwanted program လည်းမဟုတ်ဘူး ကင်းရှင်းပါတယ်ဆိုတဲ့သဘောမျိုးဖော်ပြထားပါက Restore Object တွင် click နှိပ်ကာ မူလနေရာသို့ပြန်လည်ပို့ဆောင်ထားနိုင်ပါတယ်။

►Delete Object

virus သို့ unwanted program file ဆိုတာသေချာနေသည့်အတွက် Quarantine ထဲမှာ ဆက်ထားလိုဘဲ ကွန်ပျူတာထဲကနေ အပြီးအပိုင် ဖျက်ထုတ်လိုက Delete Object တွင် click နှိပ်ကာ ဖျက်ထုတ်နိုင်ကြပါတယ်။

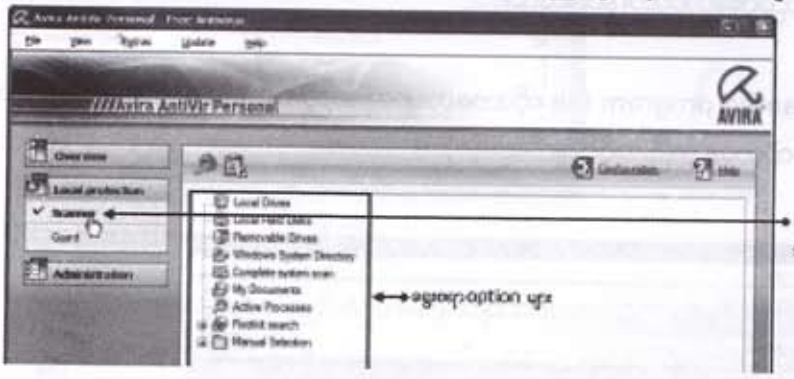


မှတ်ချက် - တစ်ကြိမ်တည်းနှင့် အားလုံးကိုဖျက်လိုက Keyboard မှ (Ctrl+A) ကိုတွဲနှိပ်ကာ select မှတ်ပါ။ထို့နောက် icon ပေါ်တွင် click နှိပ်ပါက ဖျက်ဖို့ရန် အတည်ပြုချက်တောင်းပါလိမ့်မယ်။ yes တွင် click နှိပ်ပါက Quarantine ထဲရှိသမျှအားလုံးကို ဖျက်ထုတ်သွားပါလိမ့်မယ်။

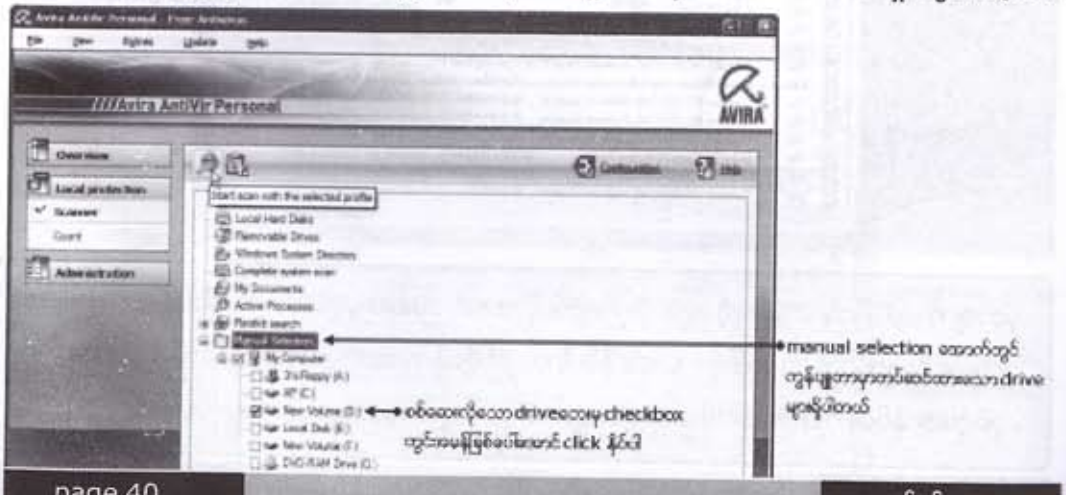
❑drive သို့ folder တစ်ခုခုကိုသာ ရွေးချယ်စစ်ဆေးခြင်း

ရှေ့မှာဖေါ်ပြခဲ့တာက ကွန်ပျူတာတစ်ခုလုံးမှာ တပ်ဆင်ထားသမျှ drive အားလုံးတို့ထဲ ရှိသမျှ နေရာအနှံ့ စစ်ဆေးရှာဖွေရှင်းလင်းပုံများပင်ဖြစ်ပါတယ်။ အဲဒီလိုစစ်ဆေးနည်းက ကောင်းတော့ကောင်းတယ်။ ဒါပေမယ့် အချိန်အများကြီးပေးရတယ်။ ဒါအပြင်လည်းပဲ scan လုပ်နေစဉ်အတွင်း အနှည်းနှင့်အများ ဆိုသလို စက်က လေးနေတတ်တယ်။ ဒါတွေကို အရေးပေါ်လိုအပ်တဲ့ အပိုင်းလိုက်ကိုသာ ရွေးချယ် စစ်ဆေးခြင်းဖြင့် ကျော်လွှားနိုင်ကြပါတယ်။

1) Control center window ထဲက Local protection အောက်မှ scanner ပေါ်တွင် click နှိပ်ပါ။ Local drives ၊ Local hard disks ၊ My Documents အစရှိသဖြင့် အပိုင်းလိုက်လိုသလို ရွေးချယ် စစ်ဆေးနိုင်အောင် အဆင်သင့်ထည့်သွင်းပေးထားသည့် ရွေးစရာ option များကိုတွေ့ရပါမယ်။



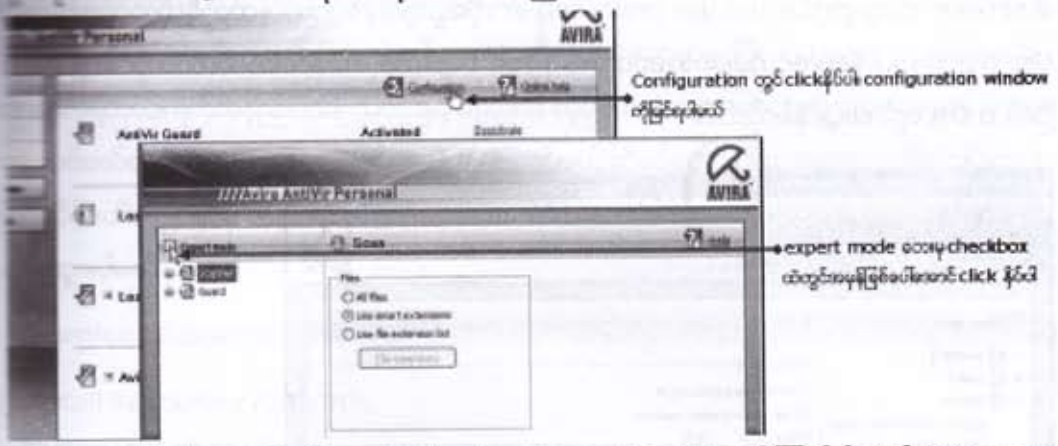
2) drive တစ်ခုချင်းရွေးချယ်စစ်ဆေးရန်အတွက် အလွယ်ကူဆုံးက Manual selection ဖြစ်ပါတယ်။ Manual selection ထဲက My Computer အောက်တွင် ကွန်ပျူတာမှာတပ်ဆင်ထားသမျှ drive များကို တွေ့ရပါမယ်။ စစ်ဆေးလိုသော drive ဘေးမှ checkbox ထဲတွင် အမှန်ခြစ်ပေါ်အောင် click နှိပ်ရွေးပါ။ အဆင်သင့်ဖြစ်ပြီဆိုရင် **Start scan** တွင် click နှိပ်ပါ။ ရှေ့ကအတိုင်းပင် စတင်စစ်ဆေးရှာဖွေပါလိမ့်မယ်။



Antivir Configuration အားပြင်ဆင်ခြင်း

Antivir ၏ Configuration တွင် Antivir Antivirus ၏အလုပ်လုပ်ပုံကိုစိတ်ကြိုက်ပြောင်းလဲသတ်မှတ်နိုင်ပါတယ်။ ဥပမာဆိုရရင် scan လုပ်စဉ်အတွင်း virus တွေ့တယ်ဆိုရင် ပုံမှန်အားဖြင့် alert များပေါ်လာမယ်။ အသုံးပြုသူတွေက delete လုပ်မှာလား၊ quarantine ထဲပို့မှာလား အစရှိသဖြင့် သတ်မှတ်ပေးရတယ်။ အဲဒီလိုမရွေးပေးချင်ရင် virus တွေ့တဲ့အခါဘာလုပ်လိုက်ပါဆိုတာမျိုး ဒီ configuration ထဲမှာထည့်သွင်းပေးထားလို့ရပါတယ်။

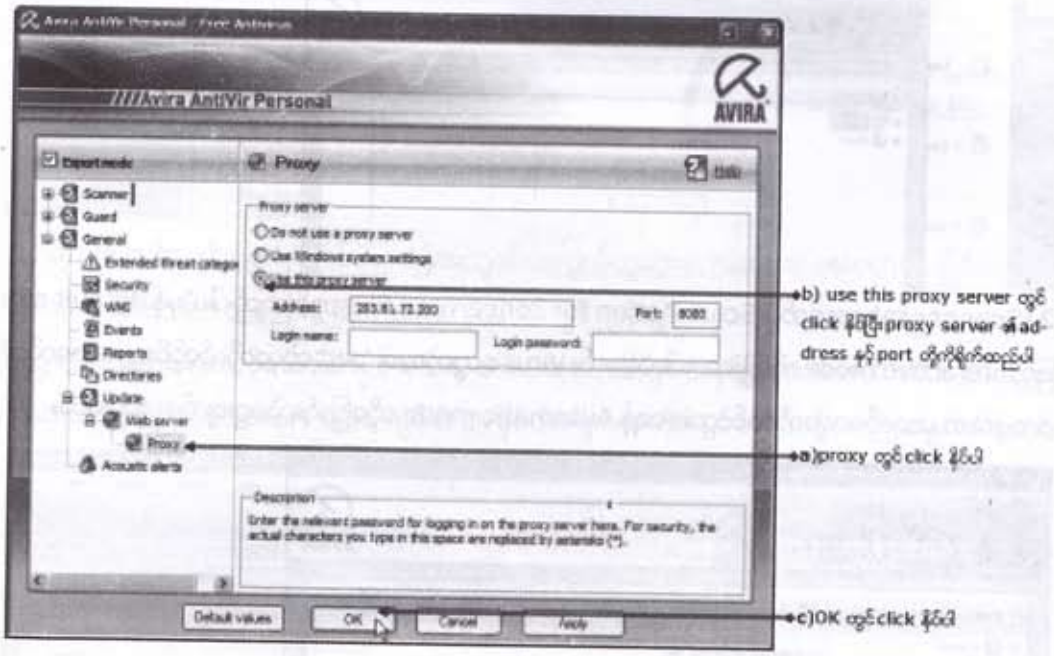
1) Configuration တွင် click နှိပ်လိုက်ပါ။ Scanner နှင့် Guard ဆိုတဲ့ tab နှစ်ခုပါသော configuration window ပွင့်လာပါမည်။ Expert Mode ဘေးရှိ checkbox ထဲတွင်အမှန်ခြစ်ပေါ်အောင် click နှိပ်လိုက်ပါ။ setting tab တစ်ခုထပ်တိုးပေါ်လာပါမည်။



2)Scanner tabအောက်မှ Scan ၊Action for concerning filesတွင် ကြည့်ပါ။ ပုံမှန် default အားဖြင့် Interactive mode ကိုရွေးထားပါလိမ့်မယ်။ Virus တွေ့တဲ့အခါ Alert ထဲမှာကိုယ်တိုင်ရွေးစရာမလိုဘဲ program မှအလိုလျောက်လုပ်သွားစေရန် Automatic mode သို့ပြောင်းလဲရွေးချယ်ပေးရပါမယ်။

နောက်တစ်ခုအရေးကြီးတာက proxy server ရွေးချယ်ထည့်သွင်းခြင်းဖြစ်ပါတယ်။ပုံမှန်အားဖြင့် (Use windows system setting) Internet Explorer မှာထည့်သွင်းထားသော setting အတိုင်းအလုပ်လုပ်မှာဖြစ်သည့်အတွက် မလိုအပ်ပါဘူး။ ဒါပေမယ့်တစ်ချို့ network တွေကနေသုံးတဲ့အခါ proxy server လိပ်စာထည့်သွင်းပေးမှ online update လုပ်လို့ရနိုင်တာမျိုးတွေရှိပါတယ်။ အကယ်၍မလိုအပ်ဘူးဆိုရင်လည်း update လုပ်လို့မရနိုင်တဲ့အခါမျိုးတွေမှာ ပထမဦးဆုံးစစ်သင့်တာက ဒီ proxy နေရာဖြစ်ပါတယ်။

3) General tab အောက်က update ထဲမှာ proxy ဆိုတာရှိပါတယ်။ပုံမှန် default အားဖြင့် windows system setting ဖြစ်ပါတယ်။ proxy ထည့်ဖို့မလိုအပ်ပါက (ဥပမာ - Yatanarpon Teleport ၏service သုံးသူများ) Do not use proxy server ကိုရွေးချယ်နိုင်ပါတယ်။ ထည့်ဖို့လိုအပ်တယ်ဆိုရင် Use this proxy server ကိုရွေးကာ address နှင့် port များထည့်ပေးနိုင်ပါတယ်။ စိတ်တိုင်းကျပြင်ဆင်ပြီးပါက **OK** တွင် click နှိပ်လိုက်ပါ။



ဒီ Configuration ထဲမှာမိမိတို့လိုအပ်ချက်များနှင့်ကိုက်ညီအောင်ပြင်ဆင်အသုံးပြုနိုင်တဲ့အခြားရွေးချယ်စရာ setting များစွာရှိပါသေးတယ်။ဖော်ပြခဲ့တဲ့နှစ်ခုကတော့ Antivirus progrm အများစုတို့မှာပါလေ့ရှိတဲ့အသုံးများသော feature နှစ်ခုဖြစ်ပါတယ်။

Kaspersky Antivirus 2010

ယခုနောက်ဆုံးပေါ် Antivirus program တို့တွင် virus များအပြင် Spyware များ၊ Adware များနှင့် Trojan များကိုပါရှာဖွေဖယ်ရှင်းပေးနိုင်တဲ့အားသာချက်များပိုမိုပါဝင်လာပါတယ်။ အဲဒီလို user များ၏ privacy နှင့် security ပိုင်းကို ပိုမိုကာကွယ်ပေးလာနိုင်သလို သူတို့၏ product ကိုလည်း တရားမဝင် pirate ကူးယူအသုံးပြုခြင်းများမှလည်းကာကွယ်ပေးနိုင်သော feature များကိုပါပိုမိုထည့်သွင်းလာပါတယ်။

အဲဒီ feature ကတော့ install ပြီးသွားတဲ့အခါ ဝယ်ယူစဉ်ကပါလာတဲ့ activate key file ကိုခြင့် activate လုပ်ခြင်းပင်ဖြစ်ပါတယ်။ activate မလုပ်ပဲ သုံးမယ်ဆိုရင်အချို့က ၁၅ရက် (သို့) ၁၀ လအသုံးပြုခွင့်ပေးခြင်းမျိုးတွေလည်းရှိပါတယ်။ မည်သို့ပင်ဖြစ်ဖြစ် ရက်ပြည့်လို့မှ active မလုပ်ရင် ပြန်အတိုင်းဆက်လက်အသုံးပြုလို့ရတော့မည်မဟုတ်ပါ။

အဲဒီတော့အချို့က အင်တာနက်ပေါ်မှာ Crack key တွေရှာဖွေပြီး activate လုပ်ကြတယ်။ ကောတော့ရတယ်။ရက်အနည်းငယ်ကြာတာနဲ့ update လုပ်ရင်း expire ဖြစ်သွားပြီး သုံးမရတော့ပြန်ဘူး။ တရားဝင်ဝယ်ယူ၍ပါလာသည့် key ဖြင့် activate လုပ်မယ် ဆိုရင်တော့ ဒီပြဿနာတွေ ဖြေရှင်းပြီးသား ဖြစ်ပါလိမ့်မယ်။ ဤတွင်မှ Kaspersky Antivirus 2010 အသုံးပြုပုံများကို အောက်ပါခေါင်းစဉ်များဖြင့် ဆက်ပြသွားပါမယ်။

1) Download Kaspersky Installer

2) Install Kaspersky Antivirus

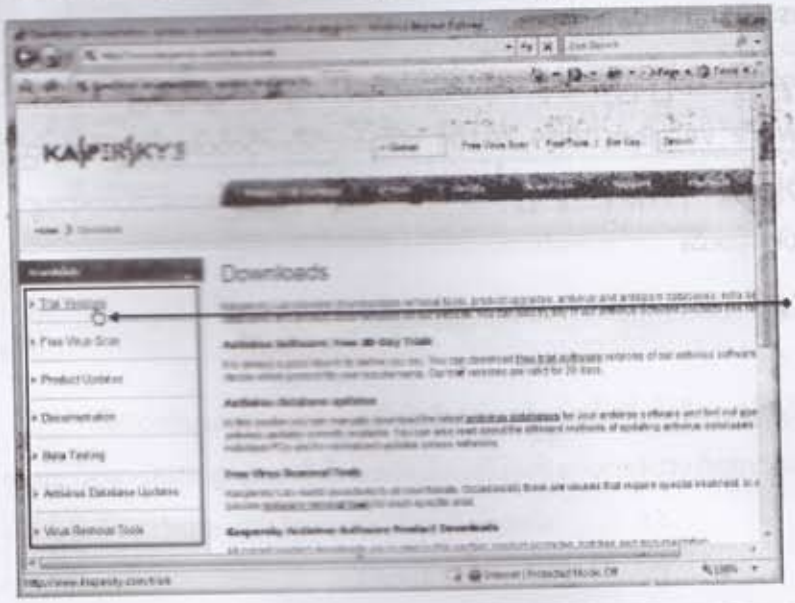
3) Setting Up Kaspersky Antivirus

ဒီနေရာမှာ တင်ကူးကြို့တင်ပြောပြထားလိုတာက download လုပ်ပုံတွေပဲဖြစ်ဖြစ်၊ install လုပ်ပုံတွေ ပဲဖြစ်ဖြစ် software version(2009,2010) ပေါ်မူတည်ပြီး လိုက်ပါလုပ်ဆောင်ရမည့် အဆင့်တွေ၊ GUI လို့ခေါ်တဲ့မြင်ကွင်းပုံသဏ္ဌာန်တွေ ပြောင်းနိုင်ပါတယ်။ သို့သော်လည်း သဘောတရားများမှာတော့ အတူအတူပင်ဖြစ်ပါလိမ့်မယ်။

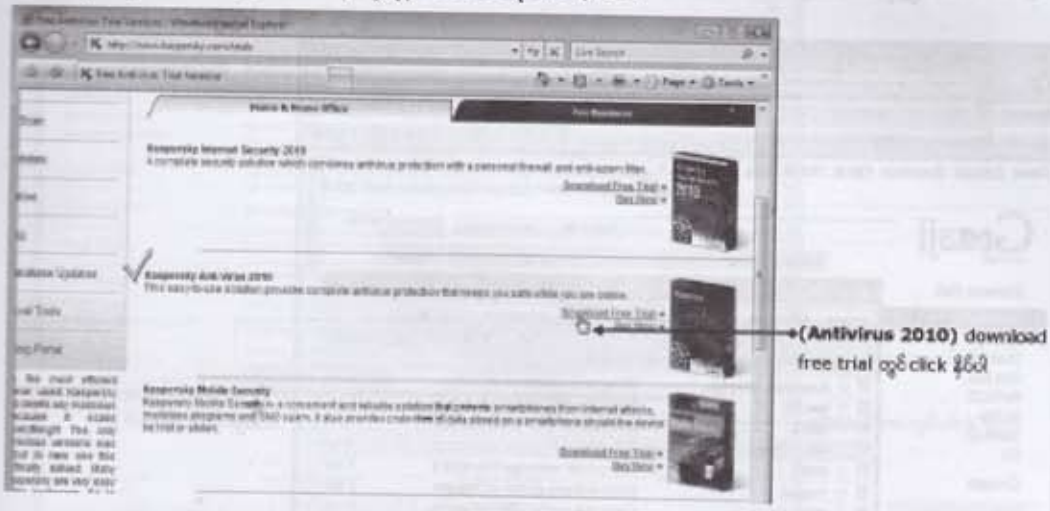
Download Kaspersky Trial Version

1) Kaspersky Antivirus အား download ရယူရန် **www.kaspersky.com** သို့သွားပါ။ ထို့နောက် home page ရှိ **Download** တွင် click နှိပ်လိုက်ပါ။ download sectionသို့ရောက်ပါလိမ့်မယ်။

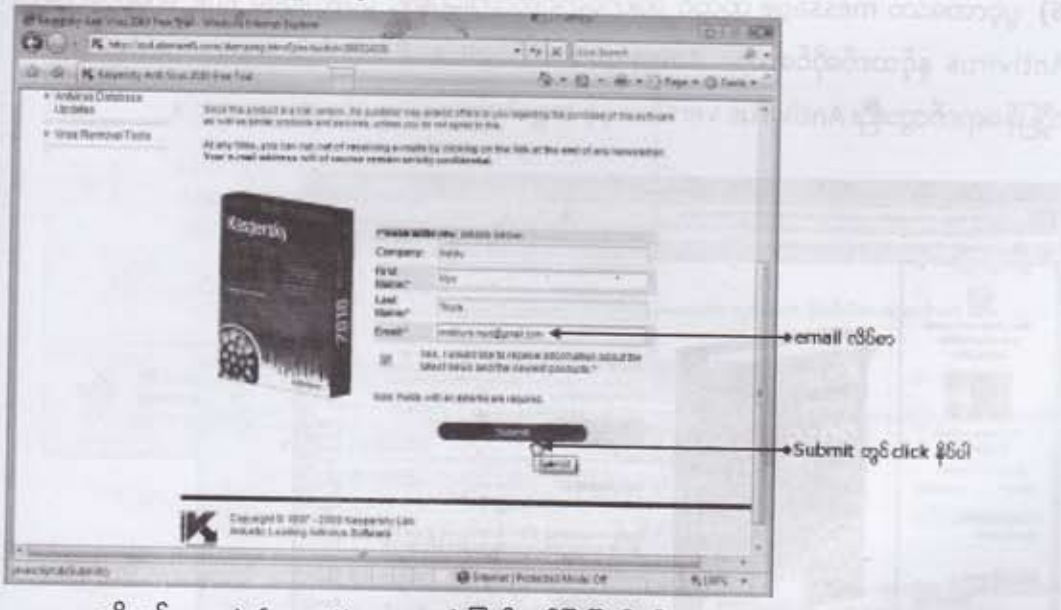
2) ဘယ်ဘက်ခြမ်း download sectionထဲမှ **Trial version** ပေါ်တွင် click နှိပ်လိုက်ပါ။ Antivirus၊ security အစရှိသော Kaspersky မှစမ်းသပ်အသုံးပြုခွင့်ပေးထားသော product များကို တွေ့ရပါမယ်။



3) Product များထဲကမှ မိမိရယူချင်သည့် Antivirus နှင့်ဆိုင်သော **Download free trial** တွင် click နှိပ်လိုက်ပါ။ Register လုပ်ဖို့ရန် တောင်းဆိုပါလိမ့်မယ်။

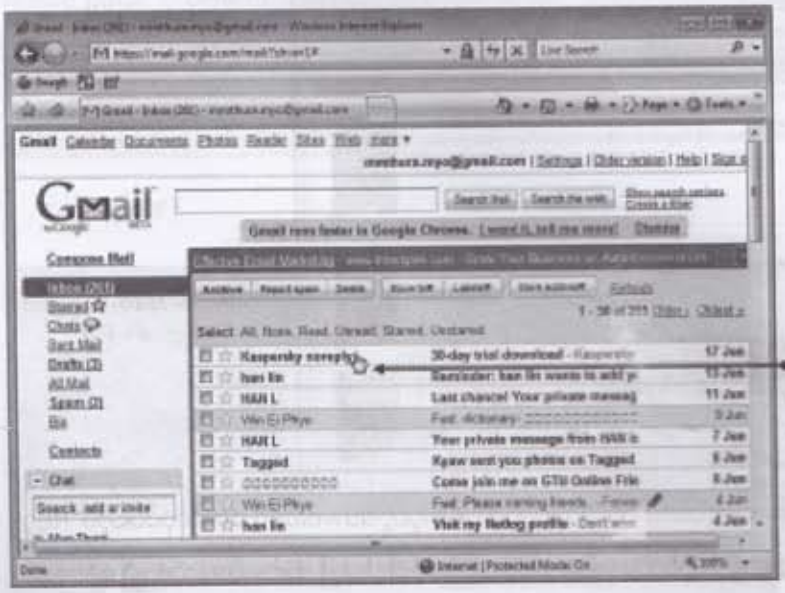


4) Kaspersky သည် အခြား website တိုက်ဘဲသို့လွယ်လွယ်ကူကူ download ပေးမလုပ်ပါဘူး။ Register လုပ်နိုင်းပါတယ်။ Register လုပ်တဲ့နေရာမှာ အရေးကြီးဆုံးက အမှန်တကယ်အသုံးပြု၍ ရနိုင်သော email လိပ်စာတစ်ခုကိုထည့်ပေးရပါမယ်။

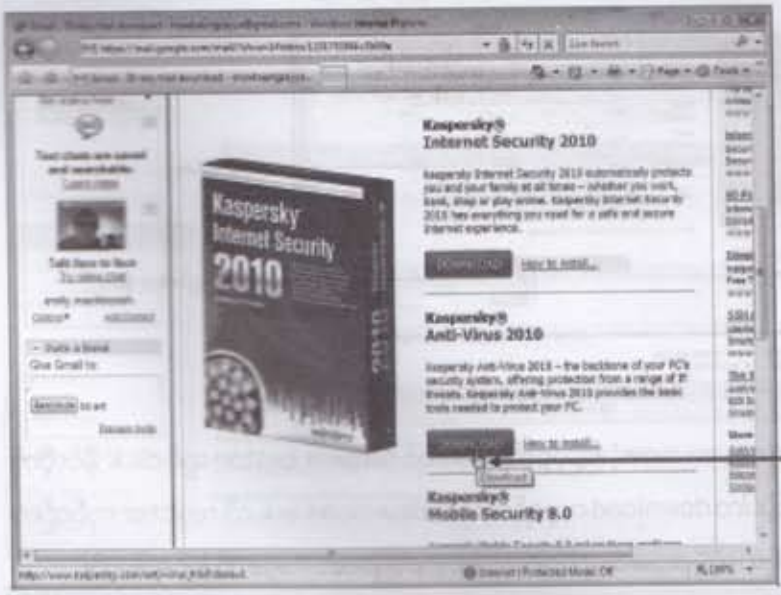


လိုအပ်သော information အားလုံးဖြည့်စွက်ပြီးပြီဆိုရင် **Submit** button တွင် click နှိပ်လိုက်ပါ။ ပြည့်စုံမှန်ကန်စွာဖြည့်စွက်ခဲ့ပါက download ရယူရန်အတွက် download link ကို register လုပ်စဉ်က ဖြည့်စွက်ခဲ့သော email လိပ်စာဆီပို့ထားပေးမည်ဖြစ်ကြောင်း ဖော်ပြသော Page ကို မြင်ရပါမယ်။

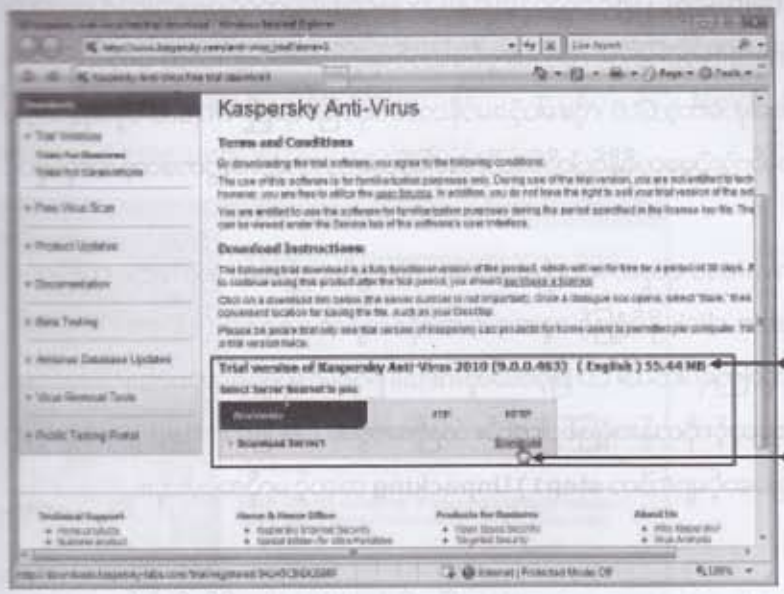
5) ခေတ္တစောင့်ဆိုင်းပြီးမိမိရဲ့email ထဲသို့ဝင်ကြည့်မယ်ဆိုရင် Kasperskyမှပေးပို့ထားသော message အားတွေ့ရပါမယ်။၄င်း messageပေါ်တွင် clickတစ်ချက်နှိပ်ပြီးဖွင့်ဖတ်ရပါမယ်။



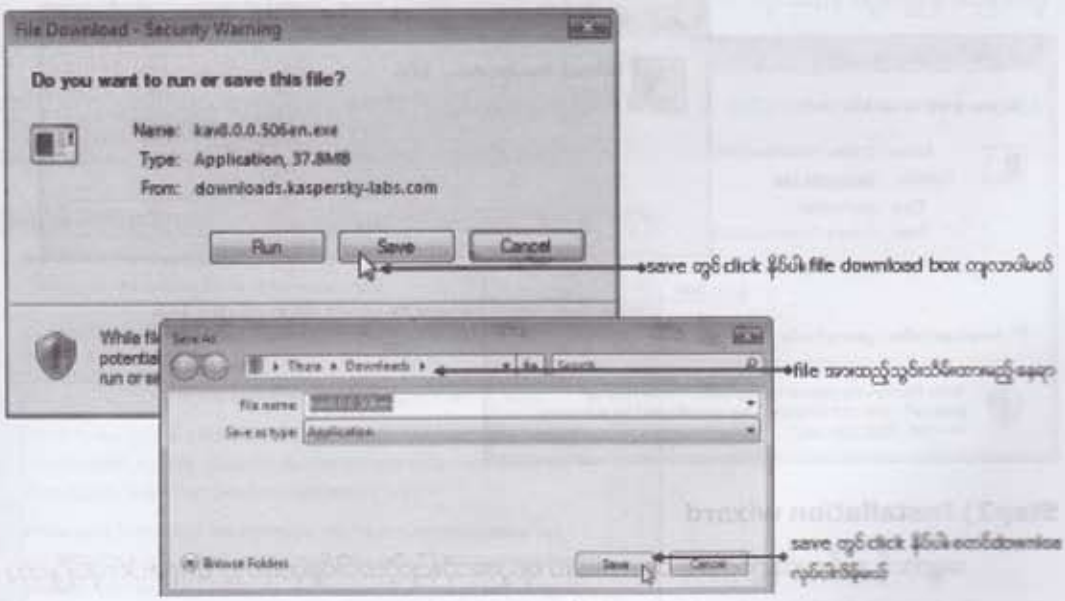
6) ပွင့်လာသော message ထဲတွင် အပြာရောင်စာသားများဖြင့် download link ကိုတွေ့ရပါမယ်။ Antivirus နှင့်သက်ဆိုင်သော download တွင် click နှိပ်လိုက်ပါ။ Kaspersky website သို့ပြန်ရောက်သွားပြီး Antivirus version နှင့် အရွယ်အစား size ကိုတွေ့ကြရပါမယ်။



7)**Download** တွင် click နှိပ်လိုက်ပါ။ download ရယူရန် download dialogbox ကျလာပါလိမ့်မယ်။



8)download dialogbox ထဲရှိ **Save** တွင် click နှိပ်ရယူပြီး မိမိမှတ်မိလွယ်မည့်နေရာတွင်သိမ်းဆည်းထားလိုက်ပါ။



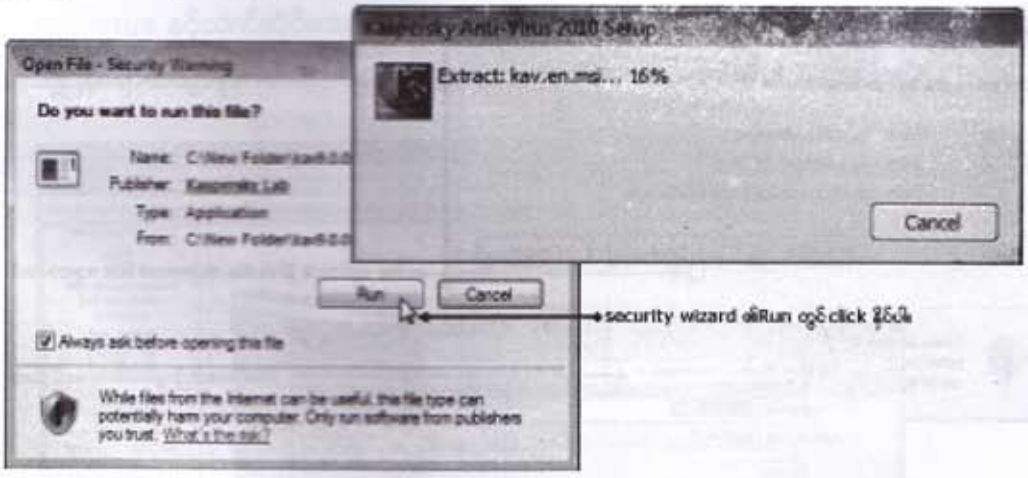
Installing Kaspersky Antivirus

Kaspersky Antivirusကို CD ဖြင့် ဝယ်ယူ installမှာပဲဖြစ်ဖြစ်၊ ရှေ့ကလို download ရယူထားသည့် installer file ဖြင့် installမှာပဲဖြစ်ဖြစ် လိုက်ပါလုပ်ဆောင်ရမည့် အဆင့်များသည် မကွာလှပါဘူး။ သို့သော် version ကွာတဲ့အခါမှာတော့ GUI လို့ခေါ်တဲ့မော်နီတာပေါ်မှာမြင်ရမည့် wizard တို့၏မြင်ကွင်းပုံသဏ္ဌာန်ကတော့အနည်းငယ်ကွဲလွဲမှုတွေရှိနိုင်ပါလိမ့်မယ်။ အခြေခံသဘောတရားတွေကတော့ အတူတူပင်ဖြစ်ပါတယ်။

အင်တာနက်မှ download ရယူထားသည့် installer fileတွင်လည်း self extracter ပါပြီးသားဖြစ်တဲ့အတွက်ကြောင့် double click နှိပ်ချဖြင့် သူဖာသာ အလိုလျောက် unpack(extract) လုပ်ပေးပါတယ်။ ပြီးမှစတင် install လုပ်ကြရပါတယ်။ CD ဖြင့်ဝယ်ယူ install ကြမယ်ဆိုရင်တော့ unpack လုပ်စရာမလိုပါဘူး။ Installation အဆင့်ကိုတန်းစချဖြစ်ပါတယ်။ သည့်အတွက် CD ဖြင့် install ကြမည့်သူတို့အတွက် ယခုဖော်ပြသွားမည့်အဆင့်များထဲက **step1) Unpacking** အဆင့်မလိုအပ်ပါဘူး။

Step1) Unpacking

အင်တာနက်မှ download ရယူထားသော file ပေါ်တွင် double click နှိပ်လိုက်ပါ။ security wizard ပွင့်လာပြီး Run လုပ်မည့်အကြောင်းကိုဖော်ပြထားပါလိမ့်မယ်။ Run ပေါ်တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ အလိုအလျောက် unpack(extract) လုပ်ပါလိမ့်မယ်။



Step2) Installation wizard

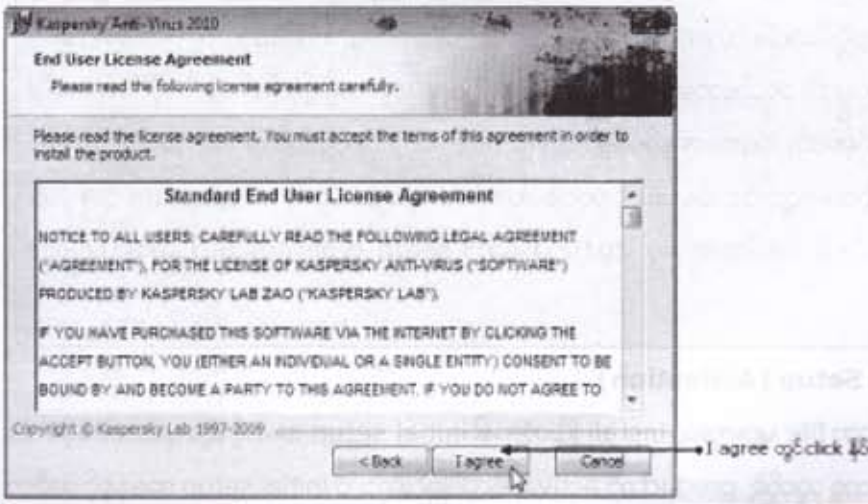
ရှေ့ကလို အင်တာနက်ကနေ download ရယူအသုံးပြုတဲ့အခါမျိုးမှာတော့ unpack လုပ်ပြီးတာနှင့် စတင် Install ဖို့ရန်အဆင်သင့်ဖြစ်နေပါလိမ့်မယ်။ CD ဖြင့် Install လုပ်မည့်သူတွေကတော့ drive ထဲသို့ထည့်လိုက်ပါက Install ဖို့ရန်အလိုအလျောက်ပွင့်လာပါလိမ့်မယ်။ အကယ်၍ အလိုလျောက်မပွင့်ပါက

.exe file ကိုရွာဖွေ double click နိပ်ပါကလည်း Installation wizard ပွင့်လာပြီး စတင် Install လုပ်ဖို့ရန် အဆင်သင့်ဖြစ်ပါလိမ့်မယ်။

ဒီ wizard ထဲမှာရှေ့ဆက်ပြီး install မလုပ်ခင် အခြားဖွင့်ထားသော program များရှိရင် ပိတ်ထားဖို့ရန် သတိပေးပါတယ်။ အခြားprogram တွေပိတ်ပစ်ပြီး **Next** တွင် click တစ်ချက်နှိပ်ပါ။ License Agreement wizard ကျလာပါလိမ့်မည်။

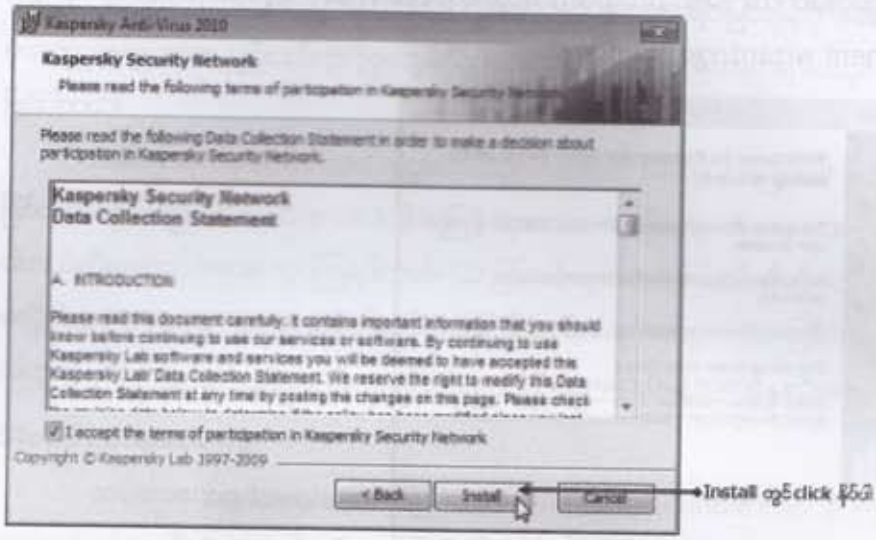
Step3) License Agreement

License Agreement ထဲမှာဆိုရင် အဓိကအားဖြင့် program ကို copy ကူးယူပြီး အခြားသူတို့အား ဖြန့်ဝေခြင်းမလုပ်ပါဘူးဆိုတာကို အာမခံခိုင်းတာမျိုးပါလေ့ရှိပါတယ်။ မည်သည့်နည်းနှင့်မဆို သဘောတူလက်ခံမှသာ ရှေ့ဆက် install လုပ်ခွင့်ရမှာဖြစ်ပါတယ်။ **I agree** button တွင် click တစ်ချက်နှိပ်ပါ။



Step4) Security Network

I accept ဘေးရှိ checkbox တွင်အမှန်ခြစ်ရှိရပါမယ်။မရှိပါက အမှန်ခြစ်ပေါ်အောင် click တစ်ချက်နှိပ်ပါ။ ဒါဆိုရင် install ဖို့ရန်အဆင်သင့်ဖြစ်ပါပြီ။



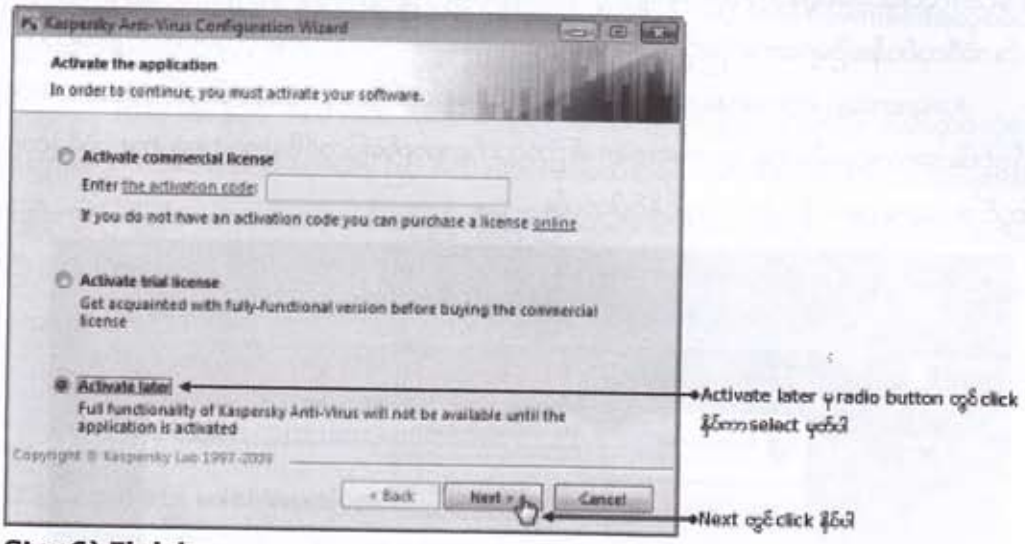
စတင်install ဖို့ရန် Install တွင် clickတစ်ချက်နှိပ်လိုက်ပါ။ destination folder ထဲသို့ file များကို ကူးထည့်ပြီးလိုအပ်သော component များကို install လုပ်ပါလိမ့်မယ်။ပြီးသွားတဲ့အခါ activate လုပ်ဖို့ရန်တောင်းဆိုသော initial setup သို့ရောက်သွားပါလိမ့်မယ်။

မှတ်ချက် - ရှေ့ကထွက်ရှိခဲ့သော version များ(ဥပမာ -Kaspersky 2009)မှာဆိုရင် ယခုလို install မလုပ်ခင် setup type လို့ခေါ်တဲ့ Express(standard) နှင့်customတို့ထဲကတစ်မျိုးမျိုးကို ရွေးချယ်ပေးရလေ့ရှိပါတယ်။ customကိုရွေးချယ်မည်ဆိုပါက program ရဲ့ဘယ်အစိတ်အပိုင်းတွေကို install လုပ်မယ်။ ဘယ်ဟာတွေကိုတော့ installမလုပ်ဘူး အစရှိသဖြင့် ကိုယ်တိုင်စဉ်းစားပြီး ရွေးချယ်ကြရပါလိမ့်မယ်။ Express နှင့်ဆိုရင် customizeမှာကဲ့သို့ကိုယ်တိုင်ရွေးစရာမလိုဘဲလိုအပ်သည်များကို အလိုအလျောက်တင်ပေးသွားမှာဖြစ်ပါတယ်။ အများစုအတွက်ကတော့ Expressနှင့်ပင် လုံလောက်ပါတယ်။ ယခု Kaspersky 2010 မှာတော့ setup type ရွေးရမယ့် အဆင့် ပါမလာတော့ပါဘူး။

Step5) Initial Setup (Activation)

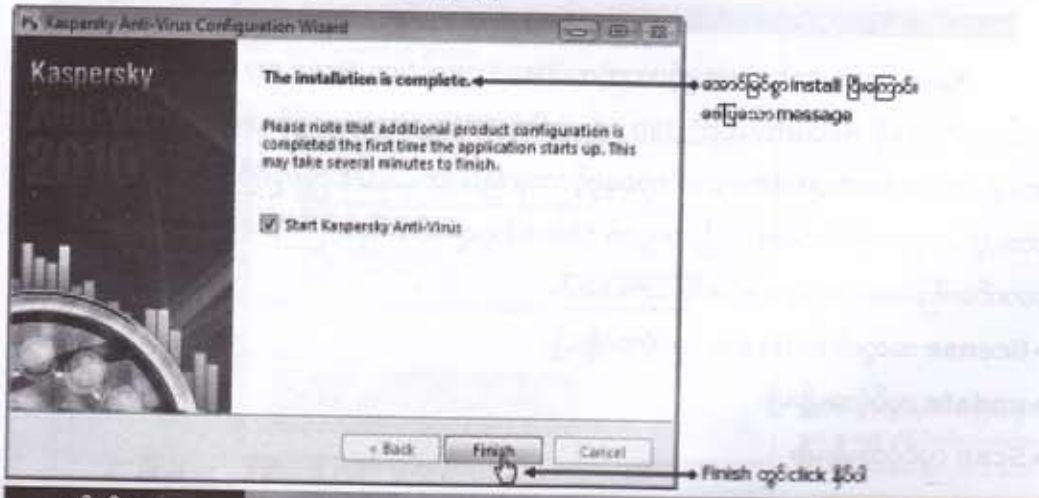
လိုအပ်သော file များကူးယူ install ပြီးတဲ့အခါ initial setup အဆင့်သို့ရောက်ပါလိမ့်မယ်။ Kaspersky ကတော့ သူတို့ရဲ့ productကို activate လုပ်ခြင်းကိုသာ initial setup အနေနှင့် အဓိက

လုပ်ဆောင်ခိုင်းပါတယ်။ရွေးစရာ option သုံးခုပါတဲ့ Activation Wizard ကျလာပါမည်။Option သုံးခုထဲက Activate Online နှင့် Activate trial version တို့ဖြင့် Activateလုပ်ပုံကို နောက်ပိုင်းမှာ ဖော်ပြပါမယ်။ ယခုလောလောဆယ် Activate later ကိုရွေးချယ်ပြီး **Next** တွင် click နှိပ်ရအောင်။ install လုပ်ခြင်း၏နောက်ဆုံးအဆင့်သို့ရောက်ပါလိမ့်မယ်။



Step6) Finish

Kaspersky Antivirus အား အောင်မြင်စွာ install လုပ်ပြီးသွားပြီဖြစ်ကြောင်း အသိပေးသော Wizardကိုတွေ့ရပါမယ်။ **Finish**တွင် clickနှိပ်ကာ install လုပ်ခြင်းအား အဆုံးသတ်နိုင်ပါပြီ။ဒါဆိုရင် Kaspersky အားကွန်ပျူတာမှာ Install လုပ်ပြီး သွားပြီ။ သို့သော် မိမိကွန်ပျူတာကို အပြည့်အဝ ကာကွယ်ပေးနိုင်တဲ့အခြေအနေမှာမရှိသေးပါဘူး Activate လုပ်ခြင်း။ Update လုပ်ခြင်း အစရှိသော လုပ်ငန်း များကို ဆက်လက်လုပ်ဆောင်ကြရပါဦးမယ်။



Setting Up Kaspersky Antivirus

Kaspersky ကို install ပြီးသွားတဲ့အခါ ကွန်ပျူတာကိုကောင်းစွာ အကာကွယ်ပေးနိုင်အောင် ပြင်ဆင်ရပါဦးမယ်။ လိုအပ်သော setting များပြင်ဆင်ထည့်သွင်းကာ activate လုပ်ခြင်း၊ update လုပ်ခြင်း၊ Scan လုပ်ခြင်းအစရှိသော လုပ်ငန်းများကို သက်ဆိုင်ရာ ကဏ္ဍများအလိုက် အပိုင်းများခွဲ၍ ဖော်ပြသွားပါမယ်။ အဲဒီလုပ်ငန်းစဉ်များအားလုံးကို main program window ကနေတစ်ဆင့်လုပ်ဆောင်နိုင်ပါတယ်။

Kaspersky Antivirus အားဖွင့်ရန် desktop ပေါ်တွင်ရှိသော icon ပေါ်တွင် double click နှိပ်၍ဖွင့်ပါ။ အလားတူပင် ကွန်ပျူတာ screen ၏ညာဘက်အောက်ခြေတွင်ရှိသော task bar ထဲရှိ icon ပေါ်တွင် double click နှိပ်၍လည်းဖွင့်နိုင်ပါတယ်။

Kaspersky Antivirus ပွင့်လာတဲ့အခါ My Protection၊ Scan my computer၊ My update center နှင့် Security ဆိုတဲ့ tab လေးခုပါတဲ့ Main window ပွင့်လာပါမယ်။ ပုံမှန် default အားဖြင့် My protection tab အောက်ကနေပွင့်လာမှာဖြစ်ပါတယ်။ tab တစ်ခုချင်းစီရဲ့အောက်မှာ လုပ်နိုင်တာတွေ မတူဘဲကွဲပါတယ်။ သည်အတွက် tab တစ်ခုချင်းစီပေါ်မူတည်ပြီး setup လုပ်ပုံများကို အောက်ဖေါ်ပြပါခေါင်းစဉ်များဖြင့် ဖေါ်ပြသွားပါမယ်။

- ▶**license** အတွက် **activate** လုပ်ပုံအမျိုးမျိုး
- ▶**update** လုပ်ပုံအမျိုးမျိုး
- ▶**Scan** လုပ်ပုံအမျိုးမျိုး

Product Activation (or) Licensing

အခကြေးငွေပေးစရာမလိုပဲ အလကားအသုံးပြုခွင့်ပေးတဲ့ freeware (ဥပမာ- AVG free Edition & Antivir) တွေကလွဲပြီး Antivirus program အများစုတို့ကို Activate လုပ်ရပါတယ်။ Activate လုပ်မှ update လုပ်လို့ရပါတယ်။ Kaspersky ကိုရှေ့ကလို free downloadရယူစမ်းသပ်အသုံးပြုမှာဘဲဖြစ်ဖြစ်၊ဝယ်သုံးမှာဘဲဖြစ်ဖြစ် Activate လုပ်ရပါတယ်။

Trial အနေနှင့် Activate လုပ်မယ်ဆိုရင် တစ်လအသုံးပြုခွင့်ရမှာဖြစ်ပြီး ဝယ်ယူအသုံးပြုသူတွေအတွက်ကတော့ ပါလာတဲ့ Key ဖြင့် Activate လုပ်မယ်ဆိုရင်တစ်နှစ်စာဖြစ်ပါတယ်။ တစ်နှစ်အသုံးပြုပြီးလို့ပဲဖြစ်ဖြစ်၊trialသက်တမ်းတစ်လပြည့်လို့ပဲဖြစ်ဖြစ် ဆက်လက်အသုံးပြုလိုတယ်ဆိုရင် ထပ်မံဝယ်ယူပြီး ပါလာသည့် Key ဖြင့် နောက်တခါ activate ထပ်လုပ်ပေးရပါမယ်။ ဤတွင်မှ activate လုပ်ပုံကို အောက်ဖော်ပြပါခေါင်းစဉ်နှစ်ခုဖြင့် ဖော်ပြသွားပါမယ်။

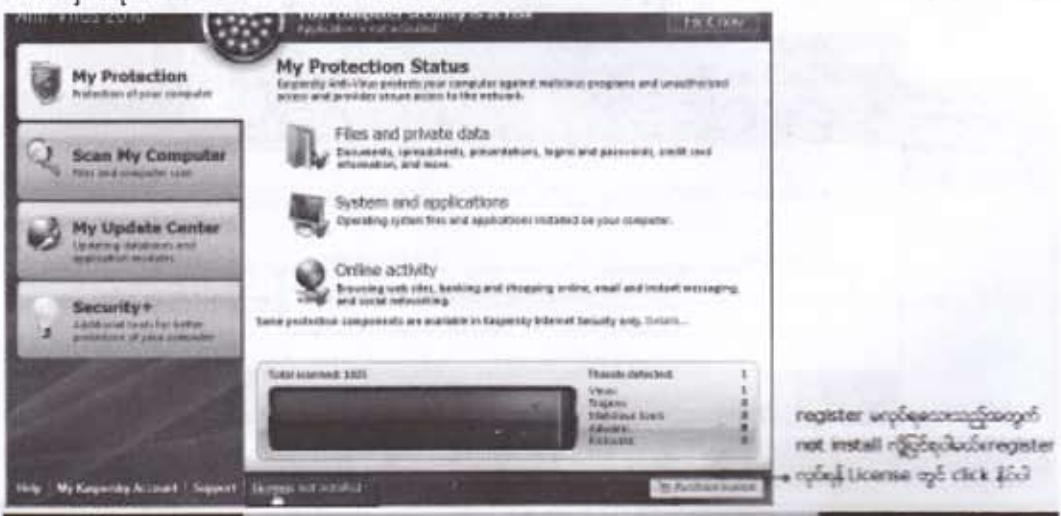
1) Activate trial Version

2) Activate commercial license

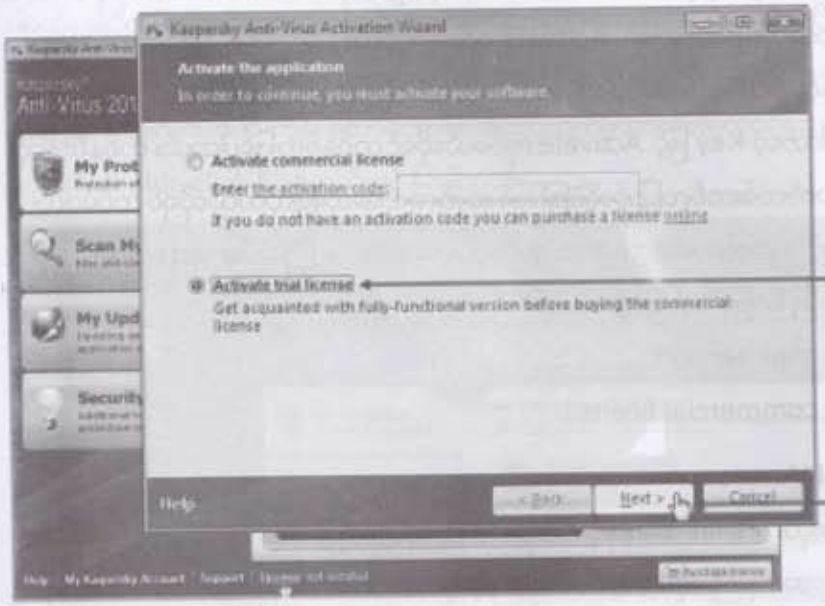
❑1) Activate trial Version

ယခုဖော်ပြသွားမှာက trial အနေနှင့် Activate လုပ်ပုံများပဲဖြစ်ပါတယ်။ trial အနေနှင့် Activate လုပ်ဖို့ရန် အဓိကအရေးကြီးဆုံးက အင်တာနက်နှင့် ချိတ်ဆက်ထားရန်ဖြစ်ပါတယ်။ အင်တာနက်ချိတ်ဆက်မထားဘဲ Activate လုပ်၍မရပါ။

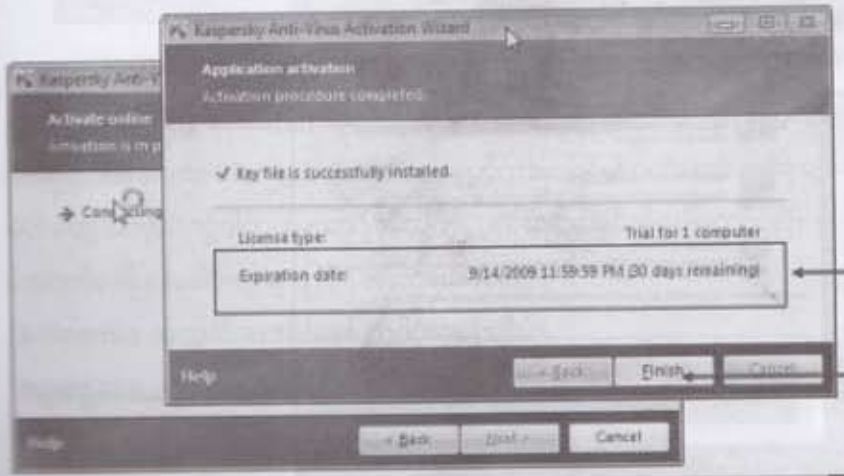
1)Kaspersky main window တွင် License ပတ်သက်သော information ကို မြင်ရပါမယ်။ Activate လုပ်ဖူးခြင်းမရှိသေးပါက License:not installed ဆိုပြီး တွေ့ရပါမယ်။ License တွင် click နှိပ်လိုက်ပါ။



2) License တွင် click နိပ်လိုက်ပါက ရွေးစရာ option နှစ်ခုပါတဲ့ Activation wizard ကျလာပါမည်။ trial အနေနှင့်ပဲဖြစ်ဖြစ်၊ ဝယ်ယူစဉ်ကပါလာတဲ့ key သို့ key file တို့နှင့် activate လုပ်မှာပဲဖြစ်ဖြစ် ဒီနေရာကိုလာပြီး activate လုပ်ကြရပါမယ်။ ယခုတော့ trial အနေနှင့် activate လုပ်မှာဖြစ်သည့်အတွက် Activate trial license ကိုရွေးပြီး **Next** တွင် click နိပ်လိုက်ပါ။



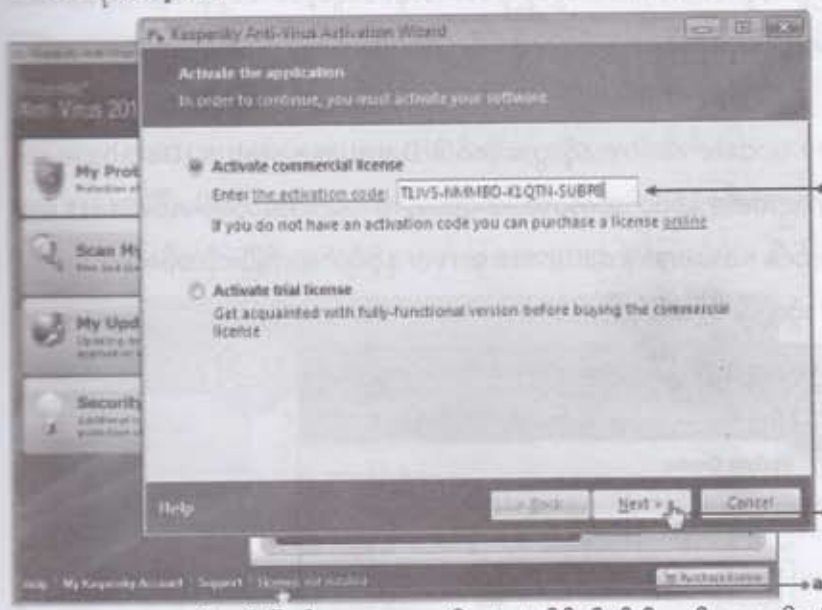
3) အင်တာနက်ပေါ်မှ Kaspersky Activation Server နှင့်ချိတ်ဆက်ပြီး Activate လုပ်ပါလိမ့်မယ်။ activate လုပ်လို့အောင်မြင်တယ်ဆိုရင် license type နှင့် ဘယ်နေ့မှာသက်တမ်းကုန်မလဲဆိုတဲ့ Expiration date တို့ကို ဖော်ပြထားပါမယ်။ **Finish** တွင် click နိပ်လိုက်ပါ။ မူလ main window ရှိ license tab အောက်တွင် license နှင့်ပတ်သက်သော information များကို ဖော်ပြထားပါလိမ့်မယ်။



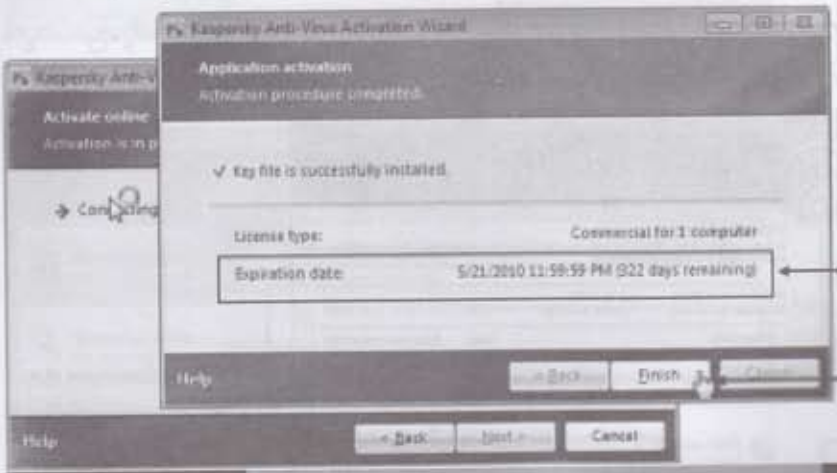
12)Activate Commercial License

Kaspersky ကိုဝယ်ယူတဲ့အခါ ပါလာသည့် Key ဖြင့် activate လုပ်မယ်ဆိုရင် Activate Online ကနေသွားရပါမယ်။ ကွန်ပျူတာသည်အင်တာနက်နှင့်ချိတ်ဆက်ပြီးသားအဆင်သင့်ဖြစ်နေရပါမယ်။

1) Activate Commercial license ကိုရွေးချယ် click နှိပ်လိုက်ပါ။ key များထည့်သွင်းပေးဖို့ရန် တောင်းဆိုပါလိမ့်မယ်။



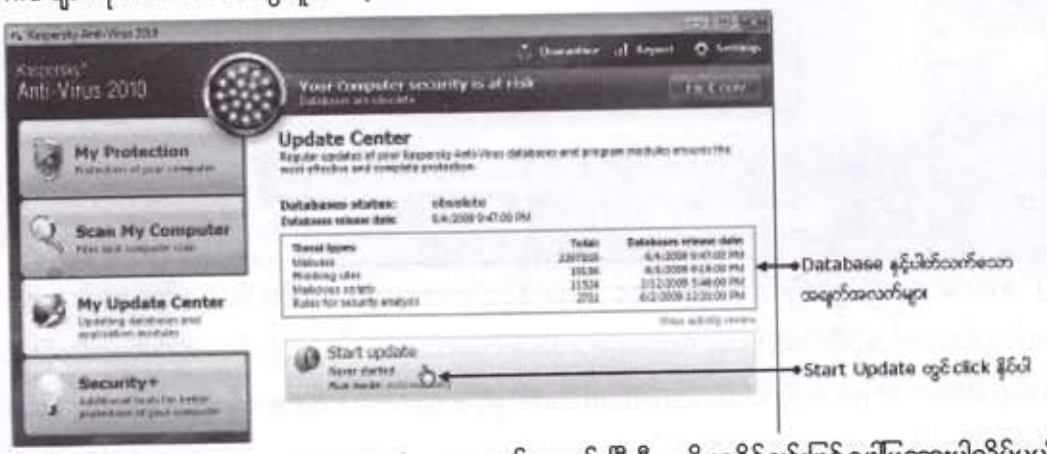
2) Key များထည့်သွင်းပြီးပါက **Next** တွင် click နှိပ်လိုက်ပါ။ အင်တာနက်ပေါ်မှ Kaspersky Activation Server နှင့်ချိတ်ဆက်ကာ Activate လုပ်ပါလိမ့်မယ်။ Activate လုပ်လို့အောင်မြင်တယ်ဆိုရင် licese information နေရာတွင် Activation date နှင့် Expiration date တို့ကိုဖော်ပြထားပါမယ်။ သက်တမ်းမှာ ၁နှစ်စာဖြစ်ပါလိမ့်မယ်။



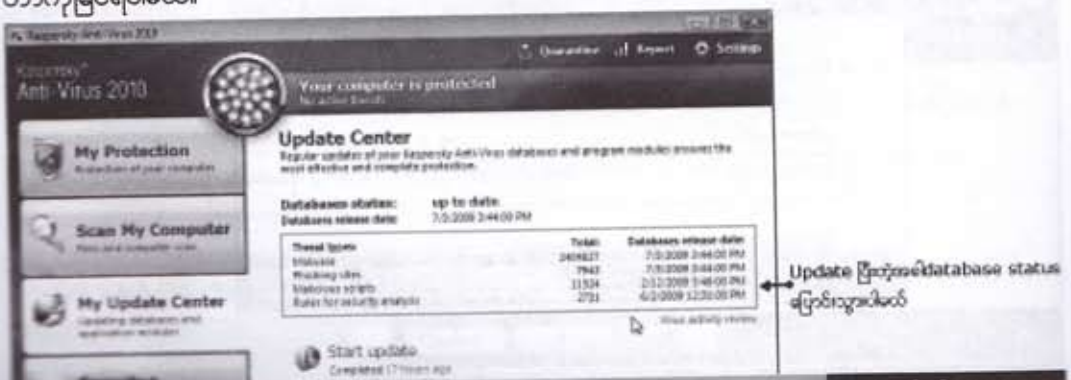
Updating Kaspersky

Activationကိစ္စတွေပြီးခဲ့ပြီဆိုရင်အရေးကြီးဆုံးက virus များရှာဖွေစစ်ဆေးခြင်းမပြုခင် update လုပ်ရန်ပင်ဖြစ်ပါတယ်။Kaspersky 2010 မတိုင်ခင် Kaspersky 2009 ထိကို online နည်းနှင့်ပဲဖြစ်ဖြစ်၊ offline နည်းနှင့်ပဲဖြစ်ဖြစ် update လုပ်လို့ရတယ်။ယခု Kaspersky 2010 အတွက် update file တွေ တင်မထားပေးတော့သည့်အတွက် download ဆွဲယူပြီးအင်တာနက်မရှိတဲ့စက်တွေမှာ offline update လုပ်ခြင်းမျိုးလုပ်လို့မရတော့ပါဘူး။ အင်တာနက်နှင့်တိုက်ရိုက်ချိတ်ဆက်ကာ online update လုပ်ကြရပါတယ်။

1) Kaspersky ၏ My update centre သို့သွားလိုက်ပါ။ Database status ၊ Database release date အစရှိသော update နှင့်ပတ်သက်သော အချက်အလက်များကိုတွေ့ရပါမယ်။ **Start update** တွင် click နှိပ်လိုက်ပါ။ Kaspersky database server နှင့်ချိတ်ဆက်ပြီး လိုအပ်သော update file များကို download ဆွဲယူပါလိမ့်မယ်။



2) update file များအား download ရယူနေစဉ်အတွင်းပြီးစီးမှုကို ရာခိုင်နှုန်းဖြင့် ဖေါ်ပြထားပါလိမ့်မယ်။ အောင်မြင်စွာပြီးစီးသွားတဲ့အခါ Database status နှင့်Database release date တို့ပြောင်းသွားတာကိုမြင်ရပါမယ်။

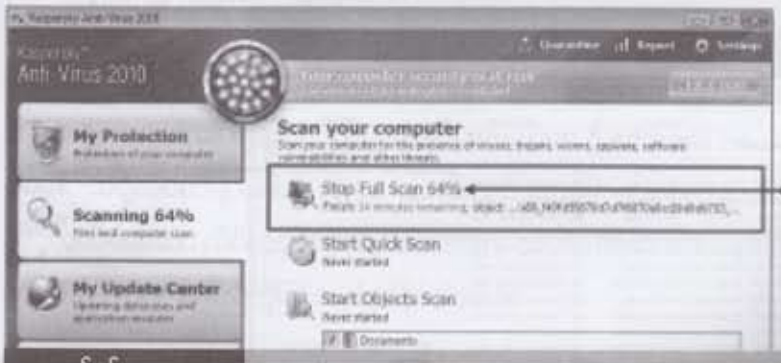


Virus များအားရှာဖွေရှင်းလင်းခြင်း (Scan Your Computer)

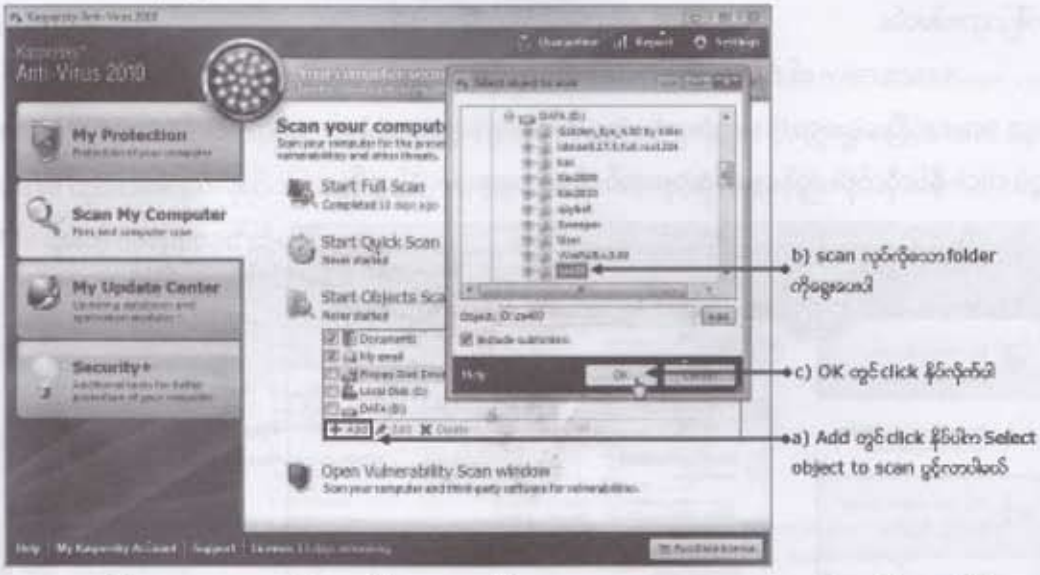
virus definition ကို update လုပ်ခဲ့ပြီးပြီဆိုရင် ကွန်ပျူတာတွင်းမှာ viurs များ၊ trojan များ၊ worm များရှိမရှိရှာဖွေရှင်းလင်းခြင်းလုပ်ငန်းအားဖေါ်ပြပါမယ်။ ရွေးကAntivir မှာကဲ့သို့ပင်အကြမ်းအားဖြင့် ရှာဖွေရှင်းလင်းပုံနှစ်မျိုးရှိတယ်။ "full scan"လို့ခေါ်တဲ့ကွန်ပျူတာတစ်ခုလုံးအနှံ့တပ်ဆင်ထားသမျှ drive အားလုံးထဲမှာရှာဖွေစစ်ဆေးခြင်းနှင့် folder (သို့) drive တစ်ခုခုကိုသာ ရွေးချယ်ပြီး စစ်ဆေးရှာဖွေခြင်း (Object Scan) တို့ဖြစ်ပါတယ်။ယခုကွန်ပျူတာတစ်ခုလုံးအနှံ့နှင့် drive တစ်ခုချင်းစစ်ဆေးရှာဖွေပုံများကို ဖေါ်ပြသွားပါမယ်။

Kaspersky ၏ Scan My Computer သို့သွားလိုက်ပါ။ Full scan ၊Quick Scan ၊Object scan ဆိုပြီးရွေးစရာ task သုံးခုကိုတွေ့ရပါမယ်။ကွန်ပျူတာအနှံ့စစ်ဆေးရှာဖွေရန် **Start full scan** တွင် click နှိပ်လိုက်ပါ။ကွန်ပျူတာအားစတင်စစ်ဆေးရှာဖွေပါလိမ့်မယ်။

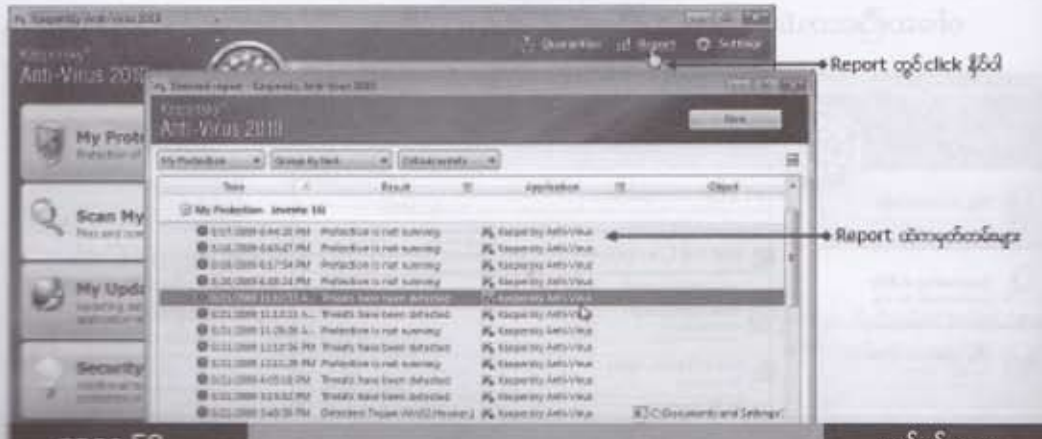
စစ်ဆေးပြီးသော fileအရေအတွက်စုစုပေါင်းပေါ်မူတည်ပြီးစီးမှုရာခိုင်နှုန်းကိုဖေါ်ပြထားပါလိမ့်မယ်။



Scan Your Computer ထဲက Object scan အောက်တွင် Documents ၊My Mail ၊ Drive (C:၊ D:) အစရှိသဖြင့် အပိုင်းလိုက်လိုသလို ရွေးချယ်စစ်ဆေးနိုင်အောင်အဆင်သင့်ထည့်သွင်းပေးထားသည့် task များကိုတွေ့ရပါမယ်။ဒါ့အပြင် folderတစ်ခုချင်းသီးသန့်စစ်ဆေးလိုက Add တွင် click နှိပ်ကာရွေးချယ်ထည့်သွင်းနိုင်ပါတယ်။ စစ်ဆေးလိုသော drive ဘေးမှ checkbox ထဲတွင် ☑ အမှန်ခြစ်ပေါ်အောင် click နှိပ်ရွေးပါ။ အဆင်သင့်ဖြစ်ပြီဆိုရင် **Start scan** တွင် click နှိပ်ပါ။ ရွေကအတိုင်းပင် စတင်စစ်ဆေးရှာဖွေပါလိမ့်မယ်။



စစ်ဆေးရှာဖွေနေစဉ်အတွင်း virus (သို့) unwanted program တစ်ခုခုကိုတွေ့ရှိပါက delete လုပ်ခြင်း၊ quarantineထဲပို့ခြင်းများကို Kaspersky မှအလိုအလျောက်လုပ်ဆောင်သွားမှာဖြစ်ပါတယ်။ ဒါ့အပြင်ဘာတွေတွေ့တယ်၊ ဘယ်လို action ယူဆောင်ရွက်ခဲ့တယ်ဆိုတာတွေကို Report အောက်မှာထည့်သွင်းပေးသွားပါလိမ့်မယ်။



Removal Tools Instruction

မိမိရဲ့ကွန်ပျူတာမှာ virus ကူးစက်နေပြီလို့သံသယရှိတယ်(သို့) ကူးစက်နေပြီဆိုပါက ထို virus များကို အပြန်ဆုံးသုတ်သင်ရှင်းလင်းဖို့လိုပါတယ်။ hard disk မှာ virus များကူးစက်ပြန့်ပွားနေမှုများပြားလာသည်နှင့်အမျှ hard disk ပျက်စီးဖို့အခွင့်အလမ်းပိုမိုများပြားလာပါလိမ့်မယ်။ virus များကိုရှင်းလင်းသော်ရှားပစ်ရန်အတွက် အရေးကြီးဆုံးကတော့ မိမိရဲ့ကွန်ပျူတာမှာရှိတဲ့ Antivirus ရဲ့ Virus definition ဟာ update ဖြစ်ရပါမယ်။ update မဖြစ်ပါက နောက်ဆုံးထုတ် virus definition ကို download ရယူပြီး install လုပ်ရပါမယ်။

Virus definition သည် update ဖြစ်သွားတဲ့အခါမိမိရဲ့ကွန်ပျူတာတစ်ခုလုံးကို စစ်ဆေးကြည့်လိုက်ပါ။ Antivirus program ဟာ virus ကိုရှာဖွေတွေ့ရှိပါက ပထမဦးစွာ virus ကပ်ငြိနေသောဖိုင်ကို clean ဖို့ရန် ကြိုးစားပါလိမ့်မယ်။ အကယ်၍ clean မလုပ်နိုင်တဲ့အခါကျမှသာလျှင် quarantine ထဲသို့ထည့်သွင်းထားပါလိမ့်မယ်။ quarantineဆိုတာက hard disk ပေါ်မှာရှိပြီး virus များနောက်ထပ်ကူးစက်မပြန့်ပွားနိုင်အောင် ထိန်းသိမ်းထားနိုင်သော လုံခြုံစိတ်ချရသော နေရာပဲဖြစ်ပါတယ်။ ဒါကပုံမှန်လုပ်ရိုးလုပ်စဉ်အတိုင်း virusများကိုရှင်းလင်းဖယ်ရှားပုံပဲဖြစ်ပါတယ်။

ဒါပေမယ့် အချို့သော virus များကို ပုံမှန်လုပ်ရိုးလုပ်စဉ်များအတိုင်း ရှင်းလင်းဖယ်ရှား၍ မရနိုင်ပါဘူး။ အချို့သော virus များဟာမိမိရဲ့ Antivirus software ကိုအလုပ်မလုပ်နိုင်အောင် disable လုပ်ထားလိုက်ပါတယ်။ အဲဒီလိုအကြောင်းတစ်ခုခုကြောင့် ပုံမှန်အတိုင်း clean လုပ်လို့မရတဲ့အခါမျိုးမှာသက်ဆိုင်ရာ virus များအလိုက် fix tool များကိုအသုံးပြုပြီး ရှင်းလင်းဖယ်ရှားရပါတယ်။

ဒါကြောင့် fix tool (or) removal tool များကိုအသုံးပြုပြီး virus များကိုရှင်းလင်းဖယ်ရှားဖို့ရန်လိုအပ်ပါက မိမိကွန်ပျူတာတွင်ကူးစက်နေသော virus ရဲ့အမည်ကို သိဖို့လိုပါတယ်။ မိမိရဲ့ကွန်ပျူတာမှာ ဘယ် virus များရှိနေသလဲ ဆိုတာကို အောက်ပါအတိုင်းအကြမ်းမျဉ်း သိနိုင်ပါတယ်။

I) Antivirus program ဖြင့်မိမိရဲ့ကွန်ပျူတာကို စစ်ဆေးကြည့်ပါ။ virus definition သည် update ဖြစ်ပါကမိမိကွန်ပျူတာထဲတွင်ရှိသော virus အားရှာဖွေတွေ့ရှိပြီး ထို virus အမည်ကို ကောင်းကောင်းပြောနိုင်ပါလိမ့်မယ်။

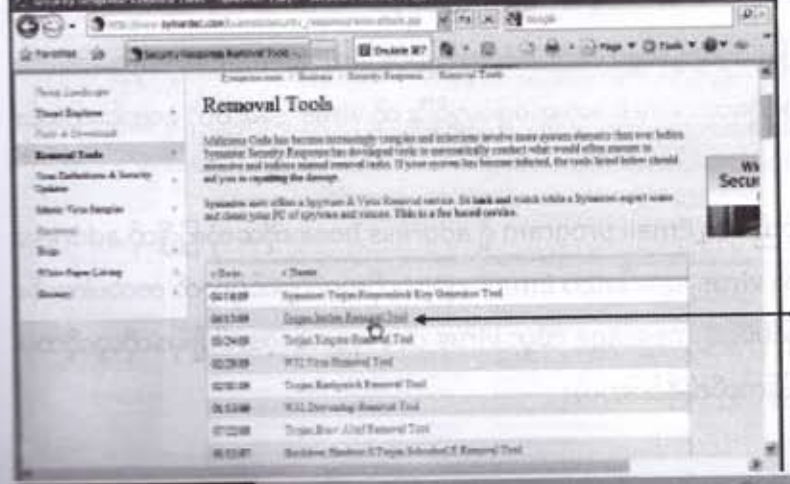
2) အချို့သော virus များသည် မိမိရဲ့ Email program ရှိ address book ကိုအသုံးပြု၍ ထို address book ထဲရှိလိပ်စာများဆီသို့ virus များပါသော Email များအလိုအလျောက်ပို့လွှတ် တတ်ပါတယ်။ ထိုပို့လွှတ်ခံရသော လိပ်စာရှင်မှမိမိရဲ့ message ထဲမှာ virus ပါလာမှန်း သိတဲ့အခါမျိုးမှာ ထိုသူတို့ထံမှ တစ်ဆင့် virus အမည်ကိုပြန်လည်သိနိုင်ပါတယ်။

3) Virus အတော်များများဟာ တစ်ခုနှင့်တစ်ခုမတူညီသော feature များရှိပါတယ်။ ဆိုရရင် မိမိရဲ့ကွန်ပျူတာကို virus ကူးစက်စေခဲ့သော email ရဲ့ title (သို့) attachment file များရဲ့အမည်များပဲဖြစ်ပါတယ်။ feature များကို virus အန္တရာယ်အသိပေးနှင့် သတင်းပေးလေ့ရှိသော website များတွင် ဝင်ရောက်ဖတ်ရှုပါက ထို feature များဟာ ဘယ်လို virus များဖြစ်တယ်ဆိုတာ ခွဲခြားသိနိုင်ပါတယ်။

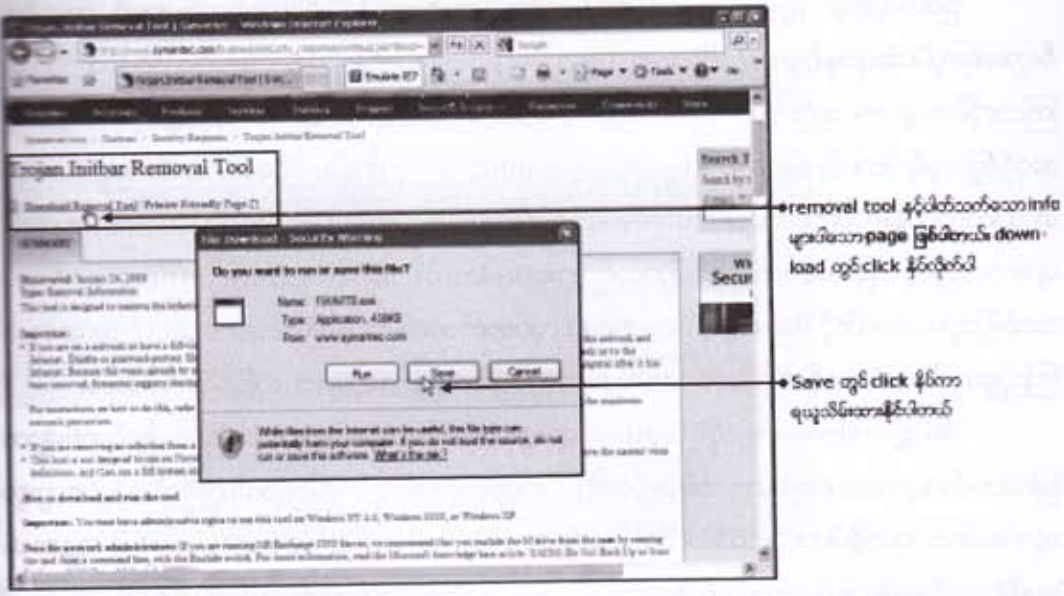
Fix tool များကို antivirus software ရေးသားထုတ်ဝေသော vendor website များမှာ အလွယ်တကူ download ရယူနိုင်ပါတယ်။ သက်ဆိုင်ရာ virus များအလိုက် fix tool များကို free download ရယူနိုင်ရန် တင်ထားပေးလေ့ရှိပါတယ်။ ဆိုရရင် Sobig virus အတွက် **w32.Sobig.worm** ဟူ၍လည်းကောင်း၊ Blaster အတွက် **w32.Blaster.worm** ဟူ၍လည်းကောင်းအစရှိသဖြင့် virus အမျိုးမျိုးတို့အတွက် fix tool အမျိုးမျိုးထဲကမှ မိမိစက်ထဲတွင် ကူးစက်နေသော virus အမည်ပါသည့် fix tool များကိုရွေးချယ် အသုံးပြုရမှာဖြစ်ပါတယ်။ Removal tools တို့အား download ရယူနိုင်သော နေရာအချို့မှာ

- ➲http://www.symantec.com/business/security_response/removaltools.jsp
- ➲http://www.kaspersky.com/removaltools
- ➲http://home.mcafee.com/VirusInfo/VirusRemovalTools.aspx
- ➲http://www.free-av.com/en/products/3/avira_antivir_removal_tool.html
- ➲http://free.avg.com/virus-removal ..... တို့ဖြစ်ပါတယ်။

removal tools ရယူအသုံးပြုပုံများမှာ ရိုးရိုးရှင်းရှင်းပင်ဖြစ်ပါတယ်။ အများအားဖြင့် သုံးလိုတဲ့ tools တစ်ခုခုပေါ်မှာ clickနှိပ်ကာ download ရယူပြီး double click နှိပ် run လိုက်ရုံဖြစ်ပါတယ်။ ဥပမာ အနေနှင့် Symantec (Norton) ကနေ tool တစ်ခုလောက်ဆွဲယူသုံးကြည့်ရအောင်



မိမိစက်ထဲတွင်ကပ်ငြိနေသော virus အမည်ပါသော tools ပေါ်တွင် click တစ်ချက်နှိပ်ပါက ထို virus အားရှင်းထုတ်ဖို့ရန်ညွှန်ကြားချက်ပါသော webpage သို့ရောက်သွားပါမည်။ ထို webpage ၏ အလယ်လောက်တွင် virusအားရှင်းထုတ်ရန် ညွှန်ကြားချက်အဆင့်ဆင့်ကို တွေ့ရပါမည်။ ထိုညွှန်ကြားချက်များသည် virus အမျိုးအစားပေါ်မူတည်ပြီး တစ်ခုနှင့်တစ်ခု အနည်းငယ်လွဲပါတယ်။ (အချို့ tools တွေအတွက် ဘာညွှန်ကြားချက်မှမပါပါဘူး)



download removal tools တွင် click တစ်ချက်နှိပ်ပါက "file download" dialogbox ကျလာပြီးသက်ဆိုင်ရာ "fix tool" file အား download ရယူပါလိမ့်မယ်။ ထို file အားမှတ်မိလွယ်သော folder ဆိုရရင် desktop ပေါ်တွင် save လုပ်ထားလိုက်ပါ။ မိမိ download ရယူခဲ့သော "fix tool" file ကို double click နှိပ်၍ run လိုက်ပါ။ ထို fix tool နှင့်သက်ဆိုင်သော virus ကိုစတင်ရှာဖွေရှင်းလင်းပေးပါလိမ့်မယ်။

တစ်ခါတစ်လေမှာ အချို့သော fix tool များဟာ virus များကို window ရဲ့ normal mode ပေါ်မှာ ရှင်းလင်းဖယ်ရှားခြင်းမပြုနိုင်ပါဘူး။ အဲဒီလို virus များအတွက် သီးခြားညွှန်ကြားချက်များ ပါလာတဲ့အခါမျိုးမှာ ထိုညွှန်ကြား ချက်များအတိုင်း လိုက်ပါဆောင်ရွက်ရမှာဖြစ်ပါတယ်။ဥပမာ - window ရဲ့ safe mode ထဲမှာ fix tool များကို run ခိုင်းတာမျိုးတွေရှိပါတယ်။

ဘယ်လိုနည်းနှင့်ပဲဖြစ်ဖြစ် fix tool အား run ပြီးသွားတဲ့အခါ ကွန်ပျူတာအား restart လုပ်ပါ။ virus ကင်းစင်မှုပိုပြီးသေချာစေရန် ကွန်ပျူတာ reboot လုပ်ပြီး window ပြန်တက်လာတဲ့အခါ fix tool အားနောက်တစ်ကြိမ်ထပ် run လိုက်ပါ။

Introducing Spyware

ကွန်ပျူတာများကိုအသုံးပြုပြီးတခြားသူများ၏ကွန်ပျူတာများပေါ်မှ information များ၊ data များကို ရယူထောက်လှမ်းနိုင်တယ်ဆိုတာ တစ်ခါက ကွန်ပျူတာနယ်မှာ အတွေ့အကြုံများသော Hackers များသာလျှင် စွမ်းဆောင်နိုင်ပါတယ်။ ဒါပေမယ့် ယနေ့ခေတ်မှာတော့ အဲဒီလိုသတင်း အချက်အလက်တွေ ရယူထောက်လှမ်းခြင်းကို လူအများအလွယ်တကူလုပ်ဆောင်နိုင်ပြီးခေတ်ရေစီးလိုပင်ဖြစ်၍နေပါပြီ။

ဥပမာဆိုရရင် ကုမ္ပဏီများဟာ spyware များကိုအသုံးပြုပြီးမိမိတို့ဝန်ထမ်းများကို ကုမ္ပဏီ၏ စီးပွားရေးလုပ်ငန်းများနှင့်မသက်ဆိုင်သော internet၊ email အသုံးပြုမှုများကို စောင့်ကြည့်ထောက်လှမ်းကြသလိုမိဘများကလည်းကလေးများမသင့်လျော်သော internet၊ email အသုံးပြုမှုများမှကာကွယ်ရန် အသုံးပြုလေ့ရှိပါတယ်။ နောက်တစ်မျိုးကတော့ online a[illegible]rtiser လို့ခေါ်တဲ့ အင်တာနက်ပေါ်မှာ ကြော်ငြာလုပ်ငန်းလုပ်ကိုင်သူများဟာ freeware တွေမှာ devel[illegible]ment kit လို့ခေါ်တဲ့ computer code များကိုထည့်သွင်းပြီး အင်တာနက်ပေါ်မှာတင်ထားပေး ပါတယ်။ အဲဒီ freeware program ကို ရယူအသုံးပြုသူဟာ ဘယ်လို file တွေကို download လုပ်တတ်တယ်၊ ဘယ်လို website တွေကို သွားရောက်ကြည့်ရှုတတ်သလဲအစရှိသဖြင့် သူရဲ့ habit များကို ရှာဖွေပြီးရေးသား သူများထံသို့ပြန်ပို့ပေးပါတယ်။

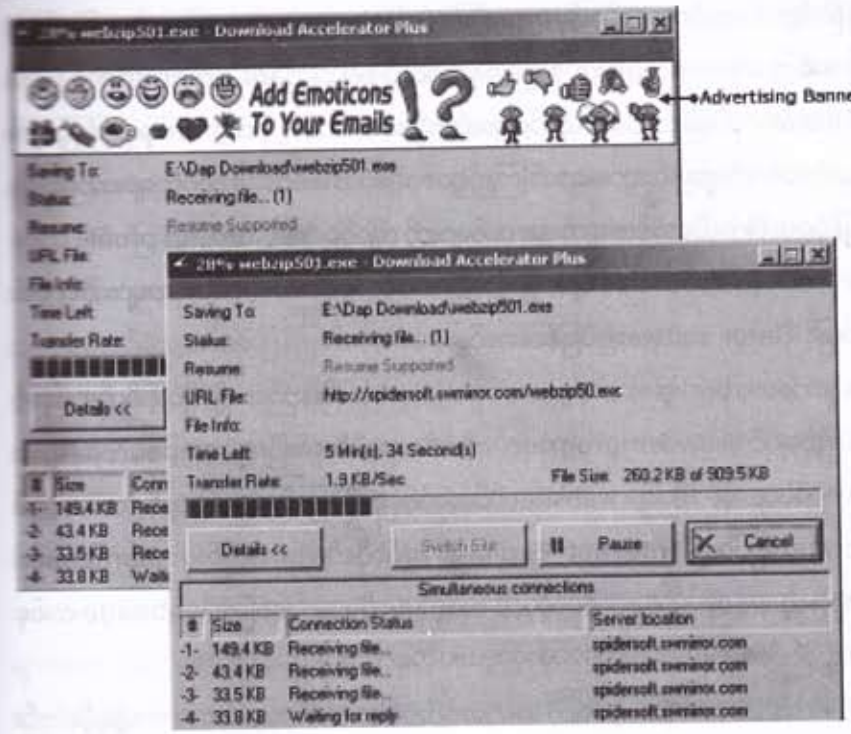
ဒါတွေက spyware တို့ရဲ့ feature များစွာထဲက သိသာထင်ရှားတဲ့အခြေခံ အချက်တစ်ချို့သာ ဖြစ်ပါတယ်။ spyware များဟာ တစ်ခုနှင့်တစ်ခု ပုံသဏ္ဌာန်များ အလုပ်လုပ်ပုံများမတူညီဘဲ ပိုမိုရှုပ်ထွေးစွာ ထွက်ပေါ်လာလျက်ရှိပါတယ်။ အဲဒီအထဲကမှအချို့ဟာ မိမိရဲ့ personal security အထိပါ အန္တရာယ်ပေးနိုင်သလို အချို့ကျပြန်တော့လည်း စိတ်အနှောက်အယှက်ဖြစ်ရုံသက်သက်မျှသာဖြစ်ပါတယ်။

What Is Adware

Spyware အကြောင်းကို မပြောခင်မှာ သူနှင့်ဆက်စပ်နေတဲ့ Adware အကြောင်းကိုပထမဦးစွာပြောဖို့လိုပါလိမ့်မယ်။ adware ရဲ့အဓိပ္ပါယ်ကတော့ advertising supported software ပဲဖြစ်ပါတယ်။ မည်သည့် software အမျိုးအစားမဆို အသုံးပြုနေစဉ်အတွင်း software ရဲ့ interface တစ်နေရာရာမှာကြော်ငြာပါတဲ့ advertising banner ရှိနေတာနှင့် အဲဒီ software ကို Adware လို့ခေါ်ပါတယ်။ Adware အတော်များများဟာ freeware များပဲဖြစ်ပါတယ်။ သူတို့ကို အင်တာနက်ပေါ်ကနေ အခကြေးငွေပေးစရာမလိုဘဲအလွယ်တကူ download ရယူအသုံးပြုနိုင်ပါတယ်။

Adware ရေးသားသည့် company များဟာ ကြော်ငြာထည့်သွင်းလိုသော company များထံမှ အခကြေးငွေများရရှိမှုဖြစ်ပါတယ်။ ကျွန်တော်တို့နောက်မှာဖေါ်ပြမယ့် download လုပ်ရာတွင်အသုံးပြုမယ့် Download Accelerator Plus ဟာလည်း Adware တစ်ခုပဲဖြစ်ပါတယ်။ ဒါကြောင့်သူရဲ့ interface ထဲမှာ advertising banner ကိုတွေ့ရမှာဖြစ်ပါတယ်။

ကြော်ငြာတွေမပါတဲ့ version ကိုသုံးချင်ရင်တော့ အခကြေးငွေပေးပြီးတော့ register လုပ်ရမှာ ဖြစ်ပါတယ်။ အဲဒါဆိုရင်တော့ advertising bannerမပါတော့ဘဲအောက်ပါအတိုင်းတွေ့ရပါတယ်။



What Is Spyware

မည်သည့် software မဆိုအသုံးပြုသူတစ်ဦး၏ သတင်းအချက်အလက်များကို အခြားသော source တစ်ခုဆီသို့ထိုအသုံးပြုသူမသိဘဲ လျှို့ဝှက်စွာပို့လွှတ်ပေးနိုင်သော software ကိုခေါ်ပါတယ်။ တစ်ချို့သော adware များဟာ marketing purpose အတွက် မိမိရဲ့ဘာနေ site ဆီသို့ information များဖြင့်ပြန်ပို့တတ်ကြပါတယ်။ ဒါကြောင့် Adwareများဟာလည်း spywareတစ်မျိုးပါလို့ပြောချင်ရင်လည်း ပြောနိုင်ပါတယ်။

အဲဒီ spyware တွေ မိမိရဲ့စက်ထဲကို ဘယ်လိုရောက်သလဲဆိုတာကို အမျိုးအစားလိုက် ခွဲခြားကြည့်မယ် ဆိုရင်ပထမအမျိုးအစားက spyware ကို တစ်ဦးတစ်ယောက်အတွက် ရည်ရွယ်ပြီး(သို့) သူရဲ့ကွန်ပျူတာတစ်လုံးအတွင်းလျှို့ဝှက်စွာတင်ထားပြီးထိုကွန်ပျူတာအသုံးပြုသူ၏information များ ဆိုရင် password များ၊ file များ၊ chat ပြောဆိုမှုများ၊ email ပို့လွှတ်မှုများစသည်တို့ကို ခိုးကြောင်ခိုးဝှက်ရယူထောက်လှမ်းခြင်းပဲဖြစ်ပါတယ်။ ဆိုရရင် နောက်ပိုင်းမှာဖေါ်ပြမယ့် **Goldeneye** လို software မျိုးပဲဖြစ်ပါတယ်။

Spyware များဝင်ရောက်လာနိုင်တဲ့ နောက်တစ်နည်းကတော့ အင်တာနက်ပေါ်မှ freeware များနှင့် shareware များကို download ရယူအသုံးပြုခြင်းနှင့် website များကို browseလုပ်ကြည့်ခြင်း တို့မှလည်းဝင်ရောက်နိုင်ပါတယ်။ အင်တာနက်ပေါ်မှ freeware (သို့) shareware programတစ်ခုကို install လုပ်တဲ့အခါမှာ အဓိက main program အပြင်နောက်ထပ် secondary programတစ်ခုကိုပါ အသုံးပြုသူမသိစေဘဲ install လုပ်ရန်ထည့်ပေးလိုက်ပါတယ်။ ထို secondary programမှအသုံးပြုသူ၏ ကိုယ်ရေးသတင်းအချက်အလက်များနှင့် သွားရောက်ကြည့်ရှုလေ့ရှိသော website လိပ်စာများအားဌာနေ site သို့လျှို့ဝှက်စွာ ပြန်ပို့ပေး ပါတယ်။ အဲဒီအချက် အလက်များကို သူတို့ရဲ့ serverပေါ်မှာ profile တစ်ခု ဆောက်ပြီး သိမ်းထားလိုက်ပါတယ်။ ထို profile များကိုကြည့်ပြီး သင်စိတ်ဝင်စားမယ့် pop-upများကိုပို့လွှတ် ပါလိမ့်မယ်။ ဥပမာအားဖြင့် Gator softwareပဲဖြစ်ပါတယ်။

နောက်တစ်မျိုးကတော့ browser programကို hijack လုပ်ပြီးနည်းအမျိုးမျိုးနှင့် စိတ်အနှောင့် အယှက်ဖြစ်စေပါတယ်။ ဆိုရရင် browser program ကို ဝင်ရောက်စီးနင်းပြီး homepage နေရာမှာ မိမိထည့်သွင်းထားသောလိပ်စာအစားအခြား website လိပ်စာတစ်ခုခုကိုပြောင်းလဲထည့်သွင်းထားလေ့ရှိပါ တယ်။ ဒါကြောင့် Browser(ဥပမာ - Internet Explorer) ဖွင့်လိုက်တဲ့အခါတိုင်းမှာ homepage အဖြစ်မိမိထည့်သွင်းထားတဲ့ webpage တက်မလာဘဲ ဘာမှန်းမသိသောတစ်ခြား webpage တစ်ခု တက်လာတာမျိုး ကြုံတွေ့နိုင်ပါတယ်။

ဒါ့အပြင် Antivirus 2009 လို့အမည်ရတဲ့ အတုအယောင် antivirus program မျိုးနှင့်လည်း ကြုံရနိုင်ပါသေးတယ်။ အဲဒီ fake program တွေကသူဖာသာ ဝင်ရောက် install နေရာယူပြီး ကွန်ပျူတာ ထဲ မှာ virus များရှာတွေ့ကြောင်းresult များထုတ်ပေးကာ ထိုvirusများရှင်းလင်းဖယ်ရှားရန် programကို ဝယ်ယူခိုင်းပါတော့တယ်။ ဆိုရရင် အမှန်တကယ်စစ်ဆေးတွေ့ရှိခြင်းမဟုတ်ပဲ စစ်ဆေးဟန်ပြုပြီး လိမ်ညာခြင်း သာဖြစ်ပါတယ်။ သူတို့ကိုပုံမှန်လုပ်ရိုးလုပ်စဉ်အတိုင် uninstall လုပ်မရပါဘူး။ သီးခြား removal tools တွေ သုံးပြီးဖြုတ်မှရပါတယ်။

ယခုဖော်ပြခဲ့တာကတော့ အင်တာနက်အသုံးပြုသူအတော်များများကြုံတွေ့နေရနိုင်တဲ့ပြဿနာများ ဖြစ်ပါတယ်။အခြားသောပုံစံများနှင့်လည်းကြုံကောင်းကြုံနိုင်ပါတယ်။တစ်ချို့ကဆိုရင် ဘာမှလျှို့ဝှက်စရာ မရှိဘူး ကြော်ငြာ popupတွေတက်လာရင်ပိတ်ပစ်လိုက်ရုံပဲလို့ပြောကောင်းပြောလာနိုင်ပါတယ်။အပေါ်ယံ ဆင်ခြေကြည့်ရင် ဟုတ်သလိုလိုပါပဲ၊ ဒါပေမယ့်အများကြီးများပါတယ်။ အဲဒီအထဲကမှ အဓိကအရေးကြီးဆုံး နှင့်အကြီးမားဆုံးပြဿနာကတော့ connection speed ကျသွားခြင်းဖြစ်ပါတယ်။

ဖော်ပြခဲ့သလိုခံယူချက်မျိုးရှိပြီး freeware၊ sharewareမျိုးစုံကိုအသုံးပြုရာမှာ ဝါသနာထုံတဲ့ အင်တာနက်အသုံးပြုသူတစ်ဦးကိုတွေ့ခဲ့ပါတယ်။ထိုသူဟာfreeware များကိုမကြာခဏ install လုပ်လိုက်၊ အသုံးမတည့်ဘူးထင်ရင် ပြန်ဖြုတ်လိုက်၊ နောက်တစ်ခါထပ်ပြီး install လုပ်လိုက်နှင့် အသုံးပြုတတ်သလို website အတော်များများကိုလည်း ရှာရှာဖွေဖွေ မွှေနောက်ကြည့်ရှုတတ်တဲ့ အလေ့အကျင့်ရှိပါတယ်။ အထူးသဖြင့်ကတော့ Googleမှာမိမိcrackလုပ်လိုတဲ့software အမည်ရိုက်ထည့်ပြီး gooleကရှာဖွေပေး သမျှcrack siteများသို့သွားရောက်ကြည့်ရှုခြင်း၊ crack file များအား download ရယူခြင်းများလုပ်လေ့ ရှိပါတယ် (ဥပမာ -"download accelerator plus" cracks)။

crack siteတွေဆိုတာက shareware ကို registerလုပ်ဖို့သုံးဖို့ရန်လိုအပ်သော codeနံပါတ် များ၊ key များကိုအခကြေးငွေပေးစရာမလိုဘဲယူသုံးနိုင်အောင် တင်ပေးထားသော siteများပဲဖြစ်ပါတယ်။ ထိုကဲ့သို့သွားရောက်ကြည့်ခြင်းအားဖြင့် spywareများမိမိစက်ထဲပို့မိုရောက်ရှိနိုင်ပါတယ်။အဲဒီလိုသုံးလာပြီး နှစ်လလောက်ကြာလာတဲ့အခါမှာ သူ့ကွန်ပျူတာကနေအင်တာနက်သုံးရတာအလွန်နေးလာပါတယ်။ဆိုရင် webpageတစ်ခုတက်လာဖို့အရင်တုန်းကနဲ့ယှဉ်ရင်အချိန် ၂ဆလောက်ပိုကြာလာသလို disconnect လည်း ခဏခဏဖြစ်လာပါတယ်။ဒါနှင့် spyware များကိုထောက်လှမ်းဖျက်ထုတ်ပေးနိုင်သော Anti-spyware program တစ်ခုကိုသုံးပြီး ကွန်ပျူတာအားစစ်ကြည့်လိုက်တဲ့အခါမှာ spyware/adware ၃၀၀နှုန်းကို ရှာတွေ့ပါတယ်။

အဲဒီ ၃၀လုံး ဒါမှမဟုတ် ၂၀မှ၃၀ ကြားရှိ spyware များဟာ အင်တာနက် အသုံးပြုနေစဉ် တစ်ချိန်တည်း အတွင်းမှာပဲ အသုံးပြုသူမသိစေပဲနောက်ကွယ်မှတိတ်တဆိတ် run နေပြီး information များကိုမိမိတို့ဌာနေရှိရာသို့ ဖြတ်ပို့နေကြပါတယ်။ဒါကြောင့်မိမိဟာ website တခုတည်းကိုသာ browse လုပ်နေသော်လည်း spyware များကြောင့်Internet Explorerအခု၃၀လောက် ဖွင့်ပြီး website အခု ၃၀လောက်ကိုတစ်ပြိုင်တည်း browseလုပ်ကြည့်နေတာနှင့် သွားတူနေပါတယ်။ဒါကြောင့်မိမိရဲ့personal security ကို လျစ်လျူရှုထား နိုင်သော်လည်း အင်တာနက်ကြည့်တဲ့နေရာမှာ အဓိကဖြစ်သော connection speed ကိုကျစေပြီးအတော်လေးစိတ်အနောင့်အယှက်ဖြစ်ရပါတယ်။အလားတူမိမိကဲ့သို့spyware များစွဲကပ်နေသော ကွန်ပျူတာတွေ များများပေါ်လာပါက ISP ရဲ့အင်တာနက် backbone ပေါ်မှာ မလိုလားအပ်သောtraffic loadများလာပြီးအသုံးပြုသူအားလုံး browseလုပ်ရာမှာနေးကွေးသောပြဿနာ

များကိုကြိုတွေ့နိုင်ပါတယ်။

Spywareများမိမိရဲ့ကွန်ပျူတာထဲမှာရှိနိုင်မရှိနိုင်ဆိုတာကိုအောက်ပါအချက်များအတိုင်းယေဘူယျစစ်ဆေးနိုင်ပါတယ်။

1) မိမိကွန်ပျူတာတွင် pop-up windows များမကြာခဏပေါ်လာခြင်း

2) Browser program တွင် မိမိထည့်သွင်းပေးလိုက်သော website သို့မဟုတ်ဘဲ အခြား website တစ်ခုခုသို့လမ်းကြောင်းလွှဲပြောင်းခံရခြင်း

3) Browser program တွင်မိမိinstall မလုပ်သော toolbar အသစ်များပေါ်လာခြင်း

4) Browser programရှိ homepageအပြောင်းခံရခြင်း

5) Browser program ထဲတွင် keyboard မှအချို့သော keyများအသုံးပြု၍မရတော့ခြင်း

6) တစ်ကြိမ်နှင့်တစ်ကြိမ်မတူညီသော windows error messageများကျဘန်းပေါ်နေခြင်း

7) program များဖွင့်ခြင်း၊ fileများsave လုပ်ခြင်းအစရှိသော လုပ်ငန်းများလုပ်ဆောင်ရာတွင်ကွန်ပျူတာ၏စွမ်းဆောင်ရည်ကျဆင်းပြီးရုတ်တရက်နေးကွေးလာခြင်း

အထက်ဖော်ပြပါအချက်များမှတစ်ချက်ချက်နှင့်ကိုက်ညီနေပြီဆိုလျှင် spyware တစ်ခု(သို့မဟုတ်)များစွာသော spywareများဝင်ရောက်ကပ်ငြိနေသည်မှာသေချာသလောက်ပင်ဖြစ်ပါတယ်။Spywareများအန္တရာယ်မှာကွယ်နိုင်ရန်အကြံပေးလိုတာကတော့ email messageများကိုသတိထားဖွင့်ဖတ်ရန်ဖြစ်ပါတယ်။မိမိမသိသော Senderများထဲမှattachmentတွဲပါလာသော messageများကိုအထူးသတိပြုရန်လိုပါတယ်။ထို attachmentများတွင် Virus များပါလာနိုင်သလို Spyware Trojan များလည်းပါလာနိုင်ပါတယ်။

အလားတူပဲအင်တာနက်ပေါ်မှshareware(သို့)freewareများကိုသတိထားပြီးdownloadလုပ်ရန်လိုပါတယ်။သိပ်ပြီးစိုးရိမ်စရာတော့မလိုပါဘူး။freeware အားလုံး(သို့) shareware အားလုံးဟာadware ၊ spywareများမဟုတ်ပါဘူး။ downloadမလုပ်ခင်မှာရယူရန်ကြိုစည်ထားသော programဟာ spywareဟုတ်မဟုတ်ဆိုတာကိုအင်တာနက်ပေါ်မှာရှာဖွေဖတ်ရှုခြင်းဖြင့်လည်းသိရှိနိုင်ပါတယ်။

ယခုဆက်လက်ပြီး spywareတို့အကြောင်းကို အကြမ်းမျဉ်းနားလည်သဘောပေါက်စေရန် နှင့်ဒါမျိုးတွေ့ရှိပါလာဆိုတာကို သိအောင်ရည်ရွယ်ပြီးGoldenEyeလို့ခေါ်သော keylogger တစ်ခုအသုံးပြုပုံများကိုဖော်ပြသွားပါမယ်။ အရေးကြီးတာကသူတစ်ဖက်သားရဲ့ privacyကိုမထိခိုက်အောင် သတိထားဆောင်ကြဉ်ကြဖို့တော့လိုပါလိမ့်မယ်။နောက်ပိုင်းမှာအဲဒီလို keylogger အပါအဝင်spyware များအားရှာဖွေရှင်းလင်းပေးနိုင်သော antispyware program တို့အကြောင်းကိုဆက်လက်ဖော်ပြသွားပါမယ်။

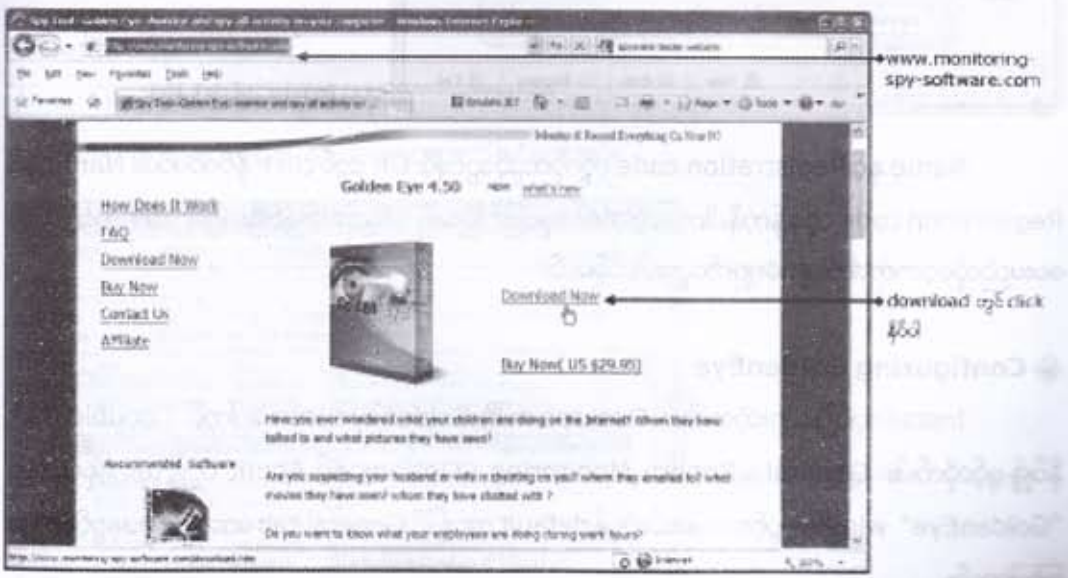
GoldenEye Spyware

ယခု spyware များကို ရှာဖွေရှင်းလင်းဖယ်ရှားပေးနိုင်သော anti-spywareအကြောင်းမဟုတ်ဘဲ spywareတစ်မျိုးဖြစ်တဲ့ GoldenEye အသုံးပြုပုံများကိုဦးစွာဖေါ်ပြလိုက်ပါတယ်။ Goldeneye ဟာ မိမိကလေးငယ်များ၊ ဝန်ထမ်းများ မသင့်လျော်သော အင်တာနက်အသုံးပြုမှုများ ကြိုတင်ကာကွယ် နိုင်ရန် အတွက် ဘယ်ကို email ပို့သလဲ၊ ဘယ် website တွေကိုသွားကြည့်ခဲ့သလဲ၊ chatထဲမှာ ဘာတွေပြောခဲ့သလဲ အစရှိသဖြင့်ကွန်ပျူတာပေါ်မှာ အသုံးပြုမှုများကို စောင့်ကြည့်ထောက် လှမ်းပေးသော keylogger software အမျိုးအစားတစ်ခုပါပဲ။

keylogger ဆိုတာကတော့ကွန်ပျူတာမှာ ဝင်ရောက်အသုံးပြုသွားသော usernameများ၊ password များ၊ folder များ၊ သွားရောက်ကြည့်ရှုခဲ့သော website လိပ်စာများနှင့် screen shot များကို ဖမ်းယူမှတ်သားထားပေးနိုင်သော softwareမျိုးပဲဖြစ်ပါတယ်။ ထို keylogger software များကို keystroke logger ၊ internet monitor ၊ net nanny ၊ spyware survillence tool ဟူ၍ အမျိုးမျိုးခေါ်ဝေါ်သုံးစွဲကြပါတယ်။

Downlod GoldenEye

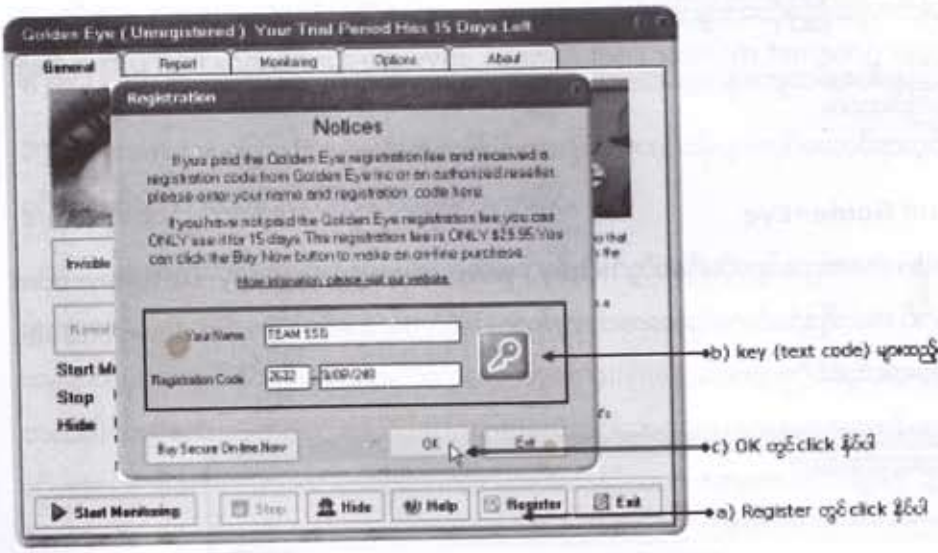
GoldenEyeဖော်ပြာနေ siteကတော့ **http://www.monitoring-spy-software.com** ပဲဖြစ်ပါတယ်။ ထို siteသို့သွားရောက်၍ အလွယ်တကူ download ရယူနိုင်သလို အခြား download site များမှလည်းရှာဖွေရယူနိုင်ကြပါတယ်။



Installing GoldenEye

download ရယူထားသော Goldeneyesetup.exe file အား double click နှိပ်၍ Run လိုက်ပါ။ install မလုပ်ခင်အခြားသော program များကိုပိတ်ထားဖို့ရန် သတိပေးချက်ပါသော "Setup" dialogue box ကျလာပါမည်။ ဤတွင်မှကျန်အဆင့်များကိုပါ Next တွင် click နှိပ်ခြင်းဖြင့် ညွှန်ကြားချက်များအတိုင်းလိုက်ပါ Install လုပ်နိုင်ပါတယ်။

နောက်ဆုံးအဆင့် install ပြီးသွားတဲ့အခါ Golden Eye program window ကိုမြင်ရပါမယ်။ အဲဒီ program window ရဲ့အပေါ် title bar ထဲတွင် register မလုပ်ပါက ၁၅ရက်စမ်းသပ်အသုံးပြုခွင့်ရမည့်အကြောင်းကိုဖေါ်ပြထားပါလိမ့်မယ်။ register လုပ်ရန် Golden Eye window ၏အောက်ခြေတွင်ရှိသော register button တွင် click နှိပ်ပါ။ Registration box ကျလာပါမည်။



Name နှင့် Registration code တို့ကိုထည့်သွင်းပြီး OK တွင် click နှိပ်လိုက်ပါ။ Name နှင့် Registration code တို့မှန်ကန်ပါက register လုပ်ခြင်းပြီးမြောက်အောင်မြင်ပြီး ၁၅ရက်သာအသုံးပြုခွင့်ပေးမည်ဆိုသောစာသားများပျောက်သွားပါလိမ့်မယ်။

Configuring GoldenEye

Install လုပ်ပြီးသွားတဲ့အခါမှာ Desktop ပေါ်ရှိ Goldeneye Icon ပေါ်တွင် double click နှိပ်၍ ဖွင့်လိုက်ပါ။ General ၊ Report၊ Monitoring ၊ Options နှင့် About ဟူ၍ tab ၅ခုပါသော "GoldenEye" window ပွင့်လာပါမယ်။ပုံမှန် default အားဖြင့် General tab အောက်ကနေပွင့်လာမှာဖြစ်ပါတယ်။

❑General

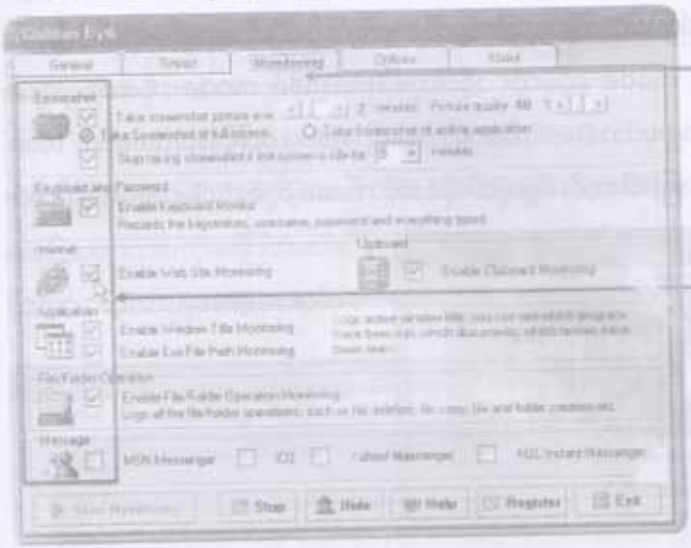
General tab အောက်တွင် Invisible mode နှင့် normal mode ဟူ၍ ၂ မျိုးရှိပါတယ်။ normal mode နှင့်ဆို ရိုးရိုး software များတင်ထားသကဲ့သို့ Goldeneye Icon ကို desktop ပေါ်မှာရော၊ start menu မှာပါမြင်နေရမှာဖြစ်ပါတယ်။သည့်အတွက် တကယ့်ကို ထိထိရောက်ရောက် လျှို့ဝှက်ထောက်လှမ်းချင်ရင်တော့ Normal mode နှင့်မသုံးသင့်ပါဘူး။ Invisible mode ကိုသာရွေးချယ်သင့်ပါတယ်။ Invisible mode ကိုရွေးမှသာ Desktop နှင့် Start menu ပေါ်ရှိ Goldeneye Icon များကို အခြားအသုံးပြုသူများမမြင်ရမှာဖြစ်ပါတယ်။ ရွေးချယ်လိုသော mode တွင် click တစ်ချက်နှိပ်ပါ။

❑Report

Report tab ထဲမှာတော့ Goldeneye မှထောက်လှမ်းထားသော Screen shots များ၊ website လိပ်စာများ၊ chat messageများကိုမြင်ရပါမယ်။

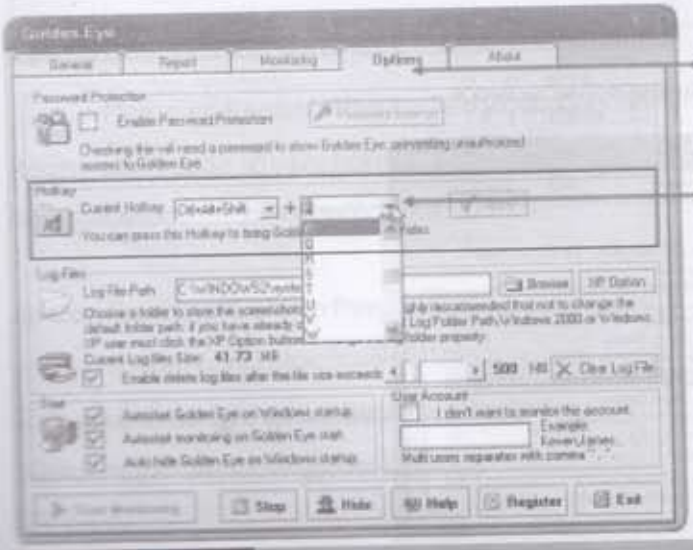
❑Monitoring

Monitoring tabထဲတွင်ထောက်လှမ်းလိုသော record များကိုလိုသလိုမိမိစိတ်ကြိုက် ရွေးချယ်ပေးနိုင်ပါတယ်။မရချင်တဲ့အကြောင်းအရာတို့ဘေးမှ checkbox ကိုအမှန်ခြစ်မရှိအောင်လုပ်ပေးရပါမယ်။



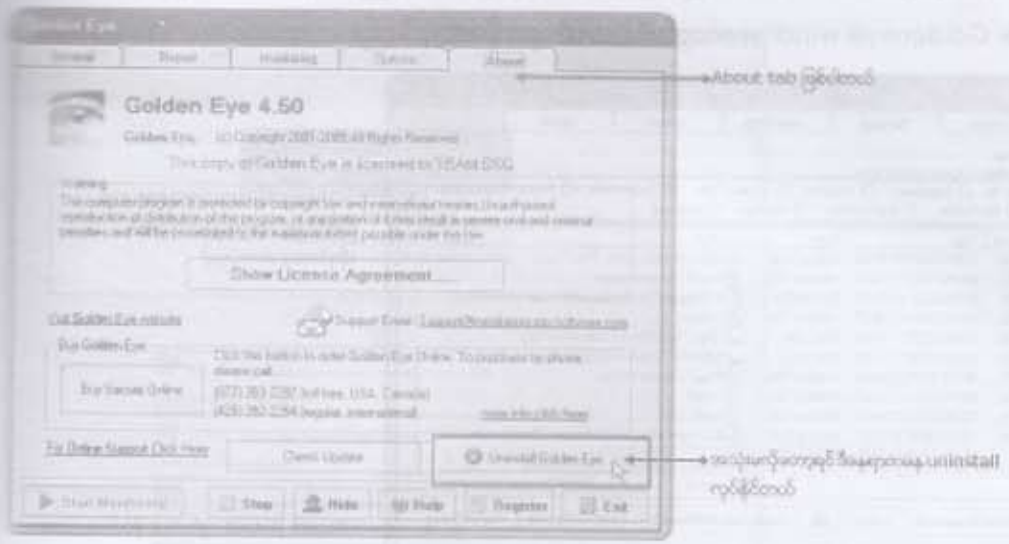
❑Options

Goldeneyeကိုဖွင့်ချင်ရင်hotkeyကိုနှိပ်ပြီးမှပြန်ဖွင့်လို့ရပါတယ်။Goldeneyeရဲ့hotkey ကတော့ Ctrl+Alt+Shift+P ပါဖြစ်ပါတယ်။ အဲဒီ keyကိုမသုံးချင်ဘူးမိမိစိတ်ကြိုက် keyကိုပြောင်းသုံးချင်တယ်ဆိုရင် ဒီtabထဲမှာပြောင်းလို့ရပါတယ်။ဒါပေမယ့်တစ်ခုသတိထားရမှာကတော့မိမိပြောင်းသုံးတဲ့ hotkey ကိုမှတ်မိဖို့လိုပါတယ်။



About

Software version (ဥပမာပုံအရ - 4.50)အပါအဝင် GoldenEye နှင့်ပါတ်သက်သော info ကိုတွေ့ရပါမယ်။ အသုံးမလိုတော့လို့ uninstall လုပ်ချင်ရင်ဒီ About tab ထဲကနေ လုပ်နိုင်ပါတယ်။

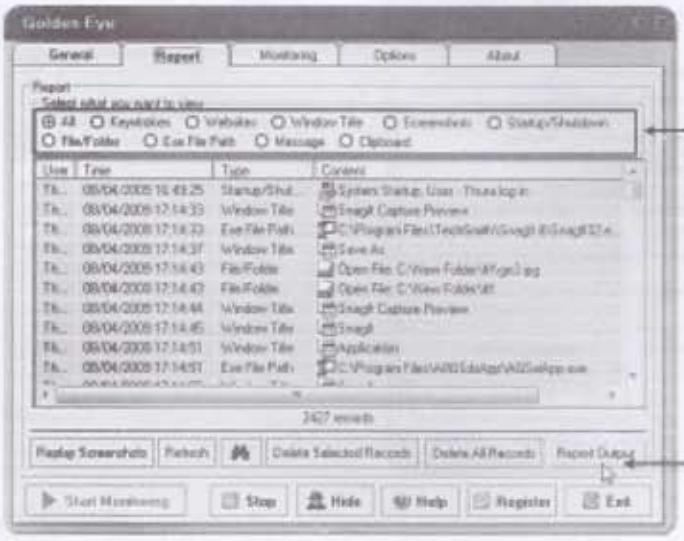


❑ Start GoldenEye

Goldeneye ကိုမိမိစိတ်ကြိုက်ပြင်ဆင်ပြီးသွားတဲ့အခါမှာ စတင်အသုံးပြုနိုင်ရန် **Start Monitoring** တွင် click တစ်ချက်နှိပ်ပါ။ထို့နောက် **Hide** button တွင် click တစ်ချက်နှိပ်ပါက "GoldenEye" window သည် desktop ပေါ်မှပျောက်သွားပြီးနောက်ကွယ်မှ လျှို့ဝှက်စွာစတင်ထောက်လှမ်းပါတော့မယ်။

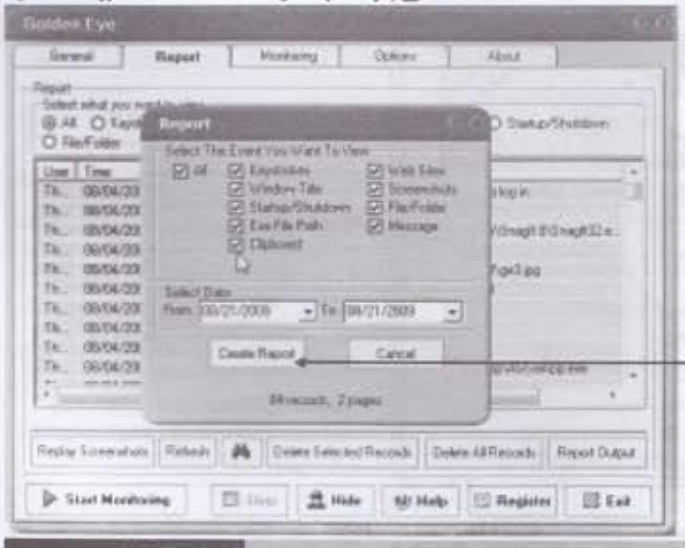
Checking the Records

1) မိမိရဲ့ကွန်ပျူတာပေါ်မှာ ဘာတွေကိုဘယ်လိုဝင်ရောက်အသုံးပြုသွားသလဲဆိုတာကို ပြန်ကြည့်ဖို့ရန် hotkey (ctrl+alt+shift+P) ကိုနှိပ်ပါ။ GoldenEyeပွင့်လာပါမည်။ Report tab တွင် click တစ်ချက် နှိပ်ပါ။ Goldeneye window ထဲတွင် Record များကိုတွေ့ရပါမည်။

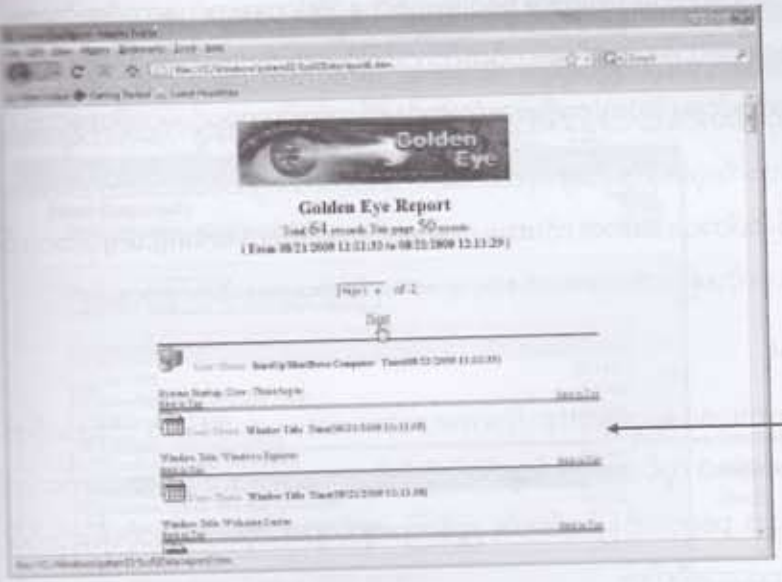


မှတ်ချက် - Invisible modeကိုသာသုံးထားမယ်ဆိုရင် desktopနှင့် start menuတို့ပေါ်မှာမမြင်ရ အောင်ဖျောက်ထားမှာဖြစ်သည့်အတွက် hotkey မသိရင်ပြန်ဖွင့်ကြည့်ဖို့ရန် မဖြစ်နိုင်တော့ပါဘူး။

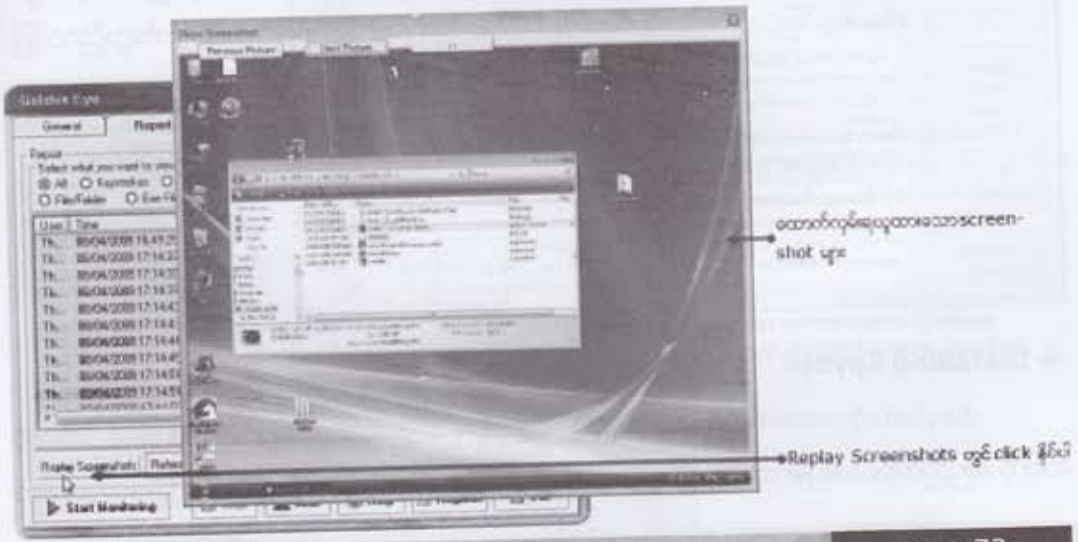
2) Report Outputတွင် click တစ်ချက်နှိပ်ပါ။ Report box ကျလာပါမည်။ ပြန်ကြည့်လိုသော Record များဘေးရှိ check box များကို အမှန်ခြစ်ပေါ်လာအောင် select လုပ်ပေးပါ။



3) **Create Report** button တွင် click တစ်ချက်နှိပ်ပါ။ Browser program ပွင့်လာပြီးထိုကွန်ပျူတာ ကြည့်ခဲ့သော folder များ၊ browseလုပ်သွားခဲ့သော website များ၊ Keyboard မှရိုက်သွားသော စာသားများနှင့် screen shot များကိုအချိန်နှင့်တကွဖော်ပြပါလိမ့်မယ်။



5) Screenshot များကိုသာသီးသန့်ကြည့်လိုပါက **Replay screen shot** တွင် click တစ်ချက်နှိပ်ပါ။ "show screen shots" window ပွင့်လာပြီး screen shot များကိုသာ သီးသန့် window တစ်ခုဖြင့် မြင်ရပါမည်။

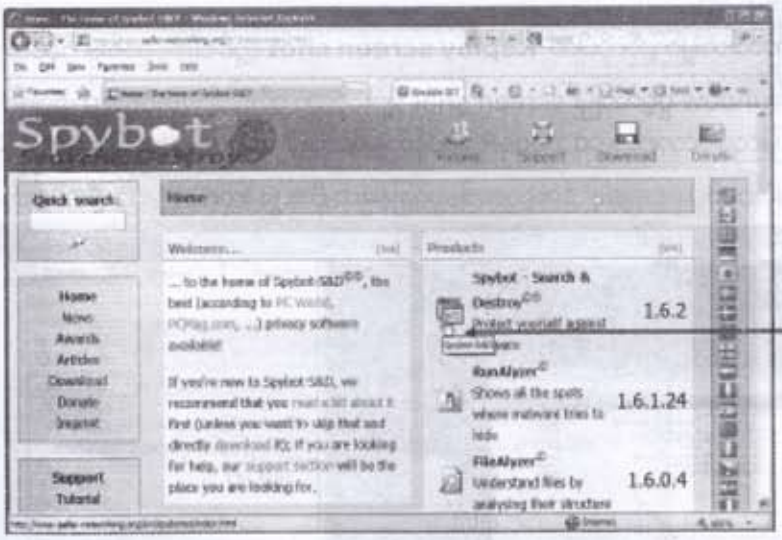


Spybot Antispyware

Spybot Antispyware သည် windows အသုံးပြုသူများကို spyware များနှင့်တခြားမလိုလား အပ်သော software များ၏နောက်ယှက်ခြင်းများမှ ကာကွယ်တားဆီးပေးနိုင်သော software program တစ်ခုပင်ဖြစ်ပါတယ်။ ဆိုရရင် spyware များကြောင့် မိမိကွန်ပျူတာ၏စွမ်းဆောင်နိုင်မှု ကိုကျဆင်းစေခြင်း၊ pop-up များကြောင့်စိတ်အနှောင့်အယှက်ဖြစ်ရခြင်း၊ Browser program တွင်သတ်မှတ်သည့်သွင်းထားသော settingများကို မိမိမသိအောင်ပြုပြင်ပြောင်းလဲခြင်း၊ မိမိရဲ့ကိုယ်ရေး အချက်အလက်များအား တိတ်တဆိတ်ဝင်ရောက်ထောက်လှမ်းရယူခြင်းများမှ ထိထိရောက်ရောက်ကာကွယ်ပေးနိုင်သော antispy ware program တစ်ခုပင်ဖြစ်ပါတယ်။ spybot ကို **http://www.safer-networking.org** မှအလွယ်တကူ download ရယူနိုင်သလိုအခြား download site များမှလည်းရှာဖွေရယူနိုင်ကြပါတယ်။

Download Spybot

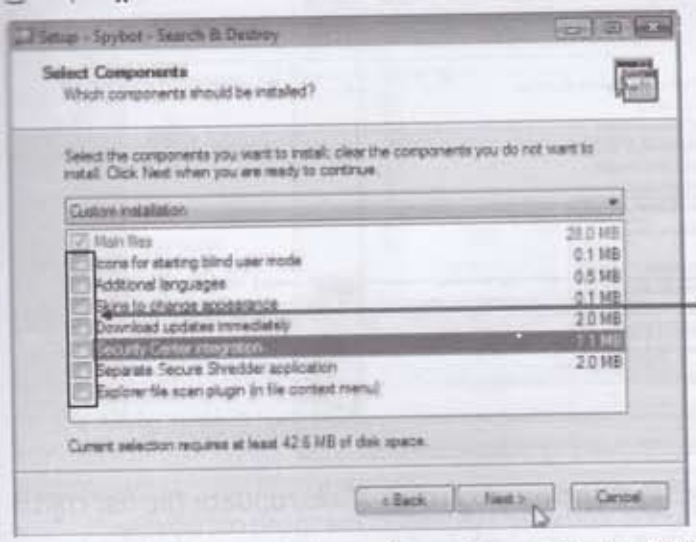
Spybot အား download ရယူရန် http://www.safer-networking.org သို့သွားလိုက်ပါ။ homepage ရှိ **Spybot-S&D** တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ Antispyware နှင့်ပတ်သက်သော information များပါဝင်သော page ကို မြင်ရပါမယ်။ ညွှန်ကြားချက်များအတိုင်း တစ်ဆင့်ချင်းလိုက်ပါလုပ်ဆောင်၍ download ရယူထားလိုက်ပါ။



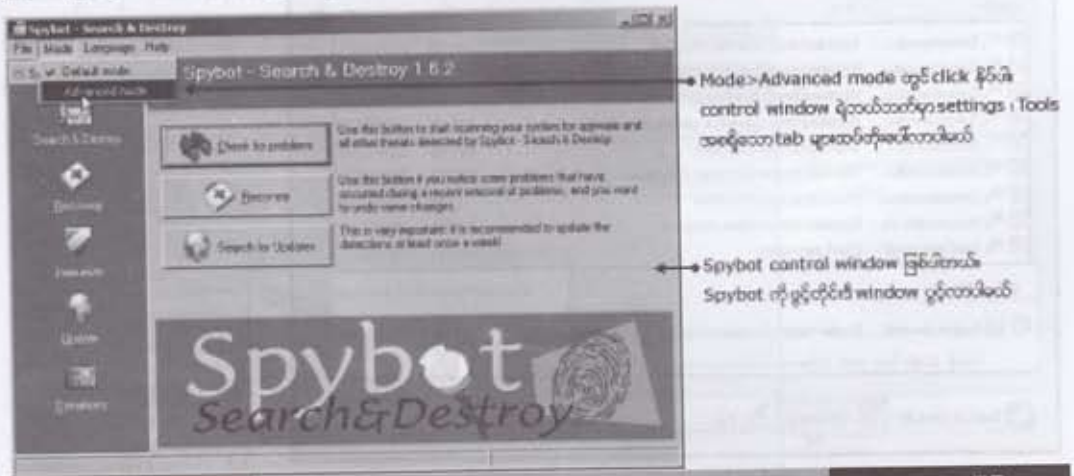
Installing Spybot

Spybotကို installလုပ်ရမည့်အဆင့်များသည် ရိုးရှင်းလွယ်ကူတဲ့အတွက် installလုပ်ပုံအဆင့်ဆင့်ကို အပြည့်အစုံမဖေါ်ပြတော့ပါဘူး။ Component အချို့ကိုပါပေါင်းစပ် install တဲ့နေရာမှာတော့ အခက်

အခဲ့ပြီးနိုင်လိမ့်မည်ယူဆသည့်အတွက် ဖေါ်ပြလိုပါတယ်။ ပုံမှန်အတိုင်း install လုပ်သွားတဲ့အခါ **selected components** အဆင့်သို့ရောက်ပါမယ်။ ထိုအဆင့်တွင် definition update အပါအဝင် component အချို့ကို ရွေးချယ်ထားပြီးဖြစ်ပါတယ်။ သည့်အတွက် installလုပ်နေစဉ်အတွင်းရွေးချယ်ထားတဲ့ component တွေကို အင်တာနက်ကနေတစ်ပြိုင်နက်download ဆွဲယူinstall လုပ်မှာဖြစ်ပါတယ်။ အဲဒီလို အင်တာနက် ကနေ တိုက်ရိုက်ဆွဲယူinstall လုပ်ခြင်းသည် အင်တာနက် connection speed ကောင်းနေချိန်တွေမှာ ပြဿနာမရှိပေမယ့် မကောင်းတဲ့အချိန်နှင့်တိုးတဲ့အခါမျိုးမှာ install မရဘဲ error များနှင့်ကြုံရတတ်ပါတယ်။

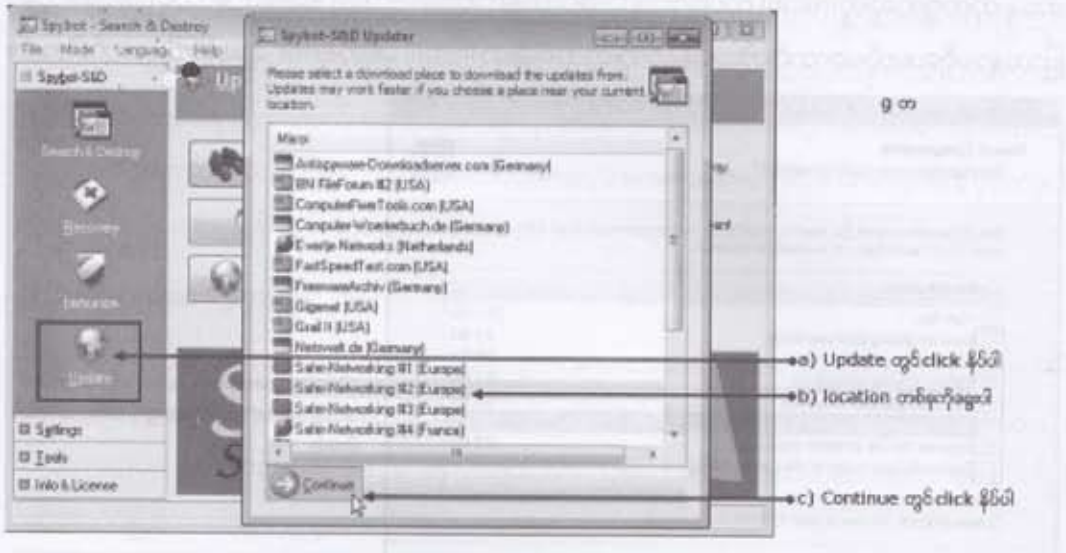


ယခုချိန်မှာ update မလုပ်သေးဘဲ install လုံးဝပြီးစီးပြီး နောက်မှ လုပ်ကြမယ်ဆိုရင်လည်း ရပါတယ်။ component တို့၏ဘေးမှ check box များထဲမှ အမှန်ခြစ်များကိုဖြုတ်ခဲ့ပြီး ဆက်လက် install သွားလိုက်ပါ။ ပြီးသွားတဲ့အခါ spybot control window ကိုတွေ့ရပါမယ်။ ပုံမှန်အားဖြင့် normal mode ဖြစ်သည့်တွက်ဘယ်ဘက်ခြမ်းတွင် Spybot-S&D tab တစ်ခုတည်းကိုသာမြင်ရပါမယ်။

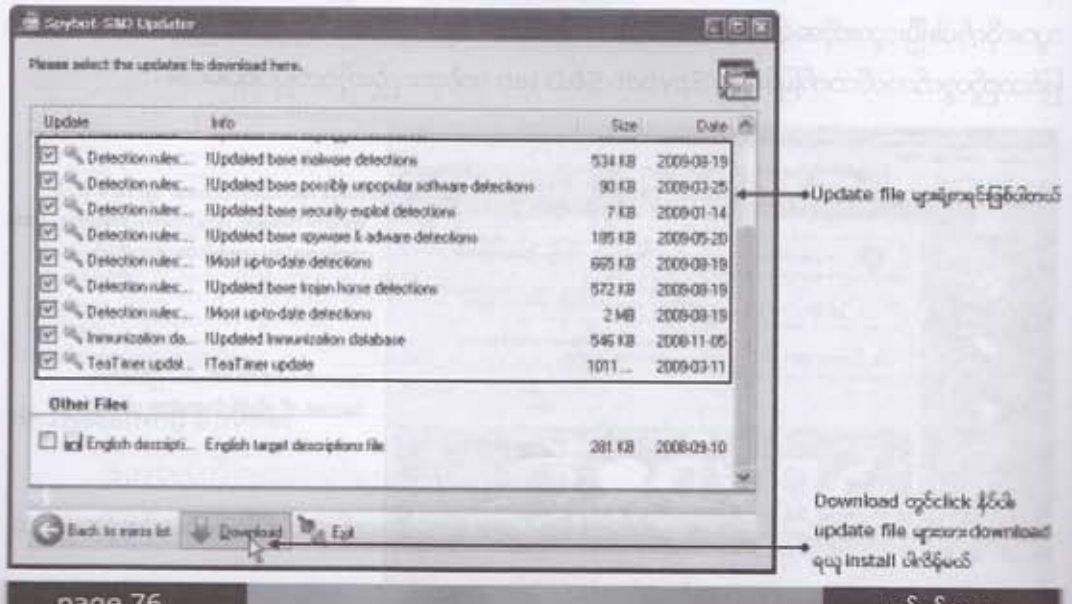


Updating Spybot

Spybotကို installပြီးသွားတဲ့အခါလုပ်ရမှာက security နှင့်နွယ်တဲ့ software တို့ရဲ့ထုံးစံအတိုင်း update လုပ်ရမယ်။ပြီးမှ scan လုပ်ကာစစ်ဆေးရှာဖွေရှင်းလင်းရပါမယ်။ Spybot S&D tab အောက်မှ **Update** တွင် click နှိပ်လိုက်ပါ။ update file ရှိရာ location များကိုမြင်ရပါမယ်။

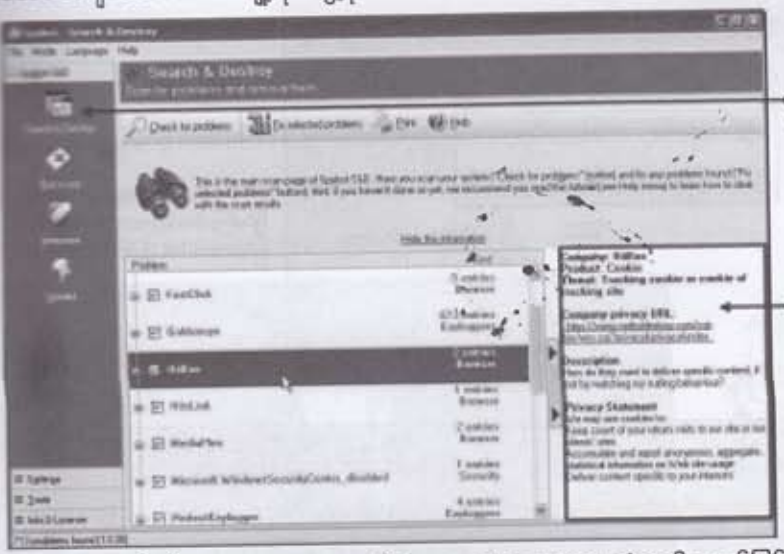


location တစ်ခုခုကိုရွေးချယ်ပြီး **Continue** တွင် click နှိပ်ပါက update file list ကျလာပါမည်။ **Download** တွင် click နှိပ်လိုက်ပါ။ update file များအား download ရယူ install ပေးသွားပါလိမ့်မယ်။

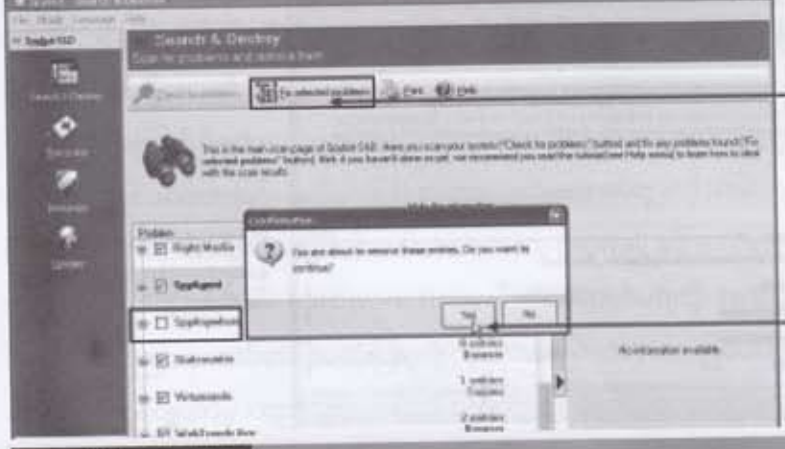


Scanning

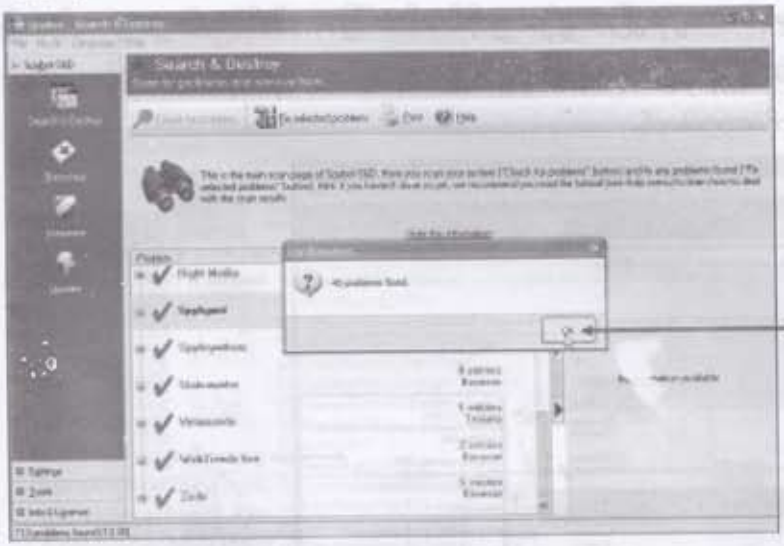
မိမိကွန်ပျူတာတွင်း spyware များကပ်ငြိနေခြင်းရှိမရှိစစ်ဆေးရန် **Search and destory** တွင် click နှိပ်လိုက်ပါ။ spybot မှစစ်ဆေးရာဖွေပြီး တွေ့ရှိသမျှကိုစီတန်းဖေါ်ပြထားပါလိမ့်မယ်။ ရှာဖွေတွေ့ရှိသည့် အဆဲတာ program အမည်တစ်ခုပေါ်တွင် click နှိပ်ကြည့်ပါ။ ညာဘက်ခြမ်းတွင် ၎င်း program နှင့်ပတ်သက်သော အချက်အလက်အချို့ကိုတွေ့ရပါမယ်။



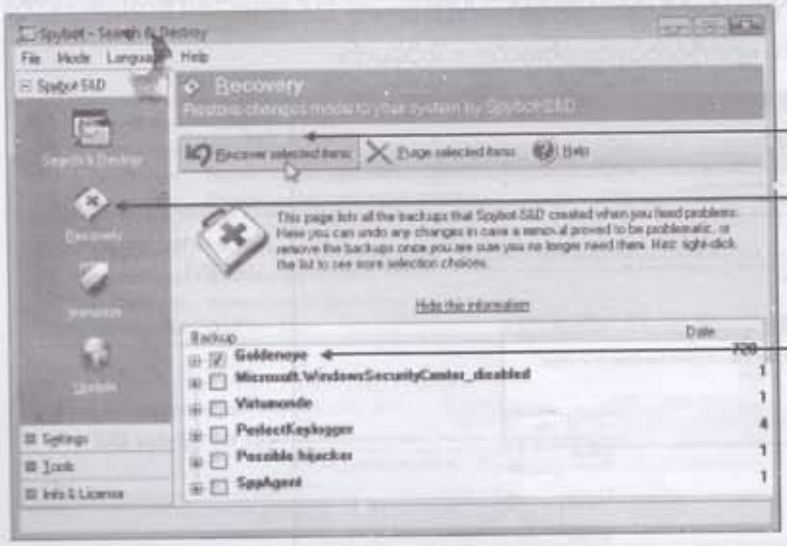
ဖျက်လိုသော program တို့ရဲ့ဘေးမှ checkbox ထဲတွင် အမှန်ခြစ်ပေါ်အောင် select မှတ်ကြ ရပါမယ်။ ပုံမှန်အားဖြင့် spyware program တို့အားဖျက်ထုတ်ဖို့ရန် အဆင်သင့် select မှတ်ပြီးသားဖြစ်ပါ တယ်။ သည့်အတွက် GoldenEye တို့လိုမိမိကိုယ်တိုင် ရည်ရွယ်ချက်ရှိရှိတင်ထားသော program များတွေ ပါနေရင် အမှန်ခြစ်ကိုဖြုတ်ခဲ့ဖို့တော့လိုပါလိမ့်မယ်။ အဆင်သင့်ဖြစ်ပြီဆိုရင် **Fix selected problems** တွင် click နှိပ်လိုက်ပါ။ spyware များကိုစတင်ရှင်းလင်းဖယ်ရှားပါလိမ့်မယ်။



ပြီးသွားတဲ့အခါ problem ဘယ်နှစ်ခုကိုရှင်းလင်းခဲ့ပါတယ်ဆိုတဲ့အကြောင်းဖေါ်ပြသော message ကိုမြင်ရပါမယ်။ **OK** တွင် click နှိပ်ပြီး Scan&Destory လုပ်ငန်းစဉ်များကို အဆုံးသတ်လိုက်ပါ။

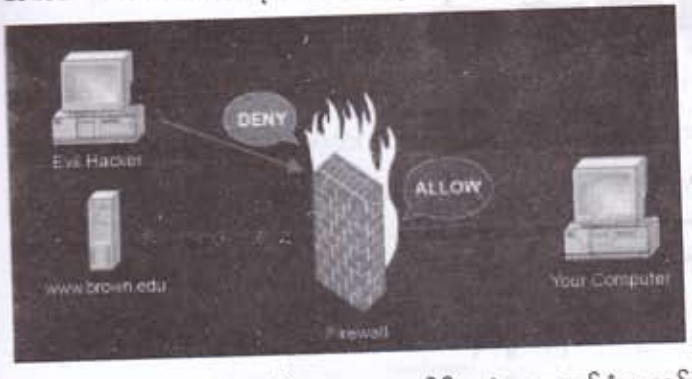


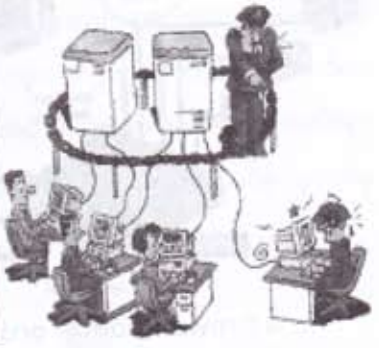
မှတ်ချက် - အကယ်၍အကြောင်းတစ်ခုခုကြောင့် ဖျက်ထုတ်ရှင်းလင်းပြီးကာမှပြန်လိုချင်တဲ့ program တွေများရှိခဲ့ရင် နှိုအတိုင်းပြန်လည်ရရှိအောင် Restore လုပ်ယူနိုင်ပါတယ်။ Recovery တွင် click နှိပ်လိုက်ပါ။Spybot မှဖျက်ထုတ်ထားသော program များရဲ့list ကိုမြင်ရပါမယ်။ပြန်လည်ရယူလိုသော program ဘေးမှ checkbox ထဲတွင် အမှန်ခြစ်ပေါ်အောင် click နှိပ်ရွေးပြီး recover selected items တွင် click နှိပ်လိုက်ပါ။



Firewall

အင်တာနက်သည် ကွန်ပျူတာ သန်းပေါင်းများစွာဖြင့် ချိတ်ဆက်တည်ဆောက်ထားသော ကမ္ဘာ အကြီးဆုံး Network ကြီးတစ်ခု။ အဲဒီအင်တာနက်ကြီးပေါ်မှာ စိတ်နေစိတ်ထားအမျိုးမျိုးနှင့် လူသန်းထောင်ချီ အသုံးပြုနေကြသလို ရနိုင်တာတွေကလည်း အများကြီးပါပဲ။ ဆိုရရင်သတင်းအချက်အလက်တွေ၊ ပညာရပ် ဆိုင်ရာ စာတမ်းတွေ၊ သီချင်းတွေ၊ ရုပ်ရှင်တွေ အစရှိသဖြင့် အမျိုးအစား အစုံအလင် ပေါ့။ သို့သော် အပေါင်း လက္ခဏာဆောင်တဲ့ အကောင်းချည်သာ အစဉ်အမြဲရနေလိမ့်မယ် လို့တော့ မျှော်လင့်၍ မရပါဘူး။ မိမိကွန်ပျူတာကိုဒုက္ခပေးမယ့် virusတွေ၊ trojanတွေအပါအဝင် fileတွေ၊ ကိုယ်ရေးအချက်အလက်တွေ ခိုးယူဖျက်ဆီးမယ့် Hacker၊ Intruderတို့ရဲ့ရန်ကလည်းမသေးလုပါဘူး။ ဒါတွေကိုကာကွယ်ဖို့ရန် အတွက် မိမိကွန်ပျူတာနှင့်အင်တာနက်ကြားမှာ အတားအဆီး barrierတစ်ခုရှိဖို့လိုအပ်လာပါတယ်။ ထိုအကာကွယ် အတားအဆီး barrier ကို firewall လို့ခေါ်ပါတယ်။





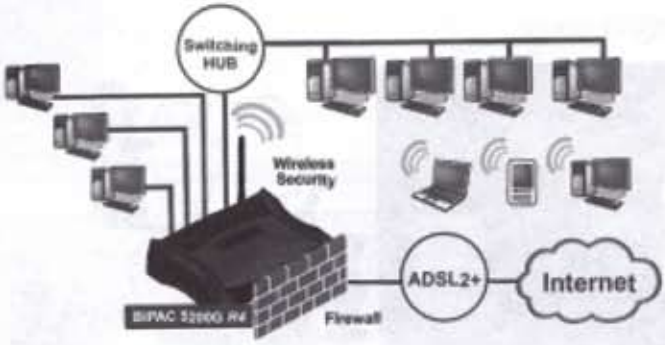
Firewall တွေဆိုတာက ဌာနဆိုင်ရာရုံးများ၊ စက်ရုံအလုပ်ရုံတို့၏ ဝင်ပေါက်ထွက်ပေါက်များတွင် စောင့်ကြပ်စစ်ဆေးလျက်ရှိသော လုံခြုံရေးဝန်ထမ်း (Security guard) တို့နှင့်အလုပ်လုပ်ပုံဆင်တူပါတယ်။ ကွန်ပျူတာတစ်လုံးမှာ Firewall ကို install လုပ်ထားမယ်ဆိုရင် ကွန်ပျူတာထဲသို့ဝင်သမျှထွက်သမျှ data အားလုံးတို့ဟာ Firewall ကိုဖြတ်သန်းသွားရပါတယ်။ Firewall ဟာ မိမိထံရောက်သမျှ data packet များကိုတစ်ခုချင်းဆေချာစွာစစ်ဆေးပြီး ခွင့်ပြုချက်နှင့် မကိုက်ညီသော data packet များကို ဝင်ခွင့်ထွက်ခွင့် မပေးဘဲပိတ်ဆို့တားဆီးပေးနိုင်ပါတယ်။

ဒါ့ကြောင့် hackerများအင်တာနက်မှတဆင့် မိမိကွန်ပျူတာထဲဝင်ရောက်ပြီး file များ၊ program များအားပြုပြင်ရေးသားခြင်း၊ ဖျက်ဆီးခြင်း၊ dataအချက်အလက်များကို အခြားကွန်ပျူတာများသို့လှှဲပြောင်းစွာ ပို့လွှတ်ခြင်းများမှကာကွယ်ပေးနိုင်ပါတယ်။ hardware firewall နှင့် software firewall ဆိုပြီး firewall အမျိုးအစား ၂မျိုးရှိပါတယ်။ hardware firewall ဆိုတာက hubတို့၊ switchတို့လိုအင်တာနက်နှင့်မိမိ Network ကြားမှာတပ်ဆင် အသုံးပြုရတဲ့ hardware device ဖြစ်ပါတယ်။ software firewall ဆိုတာက ကွန်ပျူတာမှာထည့်သွင်း install လုပ်ကာအသုံးပြုရသော software program ဖြစ်ပါတယ်။

မည်သို့ပင် အမျိုးအစားတွေကွဲကွဲ firewall တို့ရဲ့ဘုံရည်မှန်းချက်ကတော့ အင်တာနက်ဘက်ကလာမယ့် အနှောင့်အယှက်၊ ခြေးအန္တရာယ်တို့မှ ကာကွယ်ရန်ဖြစ်ပါတယ်။

Hardware Firewall

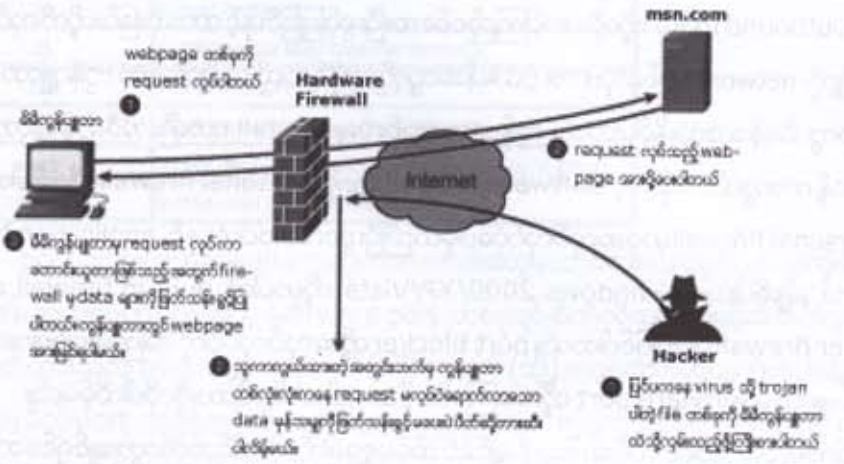
hardware firewall တွေကို ကွန်ပျူတာ တစ်လုံးတည်း အတွက် သီးသီးသန့်သန့်တပ်ဆင် အသုံးပြုမှုမှာနည်းပါတယ်။ networkတစ်ခုလုံးရဲ့ securityကိုတို့းမြှင့်လိုတဲ့အတွက်သာ အသုံးပြုကြမှု ပိုများပါတယ်။ hardware firewall မှာမှအမျိုးအစားတွေကလည်းအများကြီးပါပဲ။ သာမာန်အိမ်သုံးရုံးသုံး networkငယ်လေးတွေအတွက် Standalone firewall အမျိုးအစားဖြစ်တဲ့ broadband router များကိုတပ်ဆင်အသုံးပြုလေ့ရှိပါတယ်။



ဒီ firewall router လေးတွေဟာ ကုန်ကျစရိတ်သက်သာသလို ခက်ခက်ခဲခဲ configure လုပ်စရာမလိုတဲ့အတွက် အသုံးပြုတဲ့နေရာမှာ အလွယ်ကူဆုံး firewallအမျိုးအစားလည်းဖြစ်ပါတယ်။ ဆိုရရင်သူတို့ထဲမှာ firewallတို့ရဲ့အသက်ဖြစ်တဲ့ အခြေခံ ruleများအဆင်သင့်ထည့်သွင်းရေးသား ထားပြီးသား ဖြစ်ပါတယ်။Data packet တစ်ခုရောက်လာတိုင်း ထို rule များအရ တိုက်ဆိုင်စစ်ဆေးပြီး ဆက်လက် transfer လုပ်သင့်မလုပ်သင့်ဆုံးဖြတ်ပါတယ်။ ruleအရ transferမလုပ်သင့်တဲ့ Data packet များကို ဖြတ်သန်းခွင့်မပေးဘဲ drop လုပ်ချပါလိမ့်မယ်။ rule တွေကို configure လုပ်စရာ မလိုသည့်အတွက် networkမှာထည့်သွင်းအသုံးပြုမယ်ဆိုရင်လည်း အများအားဖြင့် ဒီအတိုင်းချိတ်ဆက် တပ်ဆင်လိုက်ရုံပါပဲ။ လိုအပ်လို့ configure လုပ်ရရင်တောင်မှ IP address တွေ၊ password တွေ ထည့်ပေးရုံလောက်ပဲ။ တပ်ဆင်အသုံးပြုနေသမျှ ကာလပတ်လုံး user တို့ရဲ့အခန်းကဏ္ဍမပါဘဲ သူ့အလုပ်သူလုပ်နေမှာဖြစ်ပါတယ်။သို့သော် ဈေးနှုန်းသက်သာပြီး အသုံးပြုရလွယ်သလို အင်တာနက် ဘက်ကလာမယ့်အနှောင့်အယှက်များကို တားဆီးတဲ့နေရာမှာလည်း အတိုင်းအတာ တစ်ခုထိသာ ကာကွယ်ပေးနိုင်စွမ်းရှိပါတယ်။ ဘယ်လိုအခါမျိုးမှာ အကာကွယ်မပေးနိုင်ဘူးလဲဆိုတာကို နားလည် သဘောပေါက်စေရန်ဖြစ်စဉ်တခုကိုလေ့လာကြည့်ရအောင်။

Webpage တစ်ခုကိုခေါ်ကြည့်တာဘဲဖြစ်ဖြစ်၊Email ဆွဲချတာပဲဖြစ်ဖြစ် အင်တာနက်ပေါ်က information(data)တွေကို မိမိကွန်ပျူတာကနေ request လုပ်ကာတောင်းယူခြင်းဖြစ်ပါတယ်။ ဆိုရရင် Webpage တစ်ခုကိုခေါ်ကြည့်ရန် Browser(ဥပမာ-IE)မှာလိပ်စာ (ဥပမာ -www.cnn.com) ရိုက်ထည့်ပြီး Enter နှိပ်လိုက်ရင်မိမိကွန်ပျူတာထဲကနေ request လုပ်တဲ့signalတစ်ခုထွက်သွားပါမယ်။ ဘက်ရောက် webserver (www.cnn.com ရှိနေသော ကွန်ပျူတာ) သည်ထိုrequest ကိုလက်ခံရရှိတဲ့အခါ ဆောင်းယူသည့် Webpage ကို နဂိုမူလ request လုပ်သော မိမိကွန်ပျူတာထံသို့ပြန်ပို့ပေးပါတယ်။ ဤနည်းဖြင့် webserver မှပြန်ပို့သော data များသည် firewallကိုဖြတ်သန်းကာမိမိကွန်ပျူတာတွင်း ရောက်ရှိပြီး IEတွင် Webpage တစ်ခုအဖြစ်မြင်ကြရပါတယ်။

ဤဖြစ်စဉ်ကိုကြည့်မယ်ဆိုရင် မိမိက request လုပ်သည့်အတွက် ကြောင့် အင်တာနက်က ဝင်လာတဲ့ data တွေကို firewall မှဖြတ်သန်းခွင့်ပြုလိုက်ခြင်းဖြစ်ပါတယ်။ အင်တာနက်ပေါ်က program တွေ download ဆွဲယူတာပဲဖြစ်ဖြစ်၊ email attach file တွေ download ဆွဲယူတာပဲဖြစ်ဖြစ် ထိုသဘောတရားအတိုင်းပဲ၊ ကိုယ်ကအရင် request လုပ်ရတယ်။ သူကာကွယ်ထားတဲ့အတွင်းဖက်က request မလုပ်ဘဲအင်တာနက်ဘက်က ဝင်လာလို့မရပါဘူး။ ဝင်လာခဲ့ရင် firewall ကပိတ်ဆို့တားဆီးမှာ ဖြစ်ပါတယ်။ ဒါက router firewallတို့ရဲ့ကွန်ပျူတာတွေကိုအကာအကွယ်ပေးရန် လုပ်ဆောင်နိုင်မှုတစ်ခု ဖြစ်ပါတယ်။



သို့သော် အဲဒီ အကာအကွယ်ပေးနိုင်မှုသည် အတိုင်းအတာတစ်ခုထိသာ သက်ရောက်မှုရှိနိုင်ပါ တယ်။ အကယ်၍များ trojan ပါတဲ့ Program fileတစ်ခုကို download ဆွဲယူမိတာပဲဖြစ်ဖြစ်၊ virusပါတဲ့ email attached fileကိုဆွဲယူမိတာပဲဖြစ်ဖြစ်၊ မိမိကိုယ်တိုင်က request လုပ်ယူတာဖြစ်သည့်အတွက် ဘာပဲပါပါ firewallက ခွင့်ပြုမှာဖြစ်ပါတယ်။ ဤနည်းဖြင့် ကွန်ပျူတာအတွင်းသို့ virusများ၊trojan များ

ကပ်ငြိနေနိုင်ပြီး၊ ထို virus ၊ trojan တို့မှ ကွန်ပျူတာထဲက information များအား ပြင်ပသို့ အသုံးပြု သူတို့မသိရှိစေဘဲ လျှို့ဝှက်ပို့လွှတ်ခဲ့မယ်ဆိုရင်လည်း firewall က ခွင့်ပြုမှာဖြစ်ပါတယ်။ ဘာလို့လဲဆိုတော့ မိမိကွန်ပျူတာသည် ကနဦးစတင် request လုပ်သည့်အတွက် firewall မှ မတားဆီးနိုင်ပါဘူး။

အဲဒီလိုဆိုတော့လည်း trojan တွေ၊ virus တွေရဲ့ရန်ကကာကွယ်ပေးနိုင်တဲ့ hardware firewall မျိုးတွေမရှိတော့ဘူးလားလို့တွေးစရာဖြစ်လာနိုင်ပါတယ်။ အဲဒီလိုတော့လည်းမဟုတ်ပါဘူး။ ကိုယ် network ရဲ့ လိုအပ်ချက်ပေါ်မူတည်ပြီး၊ firewall rule တွေ လိုသလိုပြင်ဆင်ရေးသားက trojan တို့၊ virus တို့ အပါအဝင် hacker များရဲ့ရန်မှ ထိထိရောက်ရောက်ကာကွယ်ပေးနိုင်တဲ့ hardware firewall မျိုးတွေလည်း ရှိပါဟယ်။ ဒါပေမယ့် အဲဒီ firewall မျိုးတွေဟာစျေးလည်းကြီးသလို သာမန်ကျွမ်းကျင်မှုနှင့် သူတို့ကို configure လုပ်လို့မရပါဘူး။ သည့်အတွက် သာမန်အိမ်သုံး၊ရုံးသုံး network ငယ်တွေအတွက်တော့ ဈေးနှုန်းသက်သာပြီး အသုံးပြုရလွယ်ကူသည့် firewall router ငယ်တို့သည်သာ သင့်လျော်သော ရွေးချယ်မှုဖြစ်ပါတယ်။

Software Firewall

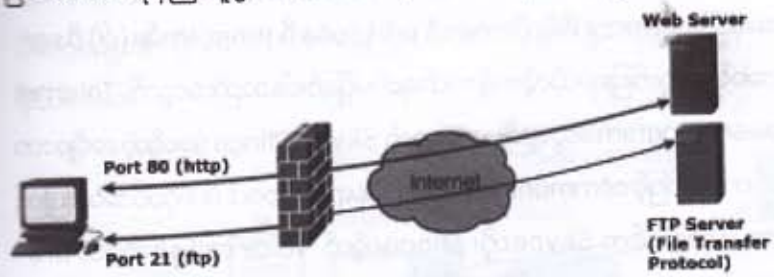
Software firewall ဆိုတာက ကွန်ပျူတာမှာထည့်သွင်း install လုပ်ကာသုံးရတဲ့ program တစ်မျိုးပင်ဖြစ်ပါတယ်။ အဲဒီ program ကိုကွန်ပျူတာမှာ install ထားမယ်ဆိုရင် ဝင်သမျှ (Inbound)၊ ထွက်သမျှ (Outbound) data တို့ကို စောင့်ကြည့်စစ်ဆေးပြီး ခွင့်ပြုခြင်းနှင့် တားဆီးခြင်းတို့ကို လုပ်ဆောင်ပါတယ်။ အချို့ကို network တစ်ခုလုံးကာကွယ်ရန်အတွက် သုံးနိုင်သလို အချို့ကိုတော့ ကွန်ပျူတာတစ်လုံးတည်းကို ကာကွယ်ရန်သာသုံးနိုင်ပါတယ်။ ကွန်ပျူတာတစ်လုံးမှာ install ထားပြီး အဲဒီကွန်ပျူတာကိုသာသီးသီးသန့်သန့် ကာကွယ်ပေးနိုင်တဲ့ Software firewall မျိုးကို personal firewall လို့ခေါ်ပါတယ်။

personal firewall မှာမှ အလုပ်လုပ်ပုံပေါ်မူတည်ပြီး port blocker နှင့် application blocker ရယ်လို့ အဓိက ၂မျိုးရှိပါတယ်။ windows 2000/XP/Vista တို့မှာပါတဲ့ built in firewall တို့သည် port blocker firewall များပဲဖြစ်ပါတယ်။ port blocker တို့အလုပ်လုပ်ပုံကို အကြမ်းမျဉ်းနားလည်ရန် အတွက် ကွန်ပျူတာမှ software port တို့အကြောင်းကို အနည်းငယ် သိထားဖို့လိုပါလိမ့်မယ်။

အိမ်တစ်လုံးမှာဆိုရင် လမ်းပေါ်ထွက်ချင်ရင် အိမ်ရှေ့ပေါက်၊ ဂိုဒေါင်ဘက်သွားချင်ရင်ဘေးပေါက်၊ နောက်ဖေးထွက်ချင်ရင် နောက်ဖေးပေါက် အစရှိသဖြင့် ဝင်နိုင်ထွက်နိုင်တဲ့ တံခါးပေါက်တွေရှိပါတယ်။ အလုပ်ပေါ်မူတည်ပြီး သက်ဆိုင်ရာတံခါးပေါက်တွေကနေဝင်ကြ ထွက် ကြတယ်။ ထိုနည်းလည်းကောင်းပဲ ကွန်ပျူတာတစ်လုံးမှာ အိမ်တံခါးပေါက်တွေနှင့်တူတဲ့ software port ပေါင်းအကြမ်းအားဖြင့် 65500 ခန့်ရှိပါတယ်။ အင်တာနက်ပေါ်က အခြားကွန်ပျူတာ(web server ၊ mail server)တို့နှင့် အပြန်အလှန်

ဆက်သွယ်တဲ့ နေရာမှာ service အလိုက်သက်ဆိုင်ရာ software port number တွေကနေသာ communicate လုပ်ကြရပါတယ်။ (ဒီနေရာမှာport ဆိုတာ ကွန်ပျူတာတွေမှာရှိတဲ့ USB၊ parallet port အစရှိတဲ့ hardware port များအားဆိုလိုခြင်းမဟုတ်ပါ)။

Webpageတိုနှင့် ပတ်သက်ရင် port 80 (သို့) port 443၊ email ပို့ရန် port25 ၊email ရယူရန် port 110 ၊file တွေ transfer လုပ်ရန် port23 အစရှိသဖြင့် service အလိုက် ၊ထို port များမှနေ၍အဝင်အထွက်လုပ်ကြရပါတယ်။ဥပမာ webpage တစ်ခုကိုခေါ်ကြည့်ရန် Internet Explorer မှာလိပ်စာ(www.cnn.com) ရိုက်ပြီး enter နှိပ်တဲ့အခါ မိမိရဲ့ requestသည် port 80 ကနေ ထွက်မှာ ဖြစ်ပါတယ်။ထိုနည်းတူစွာ Outlook Expressကနေ emailပို့တဲ့အခါ port25 ကနေ ထွက်မှာဖြစ်ပါတယ်။



Port	Description
21	FTP (File Transfer Protocol)
23	Telnet Protocol
25	SMTP(Simple Mail Transfer Protocol
110	POP3 (Post Office Protocol 3)
80	HTTP (Hypertext Transfer Protocol)
443	HTTPS (Hypertext Transfer Protocol over TLS/SSL)
5060	SIP(Session Initiation Protocol)

port blocker firewall တွေဆိုတာက တံခါးတွေသော့ခတ်၊သော့ဖွင့်လုပ်သလိုမျိုးကွန်ပျူတာ ဝင်ပေါက်၊ထွက်ပေါက်များဖြစ်တဲ့ software port တစ်ခုချင်းစီကိုလိုသလိုအဖွင့်အပိတ် လုပ်နိုင်ပါတယ်။ သူတို့ပိတ်ထားသည့် port တွေကနေအဝင်(သို့)အထွက် (သို့) အဝင်ကောအထွက်ပါနှစ်မျိုးစလုံးလုပ်လို့ မရပါဘူး။ ဒီလို port အဖွင့်အပိတ်တွေကို အသုံးပြုသူ user တွေကိုယ်တိုင် manage လုပ်နိုင်တယ်။ သို့သော် port အရေအတွက်စုစုပေါင်း 65000 လောက်ထဲကဘယ် portတွေကိုတော့ ဖွင့်ရမယ်။ဘယ် port တွေကိုတော့ ပိတ်ထားသင့်တယ်ဆိုတာ သိနားလည်ပြီး၊ အသုံးပြုသူတို့ကိုယ်တိုင် manage လုပ်ဖို့ရန် မလွယ်ပါဘူး။

မဖြစ်မနေဖွင့်ထားသင့်တဲ့ port 80 လိုမျိုးကို မှားပိတ်မိရင် webpage ဖွင့်မရတဲ့ပြဿနာမျိုး တွေကြုံရနိုင်ပါတယ်။ သည့်အတွက် လူတိုင်းအလွယ်သုံးနိုင်အောင် ယနေ့ port blocker firewall အများစု

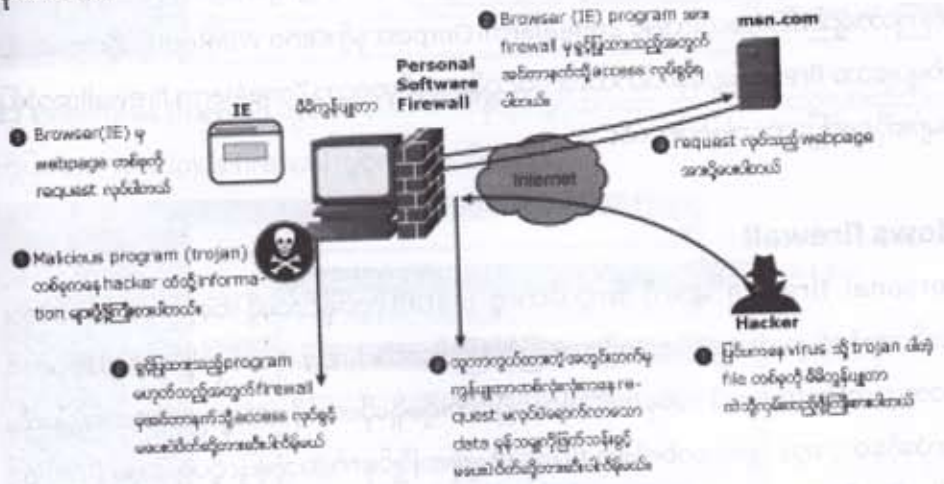
တို့တွင်(ရှေ့ကကြုံခဲ့ရတဲ့ အတွေ့အကြုံ များပေါ်တွင် အခြေခံပြီး) မဖြစ်မနေအရေးကြီးသော အချို့port များကလွဲ၍ trojan တွေ၊ virusတွေ ပျံနှံဖို့ရန် သုံးတတ်တဲ့ port တွေ၊ attackerတွေ attackလုပ်ရန် သုံးတတ်တဲ့ port တွေအစရှိတဲ့ port အတော်များများကို အဆင့်သင့်ပိတ်ထားပေးပြီးသား ဖြစ်ပါတယ်။ ဒါပေမယ့် Windows OSမှာပါတဲ့ built in firewallအပါအဝင်အခြားသော port blocker firewall တွေဟာ တကယ်တန်းတော့ များစွာအသုံးမတည့်လှပါဘူး။ မရှိတာထက်စာရင်တော်သေးတယ်လို့ပြောရမယ့် အနေအထားမှာပင်ရှိပါတယ်။ ဘာဖြစ်လို့ဒီလိုပြောရလဲဆိုတာကိုအနည်းငယ်ရှင်းပြလိုပါတယ်။

port 80သည်အင်တာနက်ပေါ်က webpage တွေခေါ်ကြည့်မည့်ကွန်ပျူတာတိုင်းအတွက်(အထူးသဖြင့် Internet Explorer ကို program များအတွက်) မဖြစ်မနေဖွင့်ထားရမည့် port ဆိုတာ သိခဲ့ပြီးဖြစ်ကြပါလိမ့်မယ်။ ဒီနေရာမှာအနည်းငယ်အကျယ်ချဲ့လိုတာက ဒီ port ကနေ ဒီ programမျိုး(ဝါ) ဒီ service နှင့်ဆိုင်တဲ့ data တွေဘဲအဝင်အထွက်ပြုရမယ်လို့ကန့်သတ်ချက်မရှိခြင်းပါ။ သည့်အတွက် Internet Explorer၊ Mozillaတို့လို browser programတွေချည်းသာမဟုတ် Skype၊ Pfingo အစရှိတဲ့အချို့သော programတွေသည်လည်းအင်တာနက်ဖြင့် communicateလုပ်တဲ့နေရာမှာ ဒီport 80ကိုပင်အသုံးပြုကြခြင်းမျိုးလည်းရှိပါသေးတယ်။ အမှန်တကယ်က Skypeတို့၊ pfingoတို့ကို Voice call နှင့်ဆိုင်တဲ့ programတွေသုံးရမယ့် Standard port သည် 5060 ဖြစ်ပါတယ်။

သို့သော်လည်း ကိုယ်ပိုင် network တွေ အပါအဝင် ISP တို့မှာ တပ်ဆင်အသုံးပြုတဲ့ firewall အများစုတို့မှာ port 5060 ကို block ထားလေ့ရှိတဲ့အတွက် အဲဒီ program တွေသည် အင်တာနက်ပေါ်က သူတို့ Server များနှင့်အဆက်အသွယ်လုပ်၍မရတော့ပဲဖွင့်လိုက်တိုင်း disconnectedဆိုတဲ့ errorမျိုးကိုသာတွေ့နေကြရပါတယ်။ ဤတွင်မှ voice service ပေးသူတို့သည် သူတို့program ကို firewallမှာ ဖွင့်တာသေချာတဲ့ port 80 နှင့် ထွက်နိုင်အောင်ပြုပြင်လိုက်ခြင်းဖြင့် disconnected ပြဿနာ ကို ပြေလည်အောင် ဖြေရှင်းလိုက်ကြပါတယ်။

ယနေ့အခါ virus တွေ၊ trojanတွေ နေ့စဉ်နှင့်အမျှဆိုသလိုတစ်မျိုးပြီးတစ်မျိုးပေါ်ထွက်လာလျက်ရှိပါတယ်။ အဲဒီများစွာထဲက အချို့မှာ port 80 ကနေ ပျံနှံနိုင်အောင် စီမံရေးသားထားသော virus များ၊ trojanများလည်းပါဝင်ပါတယ်။ ဥပမာ - Code Red Virus မျိုးဖြစ်ပါတယ်။ ထို virus များ ၊ trojan များသာ ကူးစက်ခံရရင် port 80 ကနေထွက်ပြီး အခြားကွန်ပျူတာများသို့ ဆက်လက်ပျံနှံ့စေခြင်း၊ attackလုပ်ခြင်းများကြုံရတတ်ပါတယ်။port blockerတွေရဲ့ အားနည်းချက်က သူတို့ဖွင့်ထားတဲ့ port ကနေဘယ်programတွေ accessလုပ်နေသလဲဆိုတာခွဲခြားပိတ်ဆို့ပေးနိုင်စွမ်းမရှိခြင်းဖြစ်ပါတယ်။ ဆိုရရင် port80 ကနေထွက်နေတာ IEလား၊Skypeလား၊virusလားဆိုတာမသိနိုင်ပါဘူး။ ဖွင့်ထားတဲ့ portကနေ ဘယ် programပဲ accessလုပ်လုပ် ခွင့်ပြုမှာဖြစ်ပါတယ်။

application blocker firewall တို့ရဲ့အလုပ်လုပ်ပုံသည် port blocker တို့နှင့် များစွာမကွာလှပါဘူး။ application blocker တို့ရဲ့ အားသာချက်က ကွန်ပျူတာထဲမှ program တစ်ခုခုသည် အင်တာနက်သို့ port တခုခုကနေထွက်ဖို့ကြိုးစားတိုင်း ချက်ချင်းထွက်ခွင့်မပေးဘဲ တားထားမယ်။ ပြီးရင် ဘယ် programက ဖြင့်ပြင်ပသို့ access လုပ်ရန်ကြိုးစားနေပါတယ် ဆိုတာမျိုးပါသော popup message ဖြင့် အသုံးပြုသူတို့အားအသိပေးပါတယ်။ အကယ်၍ access လုပ်ဖို့ကြိုးစားတဲ့ program သည်မိမိသုံးနေကျ စိတ်ချရတဲ့ program (ဥပမာ Internet Explorer၊ Outlook Express) မျိုးဖြစ်ပါက allow တွင် click နှိပ်ပြီးထွက်ခွင့်ပေးလိုက်ဖို့ရန်ခိုင်းစေနိုင်တယ်။ ဘာ programမှန်းလည်းမသိ၊သံသယဖြစ်ဖွယ်ရှိတယ်ဆိုရင် denyတွင် click နှိပ်ကာ ထွက်ခွင့်မပေးဘဲ ပိတ်ခိုင်းလိုက်နိုင်ပါတယ်။ ပြင်ပကွန်ပျူတာတစ်လုံးလုံးကနေ မိမိကွန်ပျူတာသို့ access လုပ်ရန်ကြိုးပမ်းလာတဲ့အခါမျိုးတွေမှာလည်းအလားတူ messageများတွေ့ရနိုင်ပါတယ်။



သတ္တုချကြည့်ရင် application blocker firewallတို့ရဲ့စွမ်းဆောင်ရည်သည်အသုံးပြုသူ Userတို့ပေါ်မှာများစွာမူတည်ပါတယ်။ခွင့်မပြုသင့်တဲ့ program တစ်ခု access လုပ်ခြင်းအားဖြင့် မှားယွင်း allowလုပ်ခဲ့မိရင်တော့ အနတ်လက္ခဏာဆောင်တဲ့ ဆိုးကျိုးများနှင့်ရင်ဆိုင်ရဦးမှာဖြစ်ပါတယ်။ ယခုမှစတင်အသုံးပြုသူတွေအတွက်အဲဒီ pop-up message တွေဟာလည်းအံ့သြစရာကောင်းလောက်အောင် များပြားတာကိုတွေ့ရဦးမှာဖြစ်ပါတယ်။ ဘယ် programတွေကို allow လုပ်သင့်တယ်။ ဘယ် program တွေကို denyလုပ်သင့်တယ် ဆိုတာတွေစဉ်းစားဆုံးဖြတ်ရတာလည်း အတွေ့အကြုံနည်းသေး သူတို့အဖို့ စိတ်ရှုပ်စရာဖြစ်ကောင်းဖြစ်နေပါလိမ့်မယ်။မည်သို့ပင်ဖြစ်စေ ကိုယ့်ကွန်ပျူတာရဲ့ securityပိုင်းကို တိုးမြှင့်ကာကွယ်လိုသူတွေအတွက် မဖြစ်မနေfirewall တစ်ခုရွေးရမယ်ဆိုရင်တော့ ဒီ application blockerတို့ဟာ အသင့်တော်ဆုံးဖြစ်ပါလိမ့်မယ်။

အထူးသဖြင့် cable DSL နှင့် Wireless connection (Broadband Wimax ၊ IP Star) ကိုသုံးပြီး အင်တာနက်ချိတ်ဆက်နေသူများအနေနှင့် firewall ကိုမဖြစ်မနေသုံးသင့်ပါတယ်။ ထို connection များထဲမှတစ်ခုခုကိုသုံးထားသောကွန်ပျူတာတို့၏ IP address များ (ဥပမာ 10.243.123.12) တို့ဟာ ပုံသေပြောင်းလဲမှုမရှိသော static နံပါတ်များဖြစ်သောကြောင့် dial-up user များထက် hacker များ အလွယ်တကူဝင်ရောက်နိုင်ပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ dial-up connection ဖြင့် အင်တာနက်သို့ ချိတ်ဆက်သုံးသော ကွန်ပျူတာများ၏ IP address တို့သည်ပုံသေမဟုတ်ဘဲတစ်ကြိမ်နှင့်တစ်ကြိမ်မတူဘဲ ကွဲပြားကြပါတယ်။ ဒါ့ကြောင့် dial-up ကိုအသုံးပြုသောကွန်ပျူတာများကို hack လုပ်ဖို့ရန်၊ attack လုပ်ဖို့ရန် ပိုမိုခက်ခဲတတ်ပါတယ်။ သို့သော်လည်း မိမိရဲ့သတင်းအချက်အလက်များကို ခိုးထုတ်နိုင်သည့် Virus များ၊ Trojan များ၊ Spyware များရဲ့ရန်မှကာကွယ်ရန်အတွက် firewall ဟာများစွာအသုံးတည့်ပါသေးတယ်။

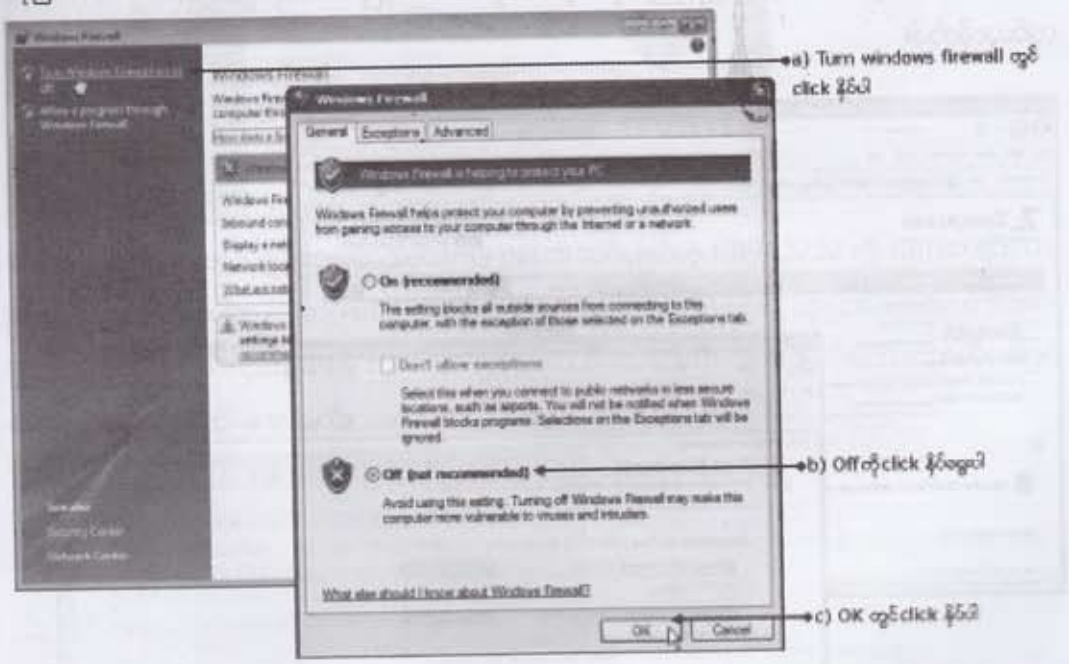
ယနေ့အခါရွေးချယ်စရာ application blocker firewall များစွာရှိပါတယ်။ သူဟာနှင့်သူတော့ အစွမ်းထက်ကြတာချည်းပါပဲ။ အထူးသဖြင့် ZoneAlarm၊ Outpost နှင့် Kerio WinRoute တို့ဟာရေပန်းစားလူကြိုက်များသော firewall များဖြစ်ပါတယ်။ ဒီလမ်းညွှန်စာအုပ်မှာတော့ ZoneAlarm firewall အသုံးပြုကာကွယ်ပုံများကိုဖော်ပြသွားမှာဖြစ်ပါတယ်။

Windows firewall

Personal firewall များကို အလွယ်တကူ install လုပ်နိုင်သလို အခြေခံသဘောတရားအနည်းငယ်သိထားရုံနှင့်များစွာအခက်အခဲမရှိအသုံးပြုနိုင်ကြပါတယ်။ firewall တစ်ခုကို install မလုပ်ခင် အဲဒီကွန်ပျူတာမှာအခြား firewall တစ်ခု install လုပ်ပြီးသားရှိမရှိဆိုတာကိုသေချာစွာစစ်ဆေးရပါမယ်။ ဘာ့ကြောင့်လဲဆိုတော့ ကွန်ပျူတာတစ်လုံးမှာ firewall ၂ခုတပြိုင်နက် အသုံးပြုလို့မရပါဘူး။ firewall နောက်တစ်မျိုးကို ထပ်မံ install လိုလျှင် ပထမရှိပြီးသားကို uninstall အရင်လုပ်ရပါမယ်။ ဒါ့ကြောင့် Windows XP ၊ Vista အသုံးပြုသူများအနေနှင့် သူတို့ထဲမှာပါတဲ့ built-in firewall ကို အသုံးပြုလိုက သုံးနိုင်ပါတယ်။ အကယ်၍ သီးခြား Personal firewall ကို install လိုပါက အဲဒီ built-in firewall ကို အလုပ်မလုပ်အောင်အရင်ပိတ်ထားပစ်ဖို့လိုပါတယ်။ ဘယ်လိုပိတ်ရမလဲဆိုတာ ကြည့်ကြရအောင်။

1) Start> Control Panel တွင် click တစ်ချက်နှိပ်ပါ။ control panel ပွင့်လာပါမယ်။ ပုံမှန်အားဖြင့် ဆိုရင် category view ဖြင့်မြင်ကြရပါမယ်။ Control Panel window ၏ဘယ်ဘက်ခြမ်းရှိ **Classic veiw** တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ ညာဘက်ခြမ်းတွင် windows firewall ကိုတွေ့ရပါမယ်။ (Windows XP ပဲဖြစ်ဖြစ်၊ Windows Vista ပဲဖြစ်ဖြစ် control panel ဖွင့်ရမှာခြင်းအတူတူဖြစ်ပါတယ်။)

2) Windows firewall တွင် double click နှိပ်ပါ။ ဖွင့်ထားသလား၊ ပိတ်ထားသလားဆိုတဲ့အခြေအနေကိုပြသော Windows firewall ပွင့်လာပါမယ်။



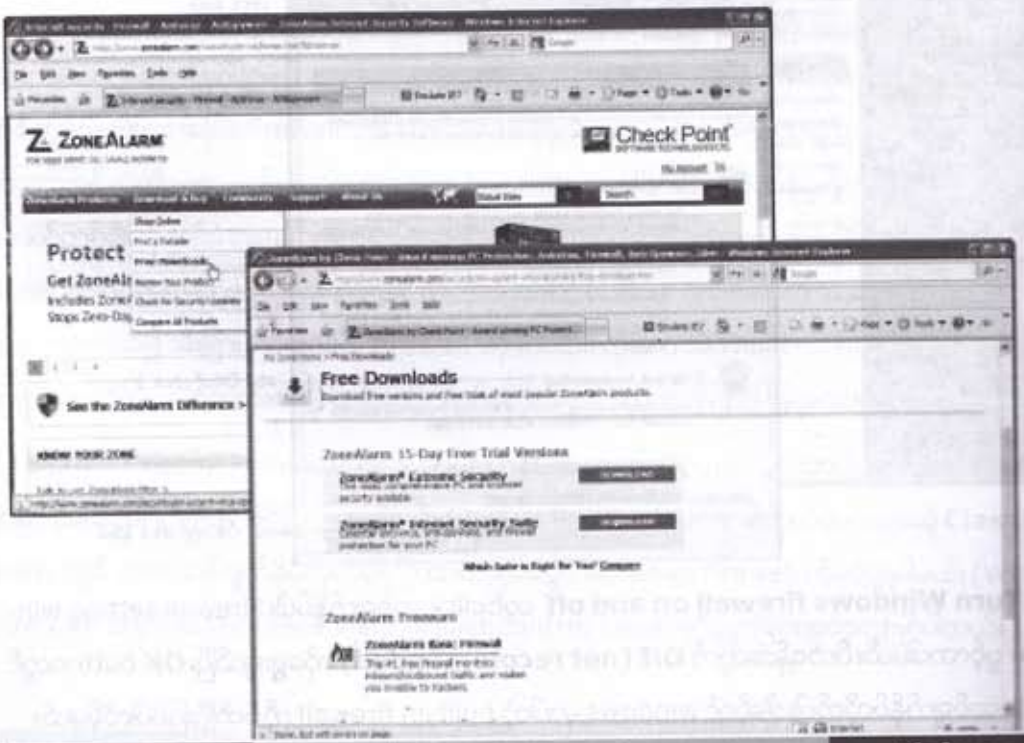
3) Turn Windows firewall on and off တွင် click တစ်ချက်နှိပ်ပါ။ Firewall setting window ပွင့်လာပါမယ်။ ပိတ်ရန်အတွက် **Off (not recommended)** ကိုရွေးချယ်ပြီး **OK** buttonတွင် click တစ်ချက်နှိပ်လိုက်ပါ။ ဒါဆိုရင် windows မှာပါတဲ့ built-in firewall ကို ပိတ်ပြီးဖြစ်ပါလိမ့်မယ်။

ZoneAlarm Personal Firewall

ယနေ့အချိန်မှာတော့ firewall အသုံးပြုမှုဟာ များစွာတွင်ကျယ်လာတာနှင့်အမျှ Macfee personal firewall ၊ ZoneAlarm ၊ Norton Internet Security ၊Outpost personal firewall စသည်ဖြင့်များစွာပေါ်ထွက်လာလျက်ရှိနေပါတယ်။ အဲဒီများစွာထဲက အမည်ကျော်ကြားလူသုံးများသလို ထိရောက်တဲ့ကာကွယ်မှုကိုပေးနိုင်စွမ်းသော ZoneAlarm firewall အသုံးပြုပုံများကိုတင်ပြသွားမှာဖြစ်ပါတယ်။ZoneAlarm firewall တွင် protection level မတူညီမှုပေါ်မူတည်၍ free versionတစ်မျိုးနှင့် Pro versionဟူ၍ရှိပါတယ်။ free versionကို **http://www.zonealarm.com** သို့သွားရောက်ပြီး ညွှန်ကြားချက်များအတိုင်းတစ်ဆင့်ပြီးတစ်ဆင့်သွားရောက်၍ download လုပ်ယူအသုံးပြုနိုင်ပါတယ်။ free versionကတော့ Trial အမျိုးအစားဖြစ်ပါတယ်။ ၁၅ရက် စမ်းသပ်အသုံးပြုခွင့်ရပါမယ်။ ရက်ပြည့်သွားရင် ဝယ်ယူမှသာ ဆက်လက်အသုံးပြုခွင့်ရမှာဖြစ်ပါတယ်။

Download ZoneAlarm

Zone alarm အားdownload ရယူရန် www.zonealarm.com သို့သွားပါ။ထို့နောက် **Download & Buy** တွင် click နှိပ်ပြီးညွှန်ကြားချက်များအတိုင်းတစ်ဆင့်ပြီးတစ်ဆင့်သွားရောက်၍ download လုပ်ယူလိုက်ပါ။

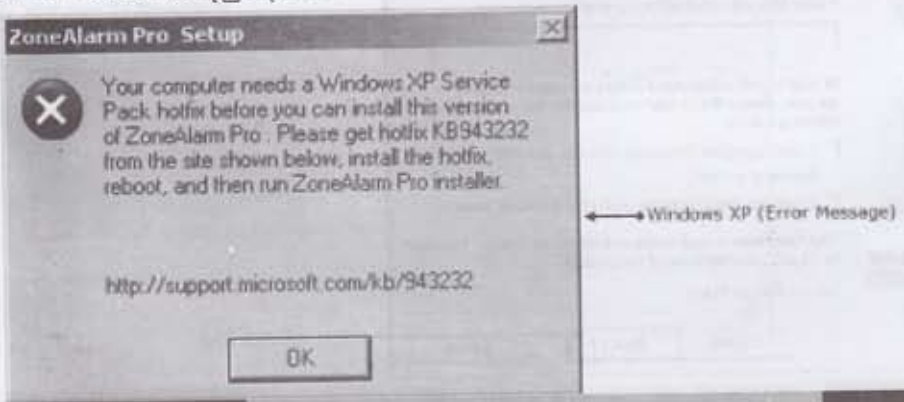


Install လုပ်ဖို့ရန်လိုအပ်ချက်များ

Zone Alarm ကို install မလုပ်ခင်မိမိတို့ကွန်ပျူတာမှာအသုံးပြုထားသော OS ပေါ်မူတည်ပြီး ကြိုတင်ပြင်ဆင်ထားရမှာတွေရှိပါတယ်။

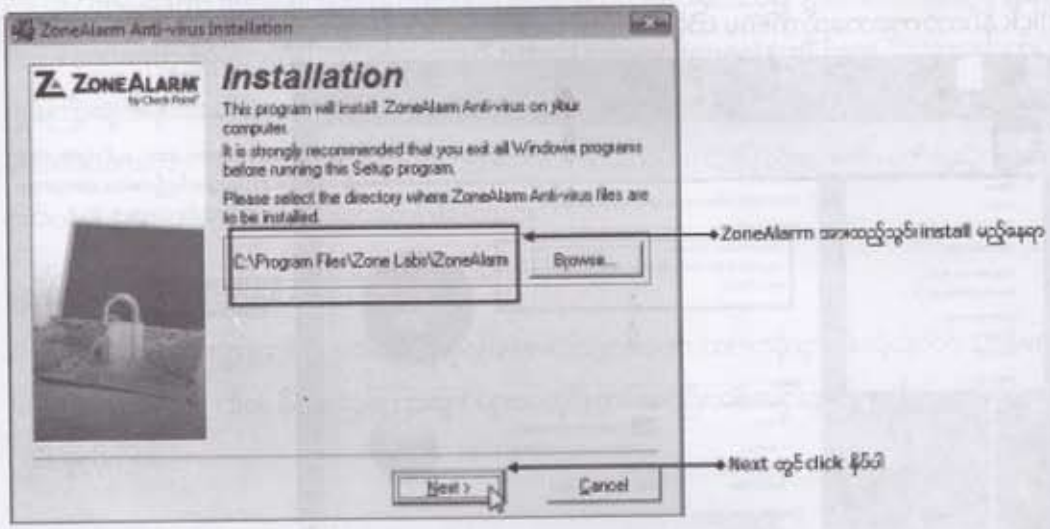
A) Windows Vista အသုံးပြုထားပါက အနည်းဆုံး service pack1 တင်ထားပြီးသားဖြစ်ရပါမယ်။ service pack1 တင်ပြီးသားဟုတ်မဟုတ်ဆိုတာကို Desktop ပေါ်ရှိ Computer icon ပေါ်တွင် right click နှိပ်ကာ ကျလာမည့် menu ထဲရှိ **Properties** တွင် click နှိပ်၍ကြည့်နိုင်ပါတယ်။

B) Windows XP အသုံးပြုထားပါက Security patch တစ်ခုဖြစ်တဲ့ KB943232 ကို run ထားပြီးသားဖြစ်ရပါမယ်။မရှိသေးပါက http://support.microsoft.com/kb/943232 သို့သွားရောက်ကာ download ရယူနိုင်ပါတယ်။ ၄င်း patch ကိုမ run ရသေးပဲ Zone Alarm တင်မည်ဆိုပါက အောက်ဖေါ်ပြပါ error message ကိုမြင်ရပါမယ်။

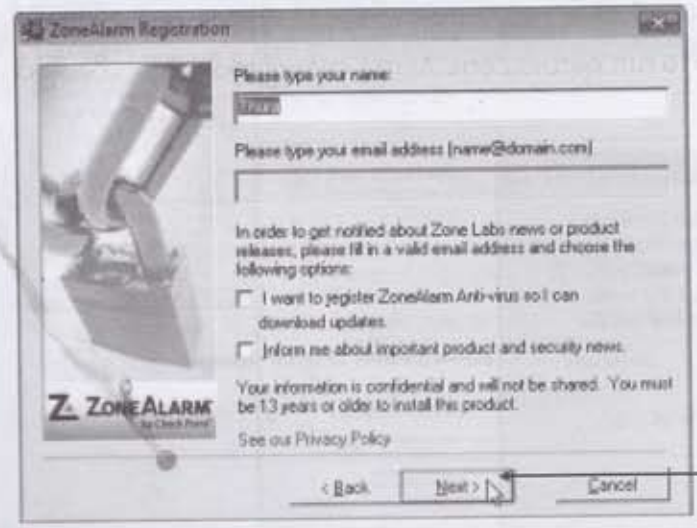


Zone Alarm Installation

1) Zone Alarmကို download ရယူပြီးသွားတဲ့အခါ installလုပ်ဖို့ရန် double click နှိပ်ပြီး run လိုက်ပါ။ Programအတွက်လိုအပ်သော file များအားထည့်သွင်းထားမည့်နေရာကိုအလိုလျောက်ရွေးချယ်ညွှန်ကြားထားပါလိမ့်မယ်။ **Next** တွင် click နှိပ်လိုက်ပါ။ User informationထည့်သွင်းပြီး register လုပ်ဖို့ရန်တောင်းဆိုပါလိမ့်မယ်။



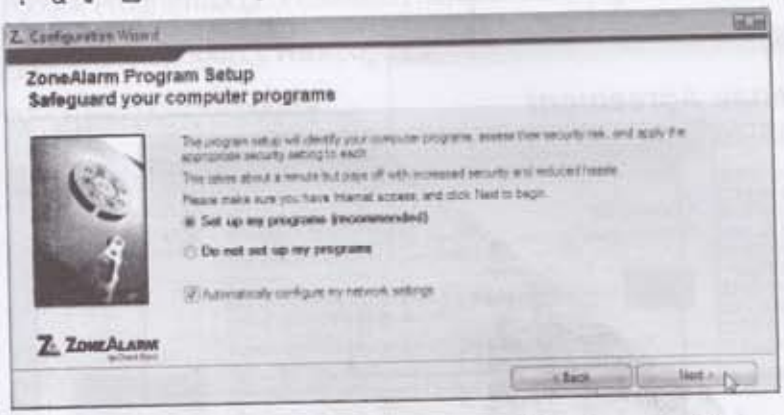
2)အမည်နှင့် emailလိပ်စာတစ်ခုဖြည့်စွက်ပေးလျှင် product သစ်ထွက်တိုင်းemail ဖြင့်အသိပေးပါလိမ့်မယ်။ Register မလုပ်လိုက checkbox များကို uncheck ☐ လုပ်ပြီး **Next** တွင် click တစ်ချက်နှိပ်ပါ။ license agreement ကိုသဘောတူလက်ခံခြင်းရှိမရှိမေးပါလိမ့်မယ်။



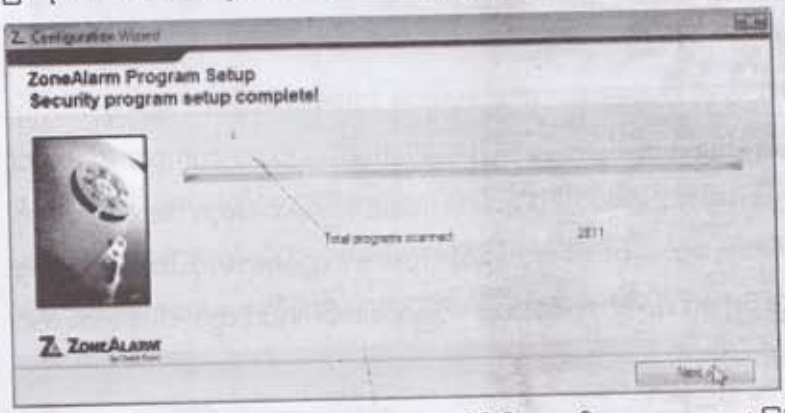
3) ထုံးစံအတိုင်း license agreement ကို သဘောတူလက်ခံပေးရပါမယ်။ license agreement ဘေးရှိ check box ☑ ထဲတွင် အမှန်ခြစ်ပေါ်အောင် clickတစ်ချက်နှိပ်ပါ။Installတွင် clickနှိပ်ပါက တောင် Installပါလိမ့်မယ်။

4) အခြားသော software အတော်များများမှာ destination folder ထဲသို့ file များကူးထည့်ပြီး လိုအပ်သော component များInstall ပြီးသွားတဲ့အခါ Installation ကရုတ်ဟာ complete ဖြစ်သွားတတ်ပါတယ်။ဒါပေမယ့် Zone Alarm မှာတော့ complete setup မဖြစ်သေးပါဘူး။ settingအချို့ကို configure လုပ်ပေးရပါဦးမယ်။ ခက်ခက်ခဲခဲတော့ configure လုပ်စရာမလိုပါဘူး။ joining DefenseNetတို့၊ Activate Smart defense Advisor တို့ဖြစ်ပါတယ်။ **Next** တွင် clickတစ်ချက်စီ နှိပ်သွားပါ။ Program setup သို့ရောက်ပါလိမ့်မယ်။

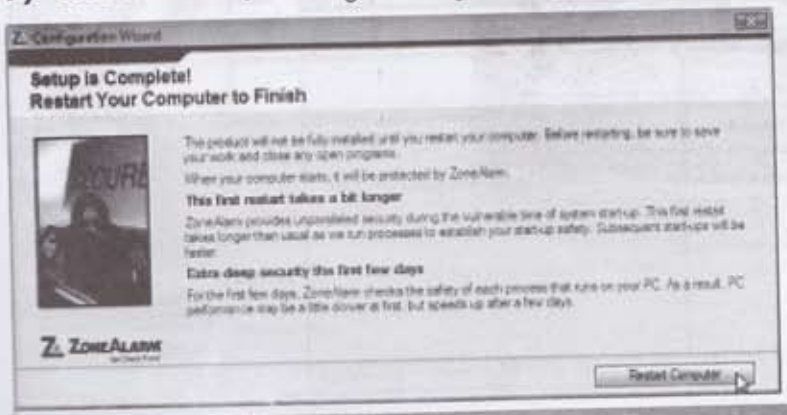
5) ဒီအဆင့်မှာဆိုရင် ကွန်ပျူတာမှာ installလုပ်ထားသော programများအားစစ်ဆေးပြီးသင့်လျော်သော permissionများပေးကာ ZoneAlarm မှ setupလုပ်မှာဖြစ်ပါတယ်။ သူ့အတိုင်း Setup my programs ကိုရွေးချယ်ပြီး **Next**တွင် clickနှိပ်လိုက်ပါ။ စတင်စစ်ဆေး setupလုပ်ပါမည်။



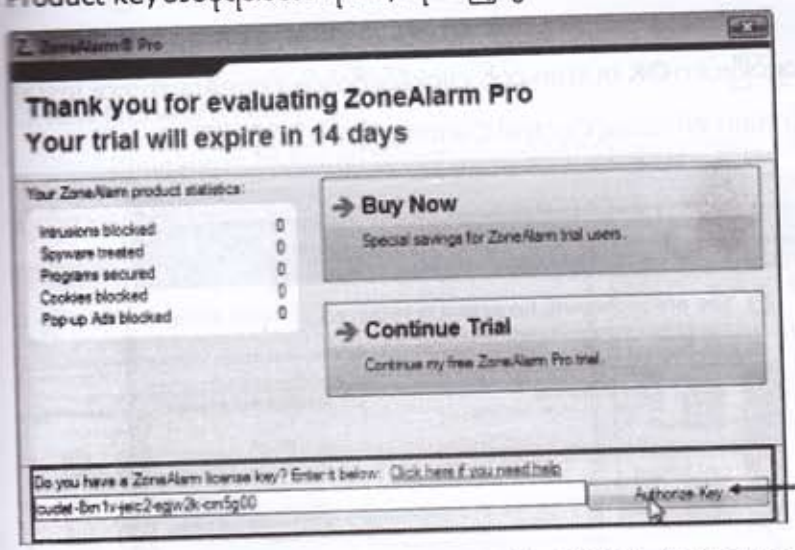
6) ပြီးလျှင် program ဘယ်နှစ်ခုကိုစစ်ဆေးတွေ့ရှိပြီး setupလုပ်ပြီးကြောင်းဖေါ်ပြသော Wizard ကို မြင်ရပါမယ်။ **Next** တွင် clickနှိပ်ပါက ကွန်ပျူတာအား restart လုပ်ခိုင်းပါလိမ့်မယ်။



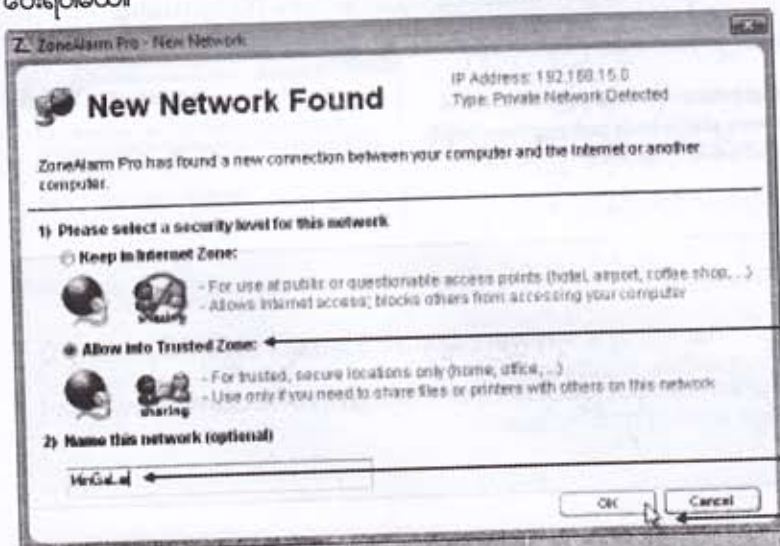
7) **Restart Computer** တွင် click နှိပ်ပါက ကွန်ပျူတာ restart ဖြစ်သွားပါမည်။



8) Rebootလုပ်ပြီး စက်ပြန်တက်လာတဲ့အခါ trialအနေနှင့် စမ်းသပ်သုံးမှာလား၊ ဝယ်ယူအသုံးပြုမှာလား ဆိုတဲ့ ရွေးစရာ Option နှစ်ခုပါတဲ့ Wizardသည်အလိုအလျောက်ပွင့်လာပါမယ်။ trialအနေနှင့် သုံးမည် ဆိုပါက ၁၅ရက်စမ်းသပ်အသုံးပြုခွင့်ရမှာဖြစ်ပါတယ်။အဲဒီ၁၅ရက်ထက် ကျော်လွန်အသုံးပြုလိုပါက ဝယ်ယူရ မှာဖြစ်ပါတယ်။ ဝယ်ယူမယ်ဆိုရင် ရှေ့က Kaspersky Antivirus မှာကဲ့သို့ပင် ZoneAlarm အတွက် Product key တစ်ခုရပါမယ်။ ထို key ကို ထည့်သွင်းကာ activate လုပ်ပေးရပါမယ်။



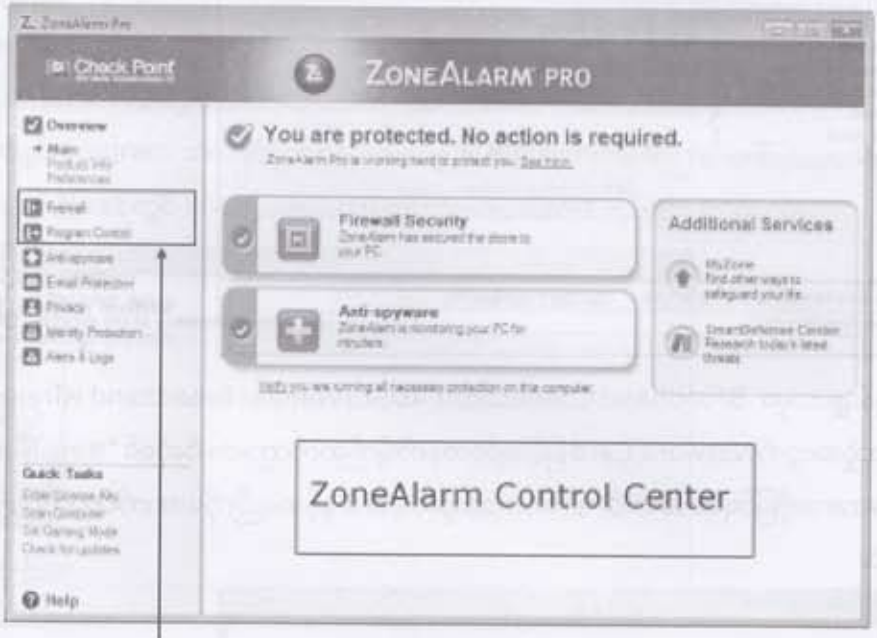
9) မိမိကွန်ပျူတာမှာ Broadband Connection (ADSL၊ Wimax၊ Broadband wireless) ကို အသုံးပြုသည့်အတွက် Network Card ဖြင့်အင်တာနက်ချိတ်ဆက်ထားတယ်ဆိုရင် "New Network Found"Wizardကိုမြင်ရပါမယ်။ အဲဒီ networkအတွက် Zoneနှင့်အမည်ကို အောက်ပါအတိုင်းရွေးချယ် ပေးရပါမယ်။



a) မိမိရဲ့Networkကို Trusted zoneအတွင်းသို့ထည့်သွင်းထားရပါမယ်။ Keep in internet zone ဘေးရှိ radio button ကို ⊙ ဖြစ်အောင် clickနှိပ်ပါ။

b) Network အတွက် အမည်တစ်ခုပေးလိုက ပေးနိုင်ပါတယ်။ defaultအားဖြင့် **New Network** ဆိုတဲ့အမည်ဖြစ်ပါတယ်။မိမိနှစ်သက်ရာအမည်ပေးလိုက New networkကိုဖျက်ပြီး အမည်တစ်ခု ရိုက်ထည့်ပါ။

10) Zoneနှင့်အမည်ရွေးချယ်ပြီးပါက **OK** button တွင် clickနှိပ်လိုက်ပါ။ ZoneAlarmအား install လုပ်ခြင်းလုံးဝပြီးဆုံးသွားပြီး Main Window(Control Center)ပွင့်လာပါလိမ့်မယ်။



Firewall နှင့် Program Control သည် ZoneAlarm ၏ အဓိက feature နှစ်ခုဖြစ်ပါတယ်။ အသင် အထွက်သားလုံးတို့ကို ဒီနေရာကနေ control လုပ်နိုင်ပါတယ်

➲Outpost Personal Firewall

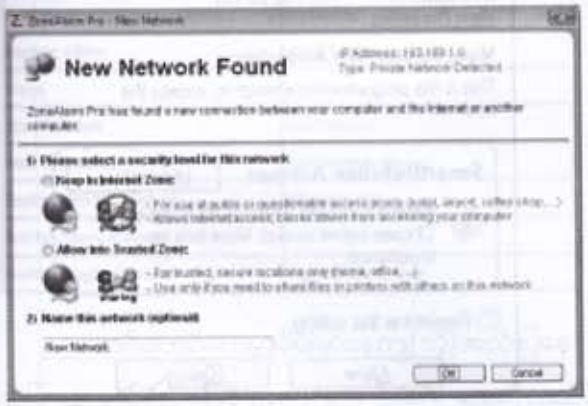
Zonealarm ကဲ့သို့ hacker များ၊ spyware များ၊ adware များ အန္တရာယ်မှ ကာကွယ်ပေးနိုင်သော firewall program တစ်ခုပင်ဖြစ်ပါတယ်။ **www.agnitum.com**မှ download ရယူနိုင်ကြပါတယ်။

Zonealarm Alerts

Zonealarm ကို install လုပ်ပြီးသွားတဲ့အခါမှာ pop-up များကဲ့သို့ alerts များကိုမကြာခဏတွေ့ရမှာဖြစ်ပါတယ်။ ဒီ alert များကို နိုင်နိုင်နင်းနင်းကိုင်တွယ်ဖြေရှင်းနိုင်ဖို့ လိုပါတယ်။ သို့မှသာမိမိရဲ့ security ကိုအပြည့်အဝကာကွယ်နိုင်ပါလိမ့်မယ်။ Alert များကို အခြေခံအားဖြင့် အမျိုးအစား၃မျိုး အဖြစ်ခွဲခြမ်းစိတ်ဖြာလေ့လာနိုင်ပါတယ်။အဲဒီအမျိုးအစားများကတော့ new network alert၊ information alert နှင့် program alertတို့ပဲဖြစ်ပါတယ်။

❑New Network Alert

Zonealarm ကို install လုပ်ထားသောမိမိရဲ့ကွန်ပျူတာကိုအခြားသော network တစ်ခုခုဖြင့်ချိတ်ဆက်လိုက်တဲ့အခါမျိုးမှာဒီ new network alert ကိုတွေ့ရပါလိမ့်မည်။

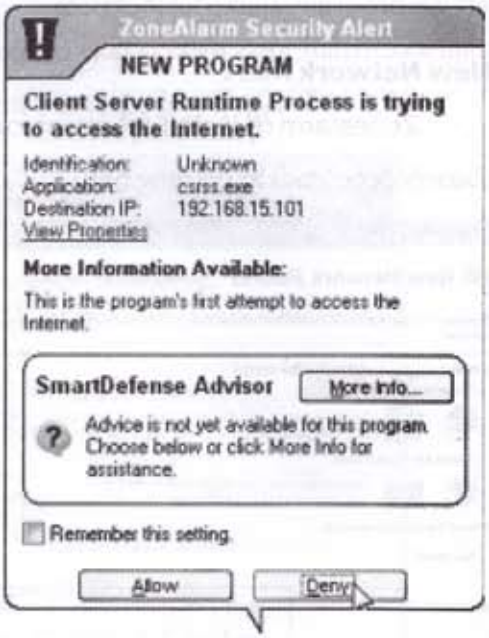


❑Information Alert

Information alertများသည်zonealarmတွင်မိမိကန့်သတ်ထားသော security setting နှင့်ကိုက်ညီမှုမရှိသော(သို့)ဘောင်ကျော်သော communicate လုပ်မှုများ ကို zonealarm မှတားဆီး ပိတ်ဆို့ထားသောကြောင့်မိမိအားအသိပေးသော Alertများပဲဖြစ်ပါတယ်။ ထို alert များနှင့် ပတ်သက်၍မိမိဘက်မှ ဆုံးဖြတ် ချက် ဘာမှပေးစရာမလိုပါဘူး။ ဒါကြောင့် **OK** button တွင် click တစ်ချက်နှိပ်ပြီး ထို information alert များကို ပိတ်လိုက်ရုံပဲဖြစ်ပါတယ်။ ဒါမျိုးတွေကို နောက်ပိုင်းမှာမပြန့်လို့ပိတ်ထားချင်ရင် don't show တွင် ☑ အမှန်ခြစ်ပေါ်အောင် click နှိပ်ခဲ့ပါ။

❑Program Alert

Program Alert များဟာ information alert များကဲ့သို့အသိပေးရုံသက်သက်မဟုတ်တော့ဘဲ မိမိမှဆုံးဖြတ်ပေးရမှာဖြစ်ပါတယ်။ မိမိရဲ့ကွန်ပျူတာထဲမှprogramတစ်ခုဟာ Internet(သို့)networkထဲက အခြားကွန်ပျူတာတစ်လုံးဆီသို့ accessလုပ်တဲ့အခါမျိုးမှာ program alert ပေါ်လာပြီးထို program အား ပြင်ပသို့ accessလုပ်ခွင့်ပြုမပြုဆိုတာကို မိမိအားမေးပါလိမ့်မည်။

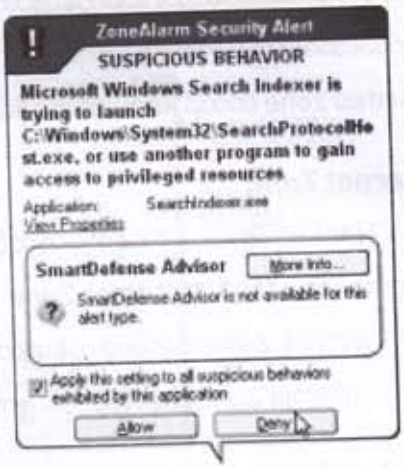


Yes ၊ No အဖြေနှစ်ခုထဲမှတစ်ခုခုကို ရွေးချယ်ပြန်လည်ဖြေကြားပေးရမှာဖြစ်ပါတယ်။ Allowတွင် click တစ်ချက်နှိပ်ပါက ထို program အား access လုပ်မှာဖြစ်ပြီး Denyတွက် click တစ်ချက်နှိပ်ပါက access လုပ်ခွင့်မပေးဘဲ zonealarm မှတားဆီးထားမှာဖြစ်ပါတယ်။ ဒါကြောင့် program alert ပေါ်တိုင်း access လုပ်ခွင့်တောင်းတဲ့ထို program ဟာ မိမိအမှန်တကယ်အသုံးပြုဖို့ရန်လိုအပ်သော program ဟုတ်မဟုတ်ဆိုတာကို သေသေချာချာစိစစ်ဖို့ လိုပါတယ်။ အဲဒီလိုစိစစ်ဖို့ရန်ထိုprogram များရဲ့ Run လုပ်နိုင်သော executable fileအမည်များကိုသိထားရပါမယ်။

ဆိုရရင် outlook express ကိုအသုံးပြုပြီး email ပို့လွှတ်တယ် ဆိုပါစို့ အဲဒီပို့လွှတ်တဲ့အခါမှာ program alert ပေါ်လာပြီးထို alertထဲရှိapplicationမှာ msimn.exe ဆိုတဲ့ file အမည်ကိုတွေ့ရမှာ ဖြစ်ပါတယ်။msimn.exe ကိုတွေ့တာနဲ့ outlook express မှန်းသိပြီး Allowတွင် click တစ်ချက်နှိပ်၍ ခွင့်ပြုမှသာလျှင် emailပို့လွှတ်နိုင်မှာဖြစ်ပါတယ်။အကယ်၍ Denyတွင် click နှိပ်မိပါက outlook express programအား zonealarm မှတားဆီးပိတ်ဆို့ထား၍ email ပို့လွှတ်နိုင်မယ်မဟုတ်ပါ။ဒါကြောင့် exe file

တစ်ခုကိုမြင်တာနှင့်ထို exe file ကဘယ် program နှင့်သက်ဆိုင်သလဲဆိုတာကိုခွဲခြားသိနိုင်ဖို့လိုပါတယ်။ သတ်တလော ခွဲခြား မသိနိုင်သေးရင်လည်း စိုးရိမ်ဖို့မလိုပါဘူး zonealarm ကို အသုံးပြုမှုအလေ့အကျင့် ရလာတာနှင့်အမျှအလိုလိုသိလာနိုင်ပါတယ်။

VLC Player	vlc.exe
Adobe Acrobat	acrobat.exe
Avira Antivirus	avcenter.exe, avnotify.exe , avgnt.exe
Mozilla Firefox	firefox.exe
Google Chrome Browser	chrome.exe
Internet Download Manager	idman.exe
Java	javaw.exe
Nero Burning Rom	nero.exe
Outlook Express Backup	Dwbackup.exe
Real Player	replay.exe
Registry Editor	regedit.exe
Skype	skype.exe
Your Freedom	freedom.exe
Your Uninstaller	yui2008setup.exe
SpyBot Search & Destory	sdupdate.exe
Realtek Sound Manager	soundman.exe
Uniblue Registry Booster	registrybooster.exe



တစ်ခါတစ်လေမှာမိမိမြင်နေကျ(သို့)အသုံးပြုနေကျနာမည်မဟုတ်ဘဲapplication ခွဲခြားရခက်တဲ့ အခြားနာမည်တစ်ခုဖြင့် program alert များကိုလည်းတွေ့ရနိုင်ပါတယ်။အဲဒီလို file အမည်များကို adware (သို့) spyware တို့မိမိကွန်ပျူတာအတွင်းရှိ information များကို အင်တာနက် connection မှတဆင့်ပြင်ပသို့ပို့လွှတ်တဲ့အခါမျိုးမှာကြုံတွေ့နိုင်ပါတယ်။ထို adware များကို Deny button တွင် click နှိပ်၍တားဆီးပိတ်ဆို့ထားနိုင်ပါတယ်။ဒါပေမယ့် ထို program ဟာနောက်တစ်ကြိမ်ထပ် run တဲ့ အခါမျိုးမှာ program alert များထပ်မံထွက်ပေါ်လာမှာဖြစ်ပါတယ်။အကယ်၍ Remember this answer ဘေးရှိcheckbox တွင် ☑ အမှန်ပေါ်အောင် selectလုပ်ပြီး Denyတွင် click တစ်ချက်နှိပ်ပါကထို programအလုပ်လုပ်သည့်အခါတိုင်း ZoneAlarm သည်မိမိထံမှခွင့်ပြုချက်တောင်းသော program alert များမထုတ်ပေးတော့ဘဲအလိုအလျောက်တားဆီးပိတ်ဆို့ထားမှာဖြစ်ပါတယ်။

ဒီနေရာမှာတစ်ခုပြောဖို့ရှိတာကတော့ access လုပ်ခွင့်ပြုသင့်သော program များကိုတားဆီးမိခြင်း၊ access လုပ်ခွင့်မပြုသင့်သော program များကိုခွင့်ပြုမိခြင်းအစရှိသောအမှားအယွင်းပြဿနာများ ရှိလာနိုင်သည်။ အဲဒီလိုအခါမျိုးမှာ ZoneAlarm control centre ရှိ program control တွင် program များအား access ပြုခွင့်၊ မပြုခွင့်များကိုပြန်လည် edit လုပ်နိုင်ပါတယ်။

Firewall Panel

ZoneAlarm personal firewall သည် အွန်လာရယ်ပေးနိုင်သော traffic ကို internet zone၊ trusted zone ဟူ၍ zoneများပိုင်းခြားပြီး ကာကွယ်ပေးပါတယ်။ အဓိကက မိမိကွန်ပျူတာနှင့် အခြားကွန်ပျူတာတစ်လုံးတို့ communicate လုပ်တဲ့နေရာမှာ တစ်ဖက်ကွန်ပျူတာသည် ဘယ် zone ထဲမှာရှိနေသလဲဆိုတာ အရေးပါပါတယ်။ အဲဒီကွန်ပျူတာ ရှိနေသော zone ပေါ်မူတည်ပြီးလုပ်နိုင်တာတွေ မတူဘဲကွဲပါတယ်။ အရေးကြီးတာက ဘယ်ကွန်ပျူတာတွေကို internet zone ၊ ဘယ်ကွန်ပျူတာတွေ ကိုတော့ ဖြင့် trusted zone ထဲထည့်ထားမယ် အစရှိသဖြင့်စနစ်တကျစီမံခန့်ခွဲပေးဖို့လိုအပ်ပါတယ်။

❑Internet Zone

Hacker များ အင်တာနက်မှတဆင့် မိမိကွန်ပျူတာအတွင်းဝင်ရောက်နှောင့်ယှက်ခြင်းများမှ အကာအကွယ်ပေးနိုင်ရန် "Internet Zone" security ကို အမြင့်ဆုံးထားပေးလေ့ရှိပါတယ်။အကြမ်းဆိုရရင် Internet Zoneထဲမှာရှိတဲ့ ကွန်ပျူတာတွေသည် မိမိမသိနိုင်သော ကွန်ပျူတာများဖြစ် ပါတယ်။ ဒါကြောင့် Internet Zone ထဲမှာရှိတဲ့ကွန်ပျူတာတွေနှင့် file sharing ၊ printer sharing တို့လုပ်မရပါ။

❑Trusted Zone

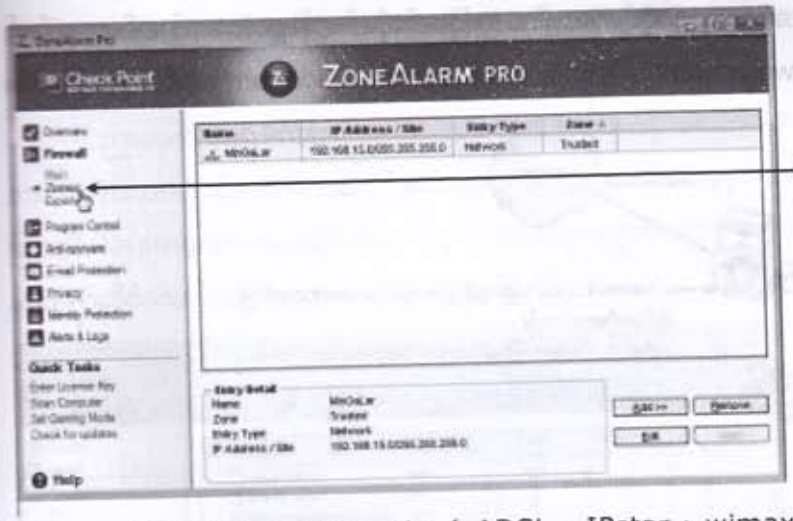
Trusted zone ထဲမှာရှိသော ကွန်ပျူတာများနှင့် file တို့ printer တို့ကို share လုပ်သုံးနိုင်တယ်။ ဒါက Internet နှင့် Trusted တို့ရဲ့အဓိကကွာခြားချက်ဖြစ်တယ်။ ဒါကြောင့် local network(home , office) ချိတ်ဆက်ထားသူတို့အနေနှင့် မိမိ network ကို trusted ထဲထားရမယ်။ သို့မှသာ network ထဲမှာရှိသောအခြားကွန်ပျူတာများနှင့် share လုပ်လို့ရမယ်။သဘောက trusted ထဲမှာရှိသော ကွန်ပျူတာတွေသည်မိမိယုံကြည်စိတ်ချရသော ကွန်ပျူတာများဖြစ်သည်ဆိုတဲ့ သဘောပင်ဖြစ်ပါတယ်။

trusted zone သည်လည်း Internet zone လောက် security မမြင့်ပေမယ့် မိမိကွန်ပျူတာတွင်းဝင်ရောက်ခြင်းများကိုကာကွယ်ပေးနိုင်ပါတယ်။ အကယ်၍များ network ထဲက ကွန်ပျူတာတစ်လုံးလုံးကနေ virus တွေ ၊ trojan တွေထွက်နေရင် အဲဒီကွန်ပျူတာတစ်လုံးတည်းကိုရွေးပြီး Internet zone ထဲသို့ ခေတ္တပို့ထားလို့ရတယ်။ ဒါဆိုရင်မိမိနှင့် network ထဲက အခြားကျန်ကွန်ပျူတာ များနှင့် share လုပ်သုံးလို့ရချိန်တွင် အဲဒီကွန်ပျူတာနှင့်တော့ ဘာမှ share လုပ်လို့ရနိုင်မည်မဟုတ်ပါ။ virus တွေ trojan တွေရှင်းပြီးသည့်နောက်ပိုင်းစိတ်ချရပြီဆိုတော့မှ trusted ထဲပြန်ပြောင်းထည့်သွင်းပေးနိုင်ပါတယ်။

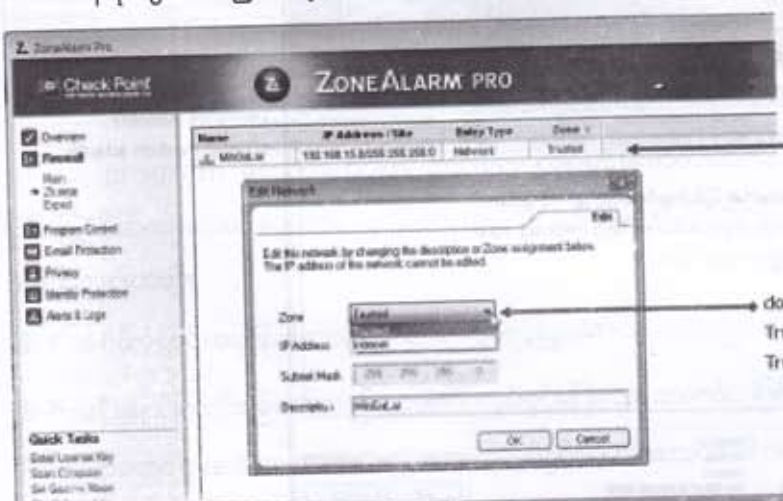
အဲဒီလို zone management တွေလုပ်ရန်အတွက် Internet zone ၊ Trusted zone တွေ အကြောင်းကို နားလည်ထားရပါမယ်။ သို့မှသာ ဘယ်ဟာတွေကို ဘယ် zone ထဲထားသင့်တယ်ဆိုတာမျိုးတွေကို ဆုံးဖြတ်နိုင်ကြပါလိမ့်မယ်။

How to define zone

Firewall panel ၏ဘယ်ဘက်ခြမ်းရှိ firewall အောက်မှ Zones tab တွင် click တစ်ချက်နှိပ်ပါ။ ညာဘက်ခြမ်းထဲတွင် zonealarm အား install လုပ်စဉ်အခါတုန်းက ထည့်သွင်းထားခဲ့သော မိမိ network နှင့်သက်ဆိုင်သော အမည်၊ IP address ၊ Zone အစရှိသော information များကိုမြင်ရပါမယ်။ detect လုပ်၍ရသော traffic source(IP address ၊ Subnet) များကို တွေ့ရပါမည်။

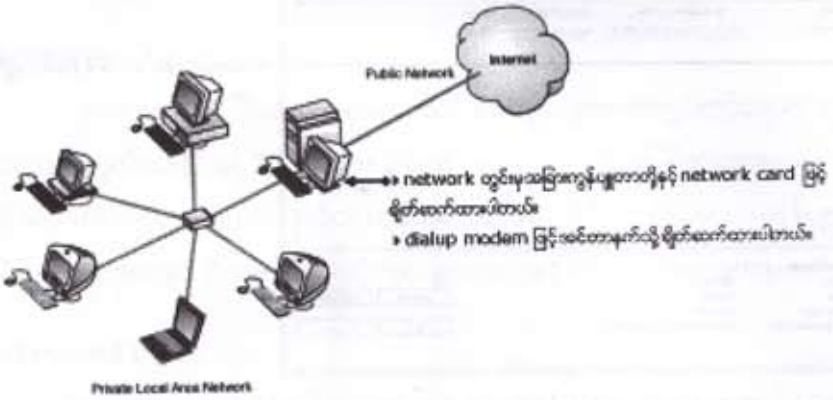


Broadband connection(ADSL ၊ IPstar ၊ wimax)ကိုအသုံးပြု၍ ကွန်ပျူတာတစ်လုံးတည်းဖြင့် သာ အင်တာနက်သို့ ချိတ်ဆက်အသုံးပြုသူများသည် Network ကို internet zone မှာထည့်သွင်းထားသင့် ပါတယ်။zone ပြောင်းပုံကိုကြည့်ရအောင်။ Network အား Trused မှ Internet zone သို့ပြောင်းရန် Network ပေါ်တွင် double click နှိပ်ပါ။ Edit Network box ကျလာပါမည်။ zone နေရာတွင် မိမိပြောင်းလိုသော zone ကို ရွေးပေးပါ (ဥပမာ - Internet zone)

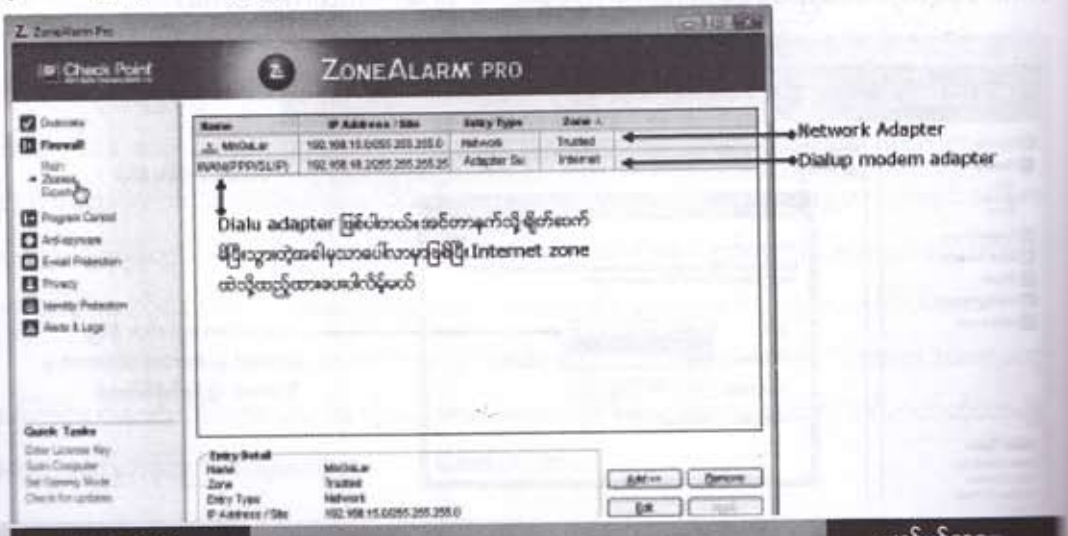


အခြားမည်သည့်ကွန်ပျူတာများနှင့်မှ network ချိတ်ဆက်ထားခြင်းမရှိဘဲ dialup connection ဖြင့်အင်တာနက်ချိတ်ဆက်သောကွန်ပျူတာများတွင်အင်တာနက်သို့ချိတ်ဆက်မိသွားတဲ့အခါမှာတော့ dialup adapter ကို internet zone ထဲအလိုအလျောက်ထည့်သွင်းပေးထားမှာဖြစ်သည့်အတွက်အခြားဘယ် zone ကိုမှပြောင်းစရာမလိုပါဘူး။

သို့သော်အောက်ပါပုံအတိုင်းအခြားကွန်ပျူတာတိုနှင့်လည်းnetwork ချိတ်ထားမယ်၊ dial-up connection ဖြင့်လည်းအင်တာနက်သို့ချိတ်ဆက်အသုံးပြုမယ်ဆိုရင်ကွန်ပျူတာသည် အင်တာနက်နှင့်ချိတ်မိပြီးသွားတဲ့အခါ network adapter နှင့် dial-up adapterဟူ၍adapter ၂မျိုးရှိလာပါလိမ့်မယ်။



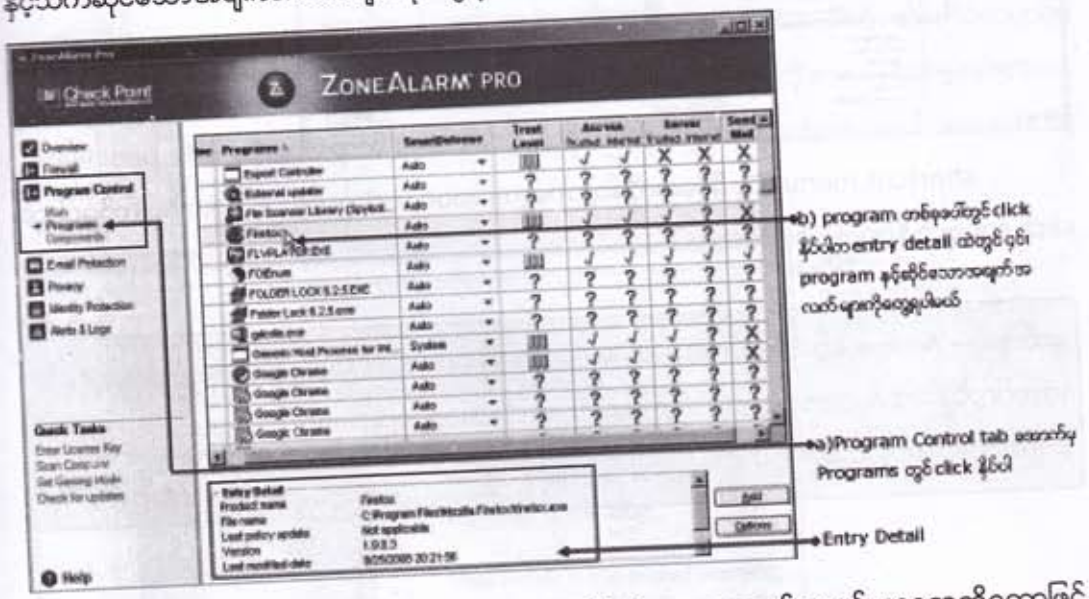
အဲဒီလိုအခါမျိုးမှာ မိမိရဲ့ကွန်ပျူတာ၏ network adapter ကို local network အတွင်းရှိအခြားသောကွန်ပျူတာများနှင့် file များ၊ printer များ၊ program များအား shareလုပ်၍အသုံးပြုနိုင်ရန် intenet zone မှ trusted zone သို့ပြောင်းပေးရပါမယ်။ dial-up adapter ကိုမူ internet zone မှာပင်ထည့်သွင်းထားရမှာဖြစ်ပါတယ်။



Program Control Panel

Program Control တွင် program များအား access ပြုခွင့်၊ မပြုခွင့်များကို edit လုပ်နိုင်ပါတယ်။ ဆိုရရင် access လုပ်ခွင့်ပြုသင့်သော program များကိုတားဆီးမိခြင်း၊ access လုပ်ခွင့်မပြုသင့်သော programများကိုခွင့်ပြုမိခြင်း အစရှိသောအမှားအယွင်းပြဿနာများကို ပြန်လည်ပြင်ဆင်နိုင် ကြပါတယ်။ zonealarm ၏ **Program control** တွင် click တစ်ချက်နှိပ်ပါက Program control ၏ main tab ထဲသို့ရောက်သွားပါမည်။

ညာဘက်ခြမ်းရှိ Programs tab တွင် click တစ်ချက်နှိပ်ပါ။ ZoneAlarm မှ detect လုပ်ထားသော Network (သို့) Internet သို့ access လုပ်ဖို့ရန် ခွင့်တောင်းခဲ့ဖူးသော program များရဲ့ list ကို မြင်ရပါမယ်။ program အမည်တစ်ခုပေါ်တွင် click နှိပ်ကြည့်ပါက entry detail ထဲတွင် ၄င်း program နှင့်သက်ဆိုင်သော အချက်အလက်များကိုတွေ့ရပါမယ်။



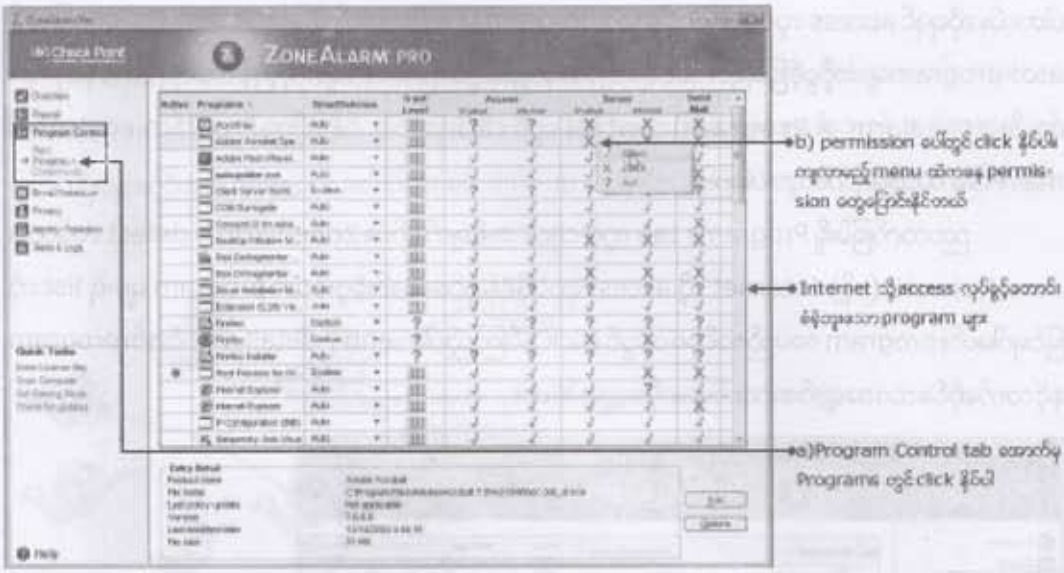
program တွေကိုတော့ဖြင့် access လုပ်ခွင့်ပေးထားတယ်၊ ဘယ်ဟာတွေကိုတော့ဖြင့် ခွင့်မပြုပဲဝိတ်ထားတယ် ဆိုတာတွေကို program တစ်ခုချင်းစီ ရဲ့ဘေးမှာ ✓ × ? သင်္ကေတတို့ဖြင့် ဖော်ပြထားပါတယ်။

◈ ✓ အစိမ်းရောင် အမှန်ခြစ်သည် access လုပ်ခွင့်ပြုသော သင်္ကေတဖြစ်ပါတယ်။

◈ × အနီရောင်ကြက်ခြေခတ်သည် access လုပ်ခွင့်မပြုသော သင်္ကေတဖြစ်ပါတယ်။

◈ ? အပြာရောင် question mark သည် accessလုပ်ခွင့်တောင်းသောအခါ program alertထုတ်ပေးမယ့် သင်္ကေတဖြစ်ပါတယ်။

Edit လုပ်လိုသော program ရှိ **permission** သင်္ကေတပေါ်တွင် click တစ်ချက် နှိပ်လိုက်ပါ။ shortcut menu ကျလာပါမည်။



shortcut menu ထဲမှ မိမိပေးလိုသော permission သင်္ကေတ (✓ × ?) တို့ပေါ်တွင် click တစ်ချက် နှိပ်၍ပြောင်းနိုင်ပါတယ်။

မှတ်ချက် - Access နှင့် Server ဟူ၍ permission ၂မျိုးရှိပါတယ် Program အတော်များများပုံမှန် အလုပ်လုပ်နိုင်ရန် access permission ပေးနိုင်ပါတယ်။ အထူးသဖြင့် internet zone တွင် server permission ပေးခြင်းများကို တတ်နိုင်သမျှရှောင်ရှားဖို့လိုပါတယ်။

MailWasher (Anti Spam Software)

MailWasherသည် virus များ၊ spamများအစရှိသော မလိုလားအပ်သည့် emailများမိမိတို့၏ ကွန်ပျူတာ ထဲသို့ မဝင်ရောက်မီ first line defence အဖြစ်ကာကွယ်တားဆီးပေးနိုင်သော program တစ်ခုပင် ဖြစ်ပါတယ်။ MailWasherရဲ့လုပ်ဆောင်မှုကတော့ မိမိတို့အသုံးပြုနေကျ email programများ ဖြစ်ကြသည့် Outlook Express programတို့နှင့်များစွာကွာခြားခြင်းမရှိပါဘူး။ email programများသည် mailserverနှင့်ချိတ်ဆက်လုပ်ဆောင်သကဲ့သို့ပင် MailWasherသည်လည်း email serverဖြင့်ဆက်သွယ် လုပ်ဆောင်မှာဖြစ်ပါတယ်။

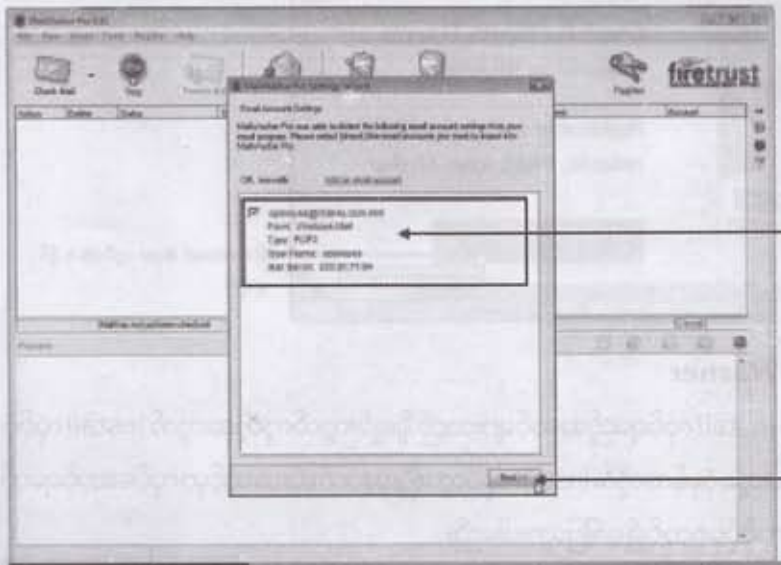
MailWasherရဲ့အဓိကထူးခြားချက်ကတော့ email program များကဲ့သို့ email များအားလုံးကို မိမိကွန်ပျူတာထဲသို့ရောက်အောင် downloadရယူပြီးမှ ဖတ်ရှုဖျက်ထုတ်နိုင်တာမျိုးမဟုတ်ဘဲ မလိုလား အပ်သော email များကို mailserver ပေါ်မှာပင် ဖတ်ရှုဖျက်ထုတ်နိုင်ခြင်းပင် ဖြစ်ပါတယ်။ နောက်တစ်ခု ထူးခြားချက်ကတော့ အချို့သော ပေးပို့သူများထံသို့ မိမိရဲ့လိပ်စာသည် အမှန်တကယ်မရှိသော လိပ်စာတစ်ခု အဖြစ် bounceလုပ်ပြီးပြန်လည်ပေးပို့နိုင်ပါတယ်။ MailWasher programကို www.mailwasher.net /download.php သို့သွားရောက် download ယူနိုင်သလို အခြားသော download website သို့ သွားရောက်ပြီးတော့လည်းရှာဖွေ download ရယူနိုင်ကြပါတယ်။

Configuring Mail Washer

MailWasherကို installလုပ်ရမည့်အဆင့်များသည် ရိုးရှင်းလွယ်ကူတဲ့အတွက် installလုပ်ပုံ အဆင့်ဆင့်ကို မဖေါ်ပြတော့ပါဘူး။ ပုံမှန်အတိုင်း installလုပ်သွားပြီးနောက်ဆုံးအဆင့်မှာ လုပ်ဆောင်ရမယ့် email account setup လုပ်ပုံမှစတင်၍ဖေါ်ပြသွားပါမည်။

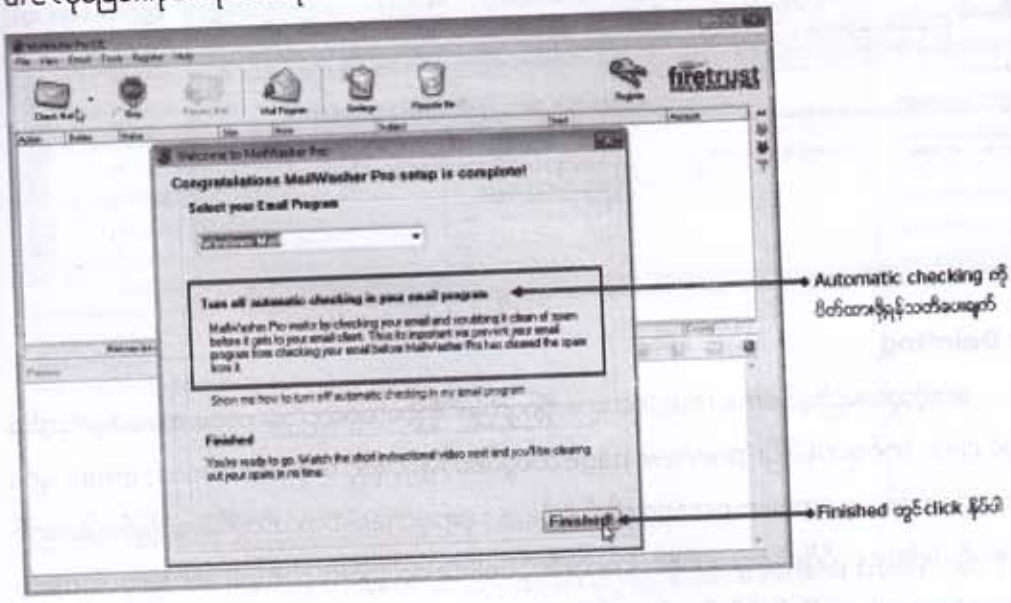
1) MailWasher ကိုပုံမှန်အတိုင်း install လုပ်ပြီးသွားပြီးပထမဦးဆုံးအကြိမ် run တဲ့အခါမှာ မိမိ email account နှင့် ပတ်သက်သော information များကို ထည့်သွင်းမည့်လုပ်ငန်းများကိုလုပ်ဆောင်ရန် wizard တစ်ခုကျလာပါမည်။ **Next**တွင် clickတစ်ချက်နှိပ်လိုက်ပါ။

2) MailWasher မှ အလိုအလျောက် ကူးယူထည့်သွင်း သွားမည့် Email account setting များကို ဖေါ်ပြထားပါလိမ့်မယ်။ ဒါ့အပြင် မူလ email program (Outlook Express၊ Windows mail) တို့၏ address book ထဲရှိ address အားလုံးတို့ကို friends list ထဲသို့အလိုအလျောက် ထည့်သွင်းပေးသွားပါလိမ့်မယ်။ MailWasher မှာ ဖေါ်ပြထားသော account setting များသည်ပြည့်စုံမှန်ကန်ပါက **Next** တွင် click တစ်ချက်နှိပ်ပါ။



3)Email account setting များထည့်သွင်းပြီးပါက mail washer တွင် account setup လုပ်ခြင်း ပြီးဆုံးသွားပြီဖြစ်ကြောင်းဖေါ်ပြသော message ပါရှိသည့် dialog box ကျလာပါမည်။ ဒီ box အတွင်းမှာ အသုံးပြုသူရဲ့ email program အတွင်းရှိ automatic checking ကို turn off လုပ်ပြစ်ဖို့ရန် သတိပေးချက် ပါဝင်ပါတယ်။

ဘာဖြစ်လို့လဲဆိုတော့ automatic checking ကို on ထားမယ်ဆိုပါက email program ဖွင့်သည် နှင့်တစ်ပြိုင်နက် email ပို့လွှတ်ရယူခြင်းများကို အလိုအလျောက်လုပ်ဆောင်သွားမှာ ဖြစ်သည့် အတွက် ကြောင့် တစ်ခါတစ်လေ mail washer ကို အရင်ဖွင့် မစစ်ဆေးရသေးခင် email program ကိုဖွင့်မိသည့် အခါ မျိုး မှာ email များအားလုံးကို download လုပ်ယူသွားနိုင်ပါတယ်။ အကယ်၍များ email ရယူခြင်းများကို MailWasher မှတစ်ဆင့်သာ အမြဲတမ်းသတိထားအသုံးပြုနိုင်မယ်ဆိုရင်တော့ automatic checking ကို ထည့်သွင်းစဉ်းစားစရာမလိုပါဘူး။ **Finish** button တွင် click တစ်ချက်နှိပ်ပြီး configure လုပ်ခြင်းကို အဆုံးသတ်နိုင်ပါတယ်။



Outlook express မှ email အလိုအလျောက်ပို့လွှတ်ရယူခြင်းမပြုရန် automatic checking ကိုအောက်ပါအတိုင်းပိတ်ရပါမယ်။

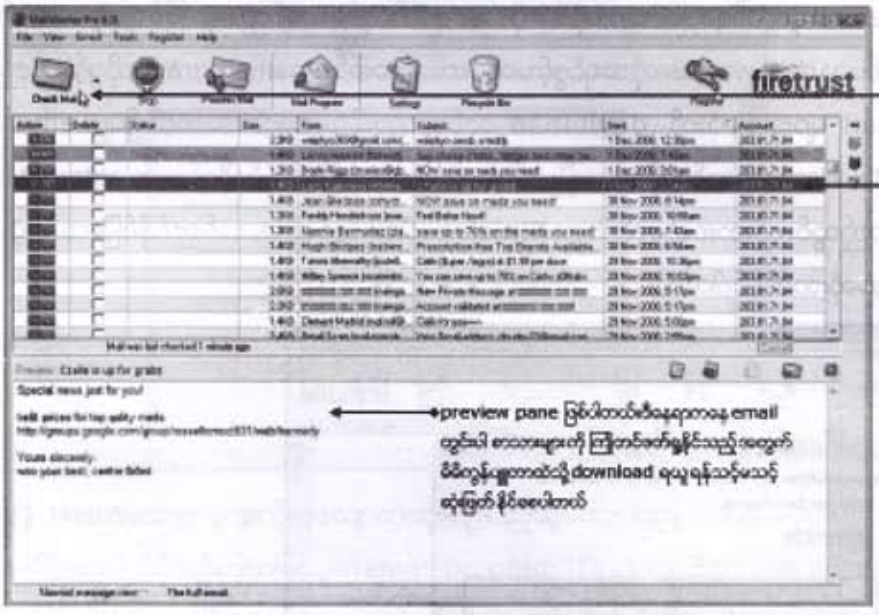
1) tools > options တွင် click နှိပ်ပါ။ Options dialogbox ပွင့်လာပါမည်။

2) General tab အောက် **Send and receive messages at startup** ဘေး checkbox ကို clear လုပ်ပါ။ **Check for new messages** ဘေး checkbox ကို clear လုပ်ပါ။

3) Options dialogbox ရှိ **OK** button တွင် click နှိပ်ပါ။

Using MailWasher

Desktopပေါ်ရှိ MailWasher iconကို double click နှိပ်လိုက်ပါကMailWasher program ပွင့်လာပြီး mail serverပေါ်မှ mailboxထဲတွင်ရှိသော new messageများရဲ့ listကိုဖေါ်ပြပါလိမ့်မယ်။ အကယ်၍ အကြောင်းတစ်စုံတစ်ခုကြောင့် အလိုလျောက်စစ်ဆေးဖေါ်ပြခြင်းမရှိပါက **Check Mail**တွင် click နှိပ်ပြီးခိုင်းစေနိုင်ပါတယ်။



❑1) Deleting

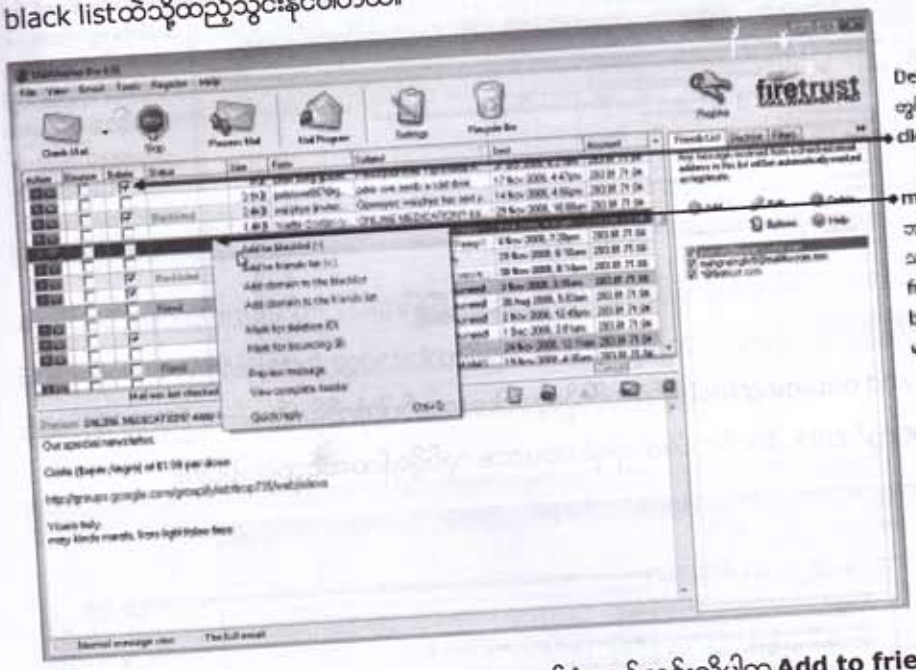
ပေးပို့သူအမည်နှင့် email subjectများကိုကြည့်ခြင်းဖြင့်သော်လည်းကောင်း message တစ်ခုပေါ်တွင် click တစ်ချက်နှိပ်ပြီး preview page ထဲတွင်ဖတ်ရှုခြင်းဖြင့် မလိုလားအပ်သော email များ၊ virus ဟုယူဆရသော email message တို့၏ delete နေရာမှcheckbox ထဲတွင်အမှန်ခြစ်ပေါ်အောင် click နှိပ်၍ delete လုပ်ဖို့ရန်ရွေးချယ်နိုင်ပါတယ်။ ဒီလို delete လုပ်ခြင်းသည် mail serverပေါ်ရှိ mail-box အတွင်းမှ mailများကိုတိုက်ရိုက်ဖျက်ထုတ်နိုင်ခြင်းဖြစ်သဖြင့် email program မှ downloadရယူတဲ့အခါ ပါလာမှာမဟုတ်ပါဘူး။

❑2)Friends List

Mail Washer မှဖေါ်ပြထားသော message listထဲရှိအချို့သော messageများ၏နေရာတွင် friendတို့၊ black listတို့ကိုတွေ့နိုင်ပါတယ်။ mailwasherသည် account setupလုပ်စဉ်အခါတုန်းက address bookထဲရှိaddressများကို friend listထဲသို့အလိုလျောက်ထည့်သွင်းပေးကြောင်းကိုဖေါ်ပြခဲ့ပြီး

ဖြစ်ပါတယ်။ မိမိထံသို့ရောက်ရှိလာသော messageသည်friends listထဲရှိလိပ်စာတစ်ခုခုမှပေးပို့လာသော message ဖြစ်နေပါက mailwasher သည် ထို message များကို friend အဖြစ် အမှတ်အသားပြု ပေးပြီးမှာဖြစ်ပါတယ်။

အလားတူပင် black list ထဲရှိလိပ်စာတစ်ခုခုမှ ပေးပို့လာသော messageဖြစ်နေပါက black listဟုအမှတ်သားပြုပေါ်ပြီးမှာဖြစ်ပြီး ထို message ကို deleteလုပ်ဖို့ရန် အလိုလျောက် ရွေးချယ်ပြီးသား ဖြစ်ပါလိမ့်မယ်။အကယ်၍ message list ထဲမှ လိပ်စာတစ်ခုခုကို friends list (သို့မဟုတ်) black list ထဲသို့ထည့်သွင်းလိုပါက ထို message ပေါ်တွင် right click တစ်ချက်နှိပ်ပါ။ ထို့နောက် submenu ထဲရှိ Add to black list (သို့မဟုတ်) Add to friend list တွင် click နှိပ်ပြီး friends list (သို့မဟုတ်) black listထဲသို့ထည့်သွင်းနိုင်ပါတယ်။



freinds list ထဲတွင် address များထပ်မံထည့်သွင်းလိုပါက **Add to friend list (+)**တွင် click တစ်ချက်နှိပ်ပြီး address တစ်ခုချင်းထည့်နိုင်ပါတယ်။ အလားတူပင် ဖယ်ထုတ်လိုပါ ကလည်း ဒီနေရာမှာပင် selectလုပ်ပြီး **Delete**တွင် click နှိပ်၍ဖျက်ထုတ်နိုင်ပါတယ်။

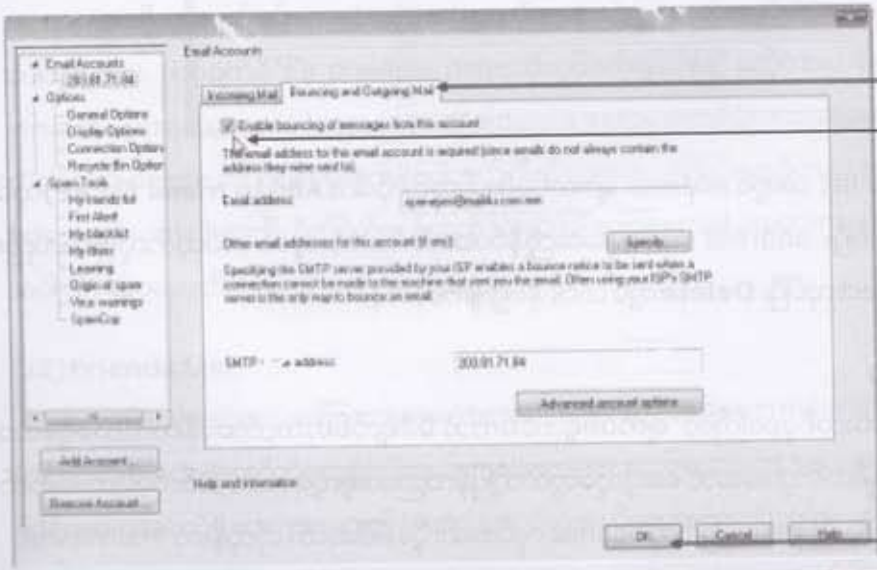
❑3)Bouncing

အကြောင်းတစ်ခုခုကြောင့် ဖျက်ပစ်ရုံတင်မကဘဲ မိမိရဲ့လိပ်စာသည်အမှန်တကယ်မရှိသော လိပ်စာတစ်ခု အဖြစ်ထင်သွားအောင် ပေးပို့သူတွေထံသို့ပြန်လည်ပေးပို့လို့ရတယ်။ အဲဒီလိုမိမိထံမရောက် သကဲ့သို့ ပြန်လည်လှည့်ပြီးပေးပို့ခြင်းကို bounce လုပ်တယ်လို့ခေါ်ပါတယ်။ ဟိုတုန်းက MailWasher

version ဟောင်းတွေမှာဆိုရင် delete တို့၊ friendlist တို့ရွေးသလိုမျိုးလွယ်လွယ်ကူကူ ရွေးပေးလိုက်ရုံပဲ။ အောက်ပိုင်း version တွေမှာတော့ mailwasher setting အချို့ကိုဝင်ပြင်ပေးမှ bounce လုပ်လို့ရပါတယ်။

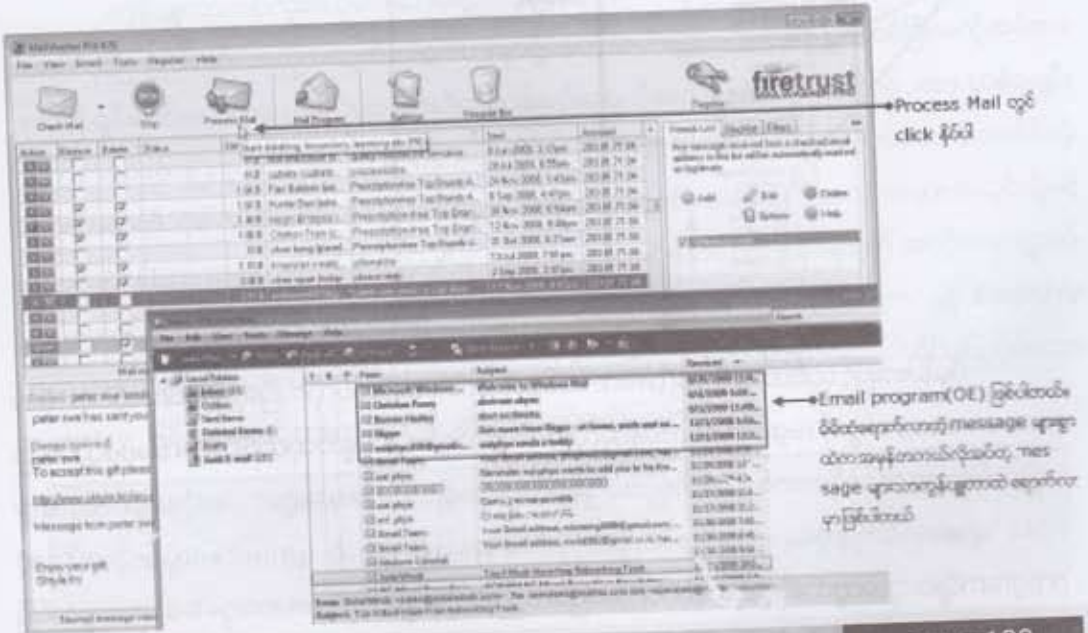
1) Tools > Email accounts တွင် click တစ်ချက်နှိပ်ပါ။ Email accounts အောက်တွင် mailwasher မှာထည့်သွင်းထားသော username ၊ password အပါအဝင် email account နှင့်သက်ဆိုင်သော information များကိုမြင်ရပါမယ်။ ပြင်လိုက်ဒီနေရာကနေလည်းပြင်နိုင်ပါတယ်။

2) Bouncing and outgoing mail အောက်သို့သွားပါ။ အောက်ပါအတိုင်းလိုအပ်သည်များကိုပြင်ဆင်ထည့်သွင်းပြီး **OK** တွင် click နှိပ်လိုက်ပါ။ ဒါဆိုရင် bounce လုပ်ဖို့ရန်အဆင်သင့်ဖြစ်ပါပြီ။



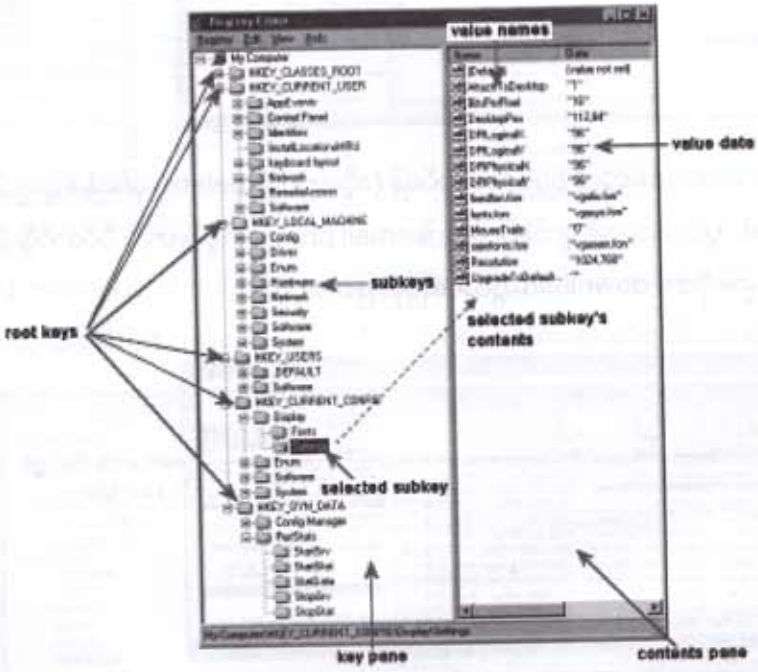
3) ဝင်လာသည့်အထဲက bounce လုပ်လိုသော email တို့၏ bounce checkbox တွင် အမှန်ခြစ်ခြစ်အောင် click နှိပ်ပေးရပါမယ်။ bounce ကိုရွေးချယ်ပါက delete ကိုပါအလိုအလျောက် ရွေးချယ်ပြီးသား ဖြစ်ပါလိမ့်မယ်။

4) မိမိမလိုအပ်တဲ့ email message တွေကို bounce လုပ်ရန် (သို့မဟုတ်) delete လုပ်ရန် ရွေးချယ်ခဲ့ပြီးပြီဆိုပါက **Process Mail** တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ email program ပွင့်လာပြီး မိမိဖတ်ဖို့ရန် ချန်ထားခဲ့သည့် message များကိုသာ download ဆွဲယူဖေါ်ပြမှာဖြစ်ပါတယ်။



Windows Registry Booster (Uniblue)

Windows Registry ဆိုတာကွန်ပျူတာတစ်လုံးဖြစ်တဲ့ operating system (windows XP၊ Vista) တို့ကောင်းစွာအလုပ်လုပ်နိုင်စေရန် လိုအပ်သော information များကို သိုလှောင်သိမ်းဆည်းရာ databaseတစ်ခုပင်ဖြစ်ပါတယ်။ သူ့ထဲမှာကွန်ပျူတာတွင် တပ်ဆင်အသုံးပြုထားသော hardware၊ Softwareတို့နှင့် ပတ်သက်သော configuration များ၊ Network နှင့်ပါတ်သက်သော setting များ၊ profile လို့ခေါ်တဲ့ အသုံးပြုသူတစ်ဦးချင်းစီအလိုက် စိတ်ကြိုက် ပြုပြင်လေ့ရှိတဲ့ display setting တွေ၊ background တွေ၊ screen server တွေအစရှိတဲ့ information များကို သိုလှောင်ထည့်သွင်းထားပါတယ်။ ဒဲ့ကြောင့် driver တွေ၊ application softwareတွေကို install လုပ်တာပဲဖြစ်ဖြစ်၊ uninstall လုပ်တာပဲဖြစ်ဖြစ်၊ display setting ကစလို့ windows sizeပြောင်းမယ်၊ အသံအတိုးအကျယ် ညှိမယ် အစရှိတဲ့ ဆောင်ရွက်မှုတိုင်းကို key များ အဖြစ်ဖြင့် Registryထဲမှာ ထည့်သွင်းရေးသားပါတယ်။



ပုံမှန်အားဖြင့် တင်ထားတဲ့ software တစ်ခုကို uninstall လုပ်လိုက်ပြီဆိုရင် သက်ဆိုင်ရာ key (entry value) တွေကို registryထဲကနေအလိုအလျောက်ရှင်းလင်းဖျက်ထုတ်ပါတယ်။ ဒါပေမယ့်လည်း အမြဲတမ်းတော့ ကုန်စင်အောင်ရှင်းလင်းခြင်းမပြုနိုင်ပါဘူး။ အချို့သော key တွေဟာ အသုံးမရှိဘဲ registry hole များအဖြစ်ကျန်ရှိနေတတ်ပါတယ်။ ပြီးမြောက်အောင်မြင်အောင် uninstallလုပ်လို့မရနိုင်တဲ့ programမျိုးတွေအတွက်ဆိုပိုဆိုးပါတယ်။ ဒဲ့အပြင်လည်းပဲ ကွန်ပျူတာမှာ virusတွေ၊ trojanတွေတဲ့

နေမယ်ဆိုရင်အဲဒီအန္တရာယ်ကောင်တွေက လက်ရှိအလုပ်လုပ်နေတဲ့ keyတွေကို ဖျက်ထုတ်ခြင်း၊ပြင်ရေးခြင်းတွေကိုလုပ်တတ်တယ်။ ဒါ့ကြောင့် softwareတွေဖြုတ်တပ်မကြာခဏလုပ်လို့ပဲဖြစ်ဖြစ်၊ virusတွေ trojanတွေကြောင့်ပဲဖြစ်ဖြစ်အသုံးပြုမှုများခြင်းနှင့် ကာလအပိုင်းအခြားပေါ်မူတည်ပြီး registry အတွင်းရှိ အချက်အလက်များစနစ်တကျတစ်စုတစ်စည်းထဲ မရှိခြင်းနှင့် ပျောက်ပျက်ခြင်း များကြောင့် ကွန်ပျူတာမှာ errorများဖြစ်ပေါ်စေပါတယ်။ ထို errorများကြောင့်ပင် သုံးနေရင်းနှင့် ကွန်ပျူတာသည် မကြာခဏရပ်သွားခြင်း၊ အချို့သော programတွေဆက်လက် အသုံးပြု မရတော့ဘဲcrash ဖြစ်ခြင်း၊ ပုံမှန်အလုပ်လုပ်နေသော်လည်းလေးလံနေးကွေးခြင်းအစရှိသောပြဿနာများကြုံကြရတတ်ပါတယ်။

ကွန်ပျူတာမှဖြစ်လေ့ဖြစ်ထရှိသောပြဿနာတို့ရဲ့ဓဝရာခိုင်နှုန်းခန့်သည် Windows registry နှင့်ဆက်နွယ်ပြီးဖြစ်သော ပြဿနာများသာဖြစ်တတ်ပါတယ်။ registry ကြောင့်ဖြစ်တတ်သော ပြဿနာအများစုမှာ -

1) ကွန်ပျူတာလုပ်ဆောင်မှုနေးကွေးလေးလံခြင်း၊
2) dll error၊ activeX error ၊ rundll error အစရှိသော system error များမကြာခဏဖြစ်ခြင်း၊
3) ကွန်ပျူတာအတက်နေးခြင်းနှင့် Shutdown ဖို့ရန်အချိန်ကြာမြင့်စွာယူရခြင်း၊
4) Programများ crash ဖြစ်ခြင်းနှင့် ကွန်ပျူတာအလုပ်မလုပ်ဘဲရပ်သွားခြင်း၊
5) အဆိုးဆုံးက registry error ကြောင့် ကွန်ပျူတာ boot မတက်နိုင်တော့ခြင်းတို့ဖြစ်ပါတယ်။

ကွန်ပျူတာတစ်လုံး၏ စွမ်းဆောင်ရည်တိုးမြှင့်ချင်တယ်ဆိုရင် ကြုံခိုင်တဲ့ registryဖြစ်အောင်အရင်လုပ်ကြရပါမယ်။ သည့်အတွက် registryမှာရှိနေတဲ့အမှားအယွင်းများကိုပြင်ဆင်ပြီး၊ မလိုအပ်တာတွေကိုရှင်းလင်းဖယ်ရှားပေးဖို့လိုပါတယ်။ ဒီလုပ်ငန်းစဉ်တွေကိုအသုံးပြုသူတို့ကိုယ်တိုင် key တစ်ခုချင်းလိုက်လံစစ်ဆေးပြီးရှင်းလင်းဖယ်ရှားဖို့ရန်ဘယ်လိုမှမဖြစ်နိုင်ပါဘူး။ အလိုလျောက်လုပ်ဆောင်ပေးနိုင်တဲ့ tools တွေကို သုံးကြရပါတယ်။ ဒီ tools တွေက registryကိုစစ်ဆေးခြင်း (Scan)၊အမှားအယွင်းရှိမရှိခွဲခြားခြင်း (Identify) နှင့် ပြင်ဆင်ခြင်း(Repair) အစရှိသော လုပ်ငန်းများကို အလိုအလျောက်လုပ်ဆောင်ပေးနိုင်ပါတယ်။ ဥပမာဆိုရရင် Registry cleaner၊ Registry mechanic နှင့် Registry boosterတို့ဖြစ်ပါတယ်။ ဒီလမ်းညွှန်စာအုပ်မှာတော့ registry booster ကိုသုံးပြီးကြံခိုင်မှုပြည့်ဝသော registry ဖြစ်နေအောင်ကာကွယ်ထိန်းသိမ်းပုံများကိုဖော်ပြသွားပါမယ်။

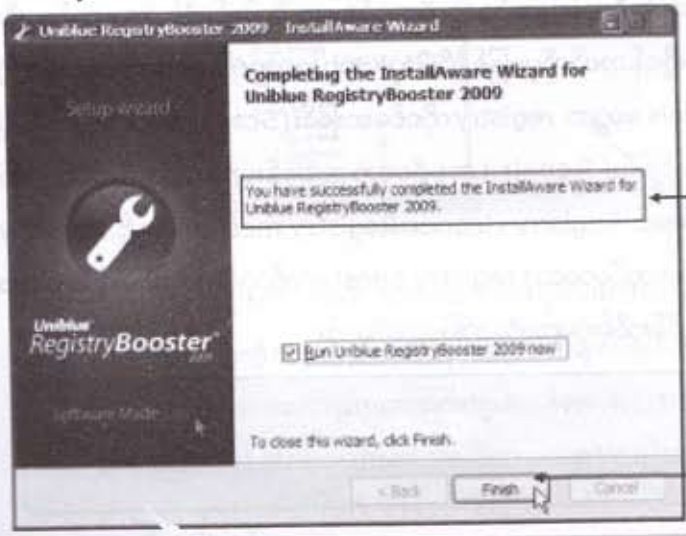
- Registry cleaner - http://www.amlsoft.com/
- Registry mechanic - http://www.pctools.com/registry-mechanic/

Download Registry Booster

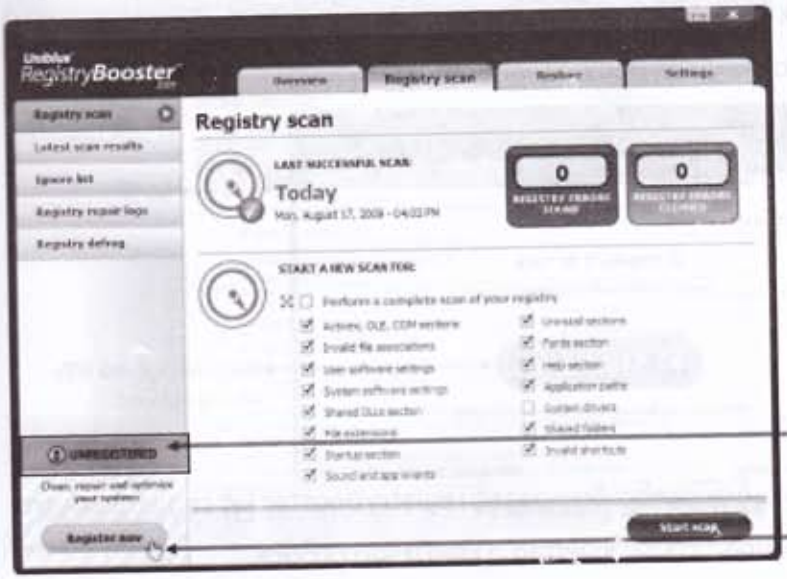
Uniblue အား download ရယူနိုင်တဲ့မူရင်းဌာနေsiteကတော့ www.registrybooster.com ပဲဖြစ်ပါတယ်။ ဌာနေ site ကနေ downloadရယူနိုင်သလို www.download.com၊ www.tucows.com အစရှိတဲ့ download siteများကနေလည်း အလွယ်တကူရှာဖွေရယူနိုင်ပါတယ်။

Installing & Registering RegistryBooster

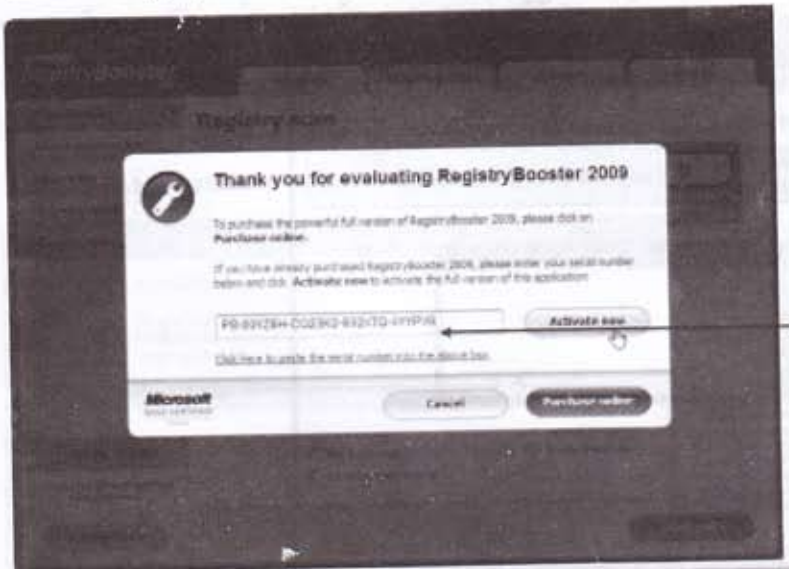
download ရယူထားသော registrybooster.exe အား double clickနှိပ်ပါ။ "set up" dialogbox ကျလာပါမည်။ ညွှန်ကြားချက်များအတိုင်းလိုက်ပါ install လုပ်နိုင်ပါတယ်။ နောက်ဆုံးမှာ Finish button ပါသော wizard ကိုမြင်ရပါမယ်။ **Finish** တွင် click နှိပ်ကာ installation အား အဆုံးသတ်လိုက်ပါ။



install ပြီးသွားတဲ့ အခါ registrybooster window အားအောက်ပါအတိုင်းတွေ့ရပါမယ်။ Registrybooster အတွက်ပထမဆုံးလုပ်သင့်တာက register ဖြစ်ပါတယ်။ register မလုပ်ရင် scan တော့စစ်လို့ရမယ်။ repair လုပ်ပေးမှာမဟုတ်ပါ။

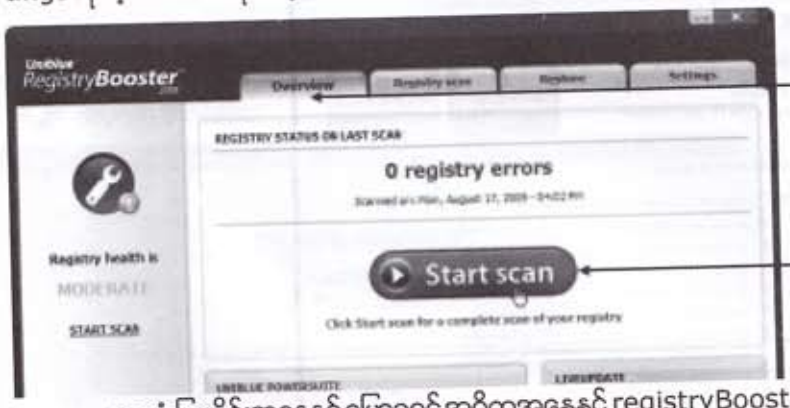


သည့်အတွက် **Register now** တွင် click နှိပ်လိုက်ပါ။ registration အတွက်လိုအပ်သော key များထည့်သွင်းပေးရမည့် box ကျလာပါမည်။လိုအပ်သော Key များထည့် သွင်းပြီး **Activate now** တွင် click နှိပ်လိုက်ပါ။ထည့်သွင်းသော key များမှန်ကန်ပါက UNREGISTERED ဆိုတာပျောက်သွားပြီး REGISTERED ဖြစ်မြင်ရပါမယ်။



Open RegistryBooster

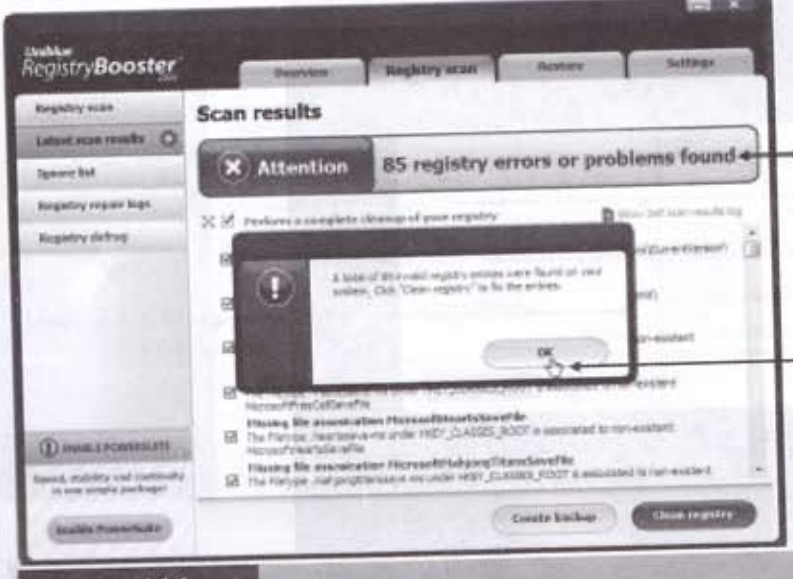
RegistryBooster အားဖွင့်ရန် desktopပေါ်တွင်ရှိသော iconပေါ်တွင် double click နှိပ်၍ ဖွင့်ပါ။ အလားတူပင် ကွန်ပျူတာ Screen ၏ညာဘက်ထောင့်အောက်ခြေတွင်ရှိသော Taskbarထဲရှိ icon တွင်လည်း double click နှိပ်၍ဖွင့်နိုင်ပါတယ်။ Overview ၊ Registry Scan ၊Restore နှင့် Settingsဆိုတဲ့ tab လေးခုပါတဲ့ RegistryBooster window ကိုမြင်ရပါမယ်။



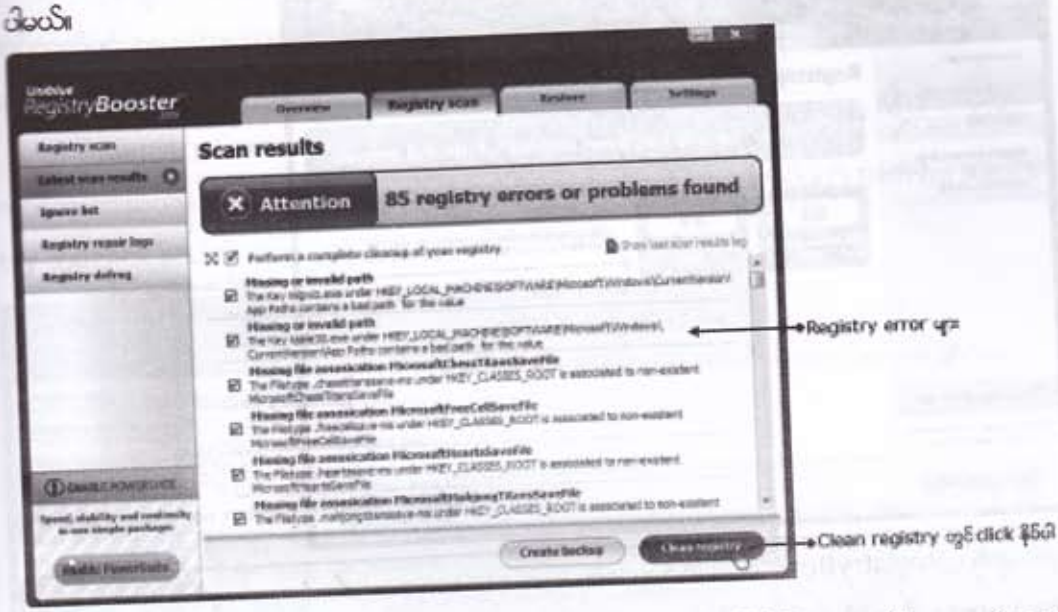
အသုံးပြုမှုပိုင်းအနေနှင့် ပြောရရင် အဓိကအနေနှင့် registryBooster ဖြင့် registry မှာerror ရှိမရှိစစ်မယ် (Scan) ၊ရှိရင် repair လုပ်မယ်၊ Defrag လုပ်မယ်။ ဒီလောက်ပါပဲ။

Scanning and Repairing registry errors

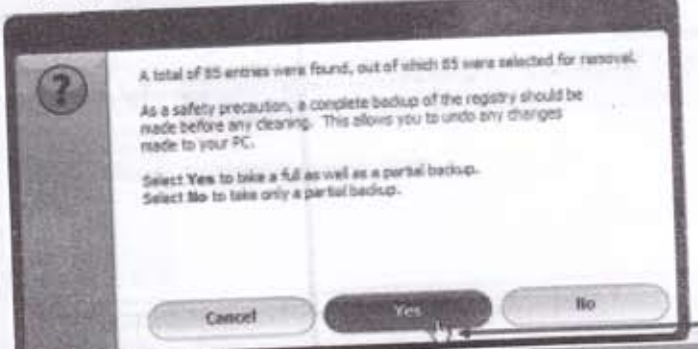
Overview tab အောက်ရှိ **Start scan** တွင် click နှိပ်လိုက်ပါ။ error ရှိနေသော registry key များအားစတင်စစ်ဆေးရှာဖွေပါလိမ့်မယ်။ စစ်ဆေးပြီးသွားတဲ့အခါ တွေ့ရှိသော registry error အရေအတွက်ကိုဖော်ပြထားသော box ကျလာပါမည်။ **OK** button တွင် click နှိပ်လိုက်ပါ။



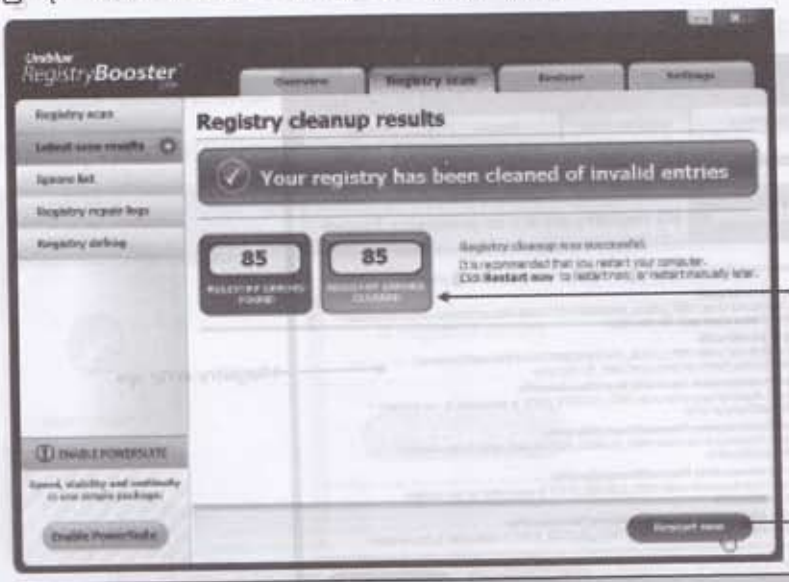
scan result တွင် registry error များ၏ list ကိုဖေါ်ပြထားပါလိမ့်မယ်။ error များအားရှင်းလင်းရန်အတွက် **Clean registry** တွင် click နှိပ်လိုက်ပါ။ full backup လား၊ partial backup လား ရွေးရပါမယ်။



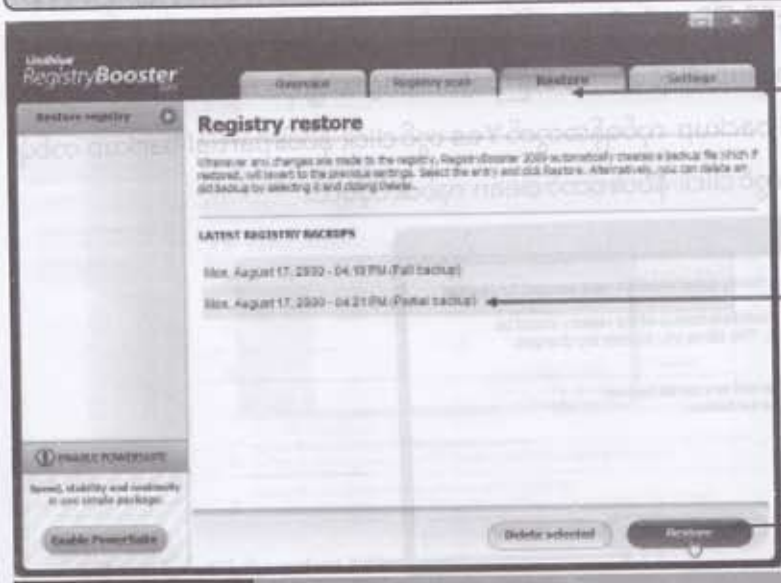
backup လုပ်တယ်ဆိုတာက registry ထဲကနေ မဖျက်ထုတ်ခင် ဒီ error လို့ယူဆရတဲ့ registry setting တွေကို တစ်နေရာမှာမှတ်သားသိမ်းဆည်းခြင်း ဖြစ်ပါတယ်။အကယ်၍များ ဖျက်ထုတ်ပြီးတာမှကွန်ပျူတာသည်ကောင်းစွာအလုပ်မလုပ်နိုင်တဲ့ပြဿနာတစ်ခုခုနှင့်ကြုံလာရတယ်ဆိုရင် ဒီbackup လုပ်သိမ်းထားတဲ့setting များအတိုင်းregistry အတွင်းပြန်လည်ထည့်သွင်းrestore လုပ်ခြင်းဖြင့် နဂိုမူလ မဖျက်ခင်ကအခြေအနေအတိုင်းပြန်လည်ရရှိစေမှာဖြစ်ပါတယ်။ full backup ဆိုရင်အားလုံးကိုမှတ်သားသိမ်းဆည်းမယ်၊ partial backup ဆိုရင်တော့အရေးကြီးတဲ့setting အချို့ကိုသာမှတ်သားသိမ်းဆည်းမှာဖြစ်ပါတယ်။ full နှင့် partial backup လုပ်ရန်အတွက် **Yes** တွင် click နှိပ်ပါ။ partial backup တစ်မျိုးတည်းလုပ်ရန်အတွက် **No** တွင် click နှိပ်ပါ။ စတင် clean လုပ်ပါလိမ့်မယ်။



clean လုပ်ပြီးသွားတဲ့အခါ error တွေထဲက ဘယ်နှစ်ခုကို ရှင်းလင်းခဲ့ပါတယ်ဆိုတဲ့ ရှင်းတမ်းကို မြင်ရပါမယ်။ **Restart now** တွင် click နှိပ်ပြီးကွန်ပျူတာအား restart လုပ်လိုက်ပါ။



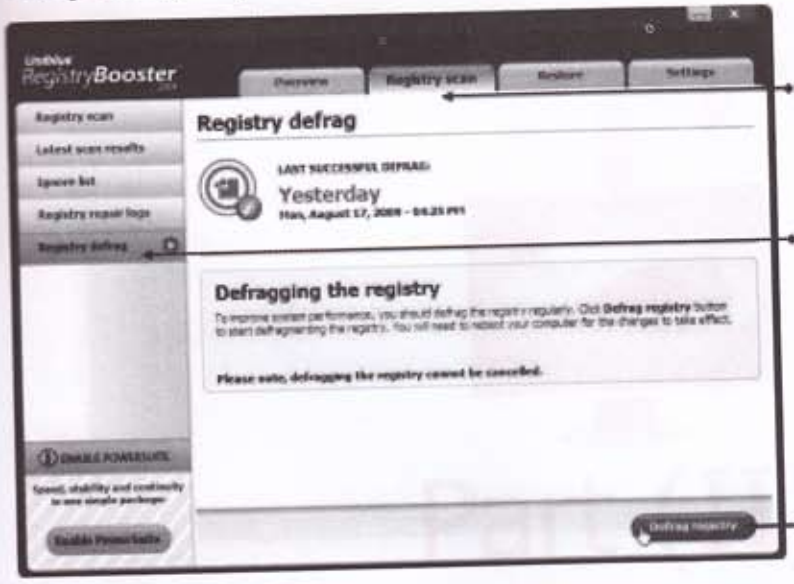
မှတ်ချက် - RegistryBooster window ထဲမှ Restore tab အောက်သို့ သွားကြည့်ပါက registry backupများကို အချိန်ရက်စွဲအလိုက် တွေ့ရပါမယ်။ အကယ်၍အမှားအယွင်းတစ်ခုခုရှိနေလို့ registry အား နဂိုမူလအခြေအနေသို့ပြန်ရောက်လိုလျှင် registry backup တစ်ခုပေါ်တွင် select မှတ်ပါ။ ထို့နောက် restore တွင် click နှိပ် ကာနဂိုမူလအတိုင်းဖြစ်အောင်လုပ်ဆောင်နိုင်ပါတယ်။ ဒါ့အပြင် backup တွေများနေလို့ရှင်းပစ်ချင်ရင်လည်း Delete ကနေဖျက်ထုတ်နိုင်ကြပါတယ်။



Defrag your Registry

ကွန်ပျူတာ hard disk ထဲက data တွေကိုဆိုင်ရာဆိုင်ရာတစ်စုတစ်စည်းထဲဖြစ်အောင် Defrag လုပ်သလိုပင် registry ထဲမှာ gap တွေမရှိအောင်၊ setting ဟိုတစ်စဒီတစ်စ ပြန့်ကျဲမနေအောင် registry defrag လုပ်ခြင်းဖြင့် ကွန်ပျူတာ၏စွမ်းဆောင်ရည်ကိုတိုးမြင့်စေနိုင်ပါတယ်။

Registry Scan tabအောက်သို့သွား၍ **Registry defrag** တွင် click နှိပ်လိုက်ပါ။ defrag လုပ်ခဲ့ဘူးရင် ဘယ်နေ့ဘယ်အချိန်က နောက်ဆုံးလုပ်ခဲ့ကြောင်းကိုဖော်ပြထားပါလိမ့်မယ်။ **Defrag Registry** တွင် click နှိပ်ပါလိုက်ပါ။ စတင် defrag လုပ်ပါလိမ့်မယ်။



အောင်မြင်စွာ defrag လုပ်ပြီးသွားတဲ့အခါကွန်ပျူတာအား restart လုပ်ဖို့ရန်တိုက်တွန်းသော message ကိုမြင်ရပါမယ်။ **Restart now** တွင် click နှိပ်ကာကွန်ပျူတာအား restart လုပ်လိုက်ပါ။

INTERNET Security

Part (II)

Freeware and Shareware guide to internet surfing

အင်တာနက်အသုံးပြုသူအတော်များများဟာsoftwareများကိုအင်တာနက်မှတစ်ဆင့် download ရယူအသုံးပြုလေ့ရှိပါတယ်။ အင်တာနက်မှ download ရယူခြင်းအားဖြင့် latest versionများရနိုင်သလို မိမိအသုံးတည့်ရာ softwareများကိုအလွယ်တကူရွေးချယ်အသုံးပြုနိုင်ပါတယ်။ အင်တာနက်ပေါ်မှာ download ရယူနိုင်သော software ပေါင်းများစွာရှိပါတယ်။ဒါပေမယ့်အဲဒီ software များဟာတစ်ခုနှင့်တစ်ခု အများအစားအုပ်စုမတူကြပါဘူး။freeware ၊ shareware ၊ demoware ၊ educational software၊ commercial softwareရယ်လို့အကြမ်းဖြင်းအားဖြင့်အုပ်စုအများအစား၅ခုခွဲခြားသတ်မှတ်ထားပါတယ်။

အဲဒီ အများအစား ၅ခုတို့ဟာ တစ်ခုနှင့် တစ်ခု သဘောသဘာဝအားဖြင့် မတူကြပါဘူး။ဒါကြောင့် အသုံးပြုသူများဟာ မိမိ download ရယူမယ့် software သည်ဘယ်လိုအမျိုးအစားဖြစ်တယ် ဆိုတာကို သိထားဖို့လိုသလို အဲဒီsoftware အများအစားအုပ်စုရဲ့သဘောသဘာဝကိုနားလည်သဘောပေါက်ထားရန် လိုပါလိမ့်မယ်။

➲Freeware

Freeware ဆိုတာဟာ အင်တာနက်ပေါ်မှ download ရယူပြီး အခကြေးငွေပေးစရာမလိုဘဲ အကန့်အသတ်မရှိအသုံးပြုနိုင်သော softwareအမျိုးအစားကိုခေါ်ပါတယ်။

➲Shareware

Shareware ဆိုတာဟာ "try before you buy" ဟူသောစည်းမျဉ်းစည်းကမ်းဖြင့် အသုံးပြုခွင့်ပေးထားသော software ပဲဖြစ်ပါတယ်။ဆိုရရင် ထိုsoftwareကိုဝယ်သင့်မဝယ်သင့် စဉ်းစားဆုံးဖြတ်နိုင်အောင် အချိန်ကာလ တစ်ခုကြာသည့်အထိ စမ်းသပ်အသုံးပြုနိုင်ပါတယ်။ သတ်မှတ်ထားတဲ့အချိန်ကာလပြည့်တဲ့အခါမှာ Registration fee ပေးပြီး ဝယ်ယူအသုံးပြုရမှာဖြစ်ပါတယ်။ထိုသို့ Register မလုပ်ပါက အဲဒီsoftware ဟာ expireဖြစ်သွားပြီးအသုံးပြု၍ရတော့မည်မဟုတ်ပါ။

➲Education software

လေ့ကျင့်ရန်အတွက်သာရည်ရွယ် ရေးသားထားပြီး စီးပွားရေးလုပ်ငန်းတွင် အသုံးပြု၍မရနိုင်သော softwareမျိုးကိုခေါ်တယ်။

➲Commercial software

ကုန်ပစ္စည်းများထုတ်လုပ်ရန် စီးပွားရေးလုပ်ငန်းတွင် အသုံးပြုနိုင်ပြီးအဖိုးအခမြင့်မားစွာပေး၍ ဝယ်ယူရသော softwareများကို commercial softwareလို့ခေါ်ပါတယ်။

➲Trial versions/ demoware

software ရေးသားသူ (Vendor) မှစွမ်းရည်ပြည့် အသုံးပြုခွင့်မပေးဘဲ အကန့်အသတ် ဖြင့်သာ အသုံးပြုခွင့်ပေးထားသော softwareကို demoware (သို့) evaluation softwareလို့ခေါ်ပါတယ်။ ဆိုရရင် ထို software မှfeatureအချို့ကို disableလုပ်ထားပြီးအဖိုးအခပေးဝယ်ယူမှသာလျှင်featureအားလုံးကို အပြည့်အဝအသုံးပြုနိုင်ရန်စီမံထားပါသည်။

Plug-in(Add-On)

ယခုဆက်လက်ပြီးတော့ ယနေ့အင်တာနက် webpage တွေကြည့်တဲ့နေရာမှာမဖြစ်မနေ အသုံးပြုသင့်တဲ့ plug-inလို့ခေါ်တဲ့ softwareများအကြောင်းကိုအနည်းငယ်ရှင်းပြလိုပါတယ်။ plug-inဆိုတာ Internet Exploren Firefox တို့လိုအဓိက main program ကြီးများ၏စွမ်းရည်ကို တိုးတက် ကောင်းမွန်စေရန် ထပ်မံဖြည့်စွက်တပ်ဆင်ထားတဲ့ softwareများကို plug-in လို့ခေါ်ပါတယ်။ Browser Programများသည် Multimedia လို့ခေါ်တဲ့ sound၊ image၊ animationနှင့် video fileများကိုတွေ့တဲ့အခါမှာထို fileများကို Run ဖို့ရန်(သို့)ဖွင့်ကြည့်ရန် plug-inလို့ခေါ်တဲ့ programဆီသို့လွှဲပြောင်းပေးလိုက်ပါတယ်။

ယခုကဲ့သို့ Browser programနှင့် plug-inတို့ပူးပေါင်းပြီးလုပ်ဆောင်ခြင်းအားဖြင့်ပြီးမြောက်သောသာယာသော internet surfingကို ခံစားရရှိနိုင်ပါတယ်။ plug-inအများစုဟာ freewareများဖြစ်ပြီး အဲဒီအထဲမှ Real One playen Quicktime player၊ Flash playen ShockWave playen Adobe Acrobat Reader၊ Javaနှင့် DirectX တို့ဟာ မဖြစ်မနေ အသုံးပြုသင့်သော "plug-in"freeware များဖြစ်ပါတယ်။

❑Real One Player

RealOne player အား http://www.real.com မှ downloadရယူနိုင်ပါတယ်။

❑Quick Time Player

Quick Time Player အား http://www.apple.com/quicktime မှ download ရယူနိုင်ပါတယ်။

❑Flash Player

Flash Player အား www.macromedia.com မှ downloadရယူနိုင်ပါတယ်။

❑Window Media Player

Window Media Player(update version) များအား http://www.microsoft.com/windows/windowsmedia/player/download မှ downloadရယူ install နိုင်ပါတယ်။

❑Adobe Acrobat Reader

Adobe Acrobat Readerဟာလည်း webပေါ်မှာအသုံးများသော plug-inတစ်ခုပဲဖြစ်ပါတယ်။ portable document format (pdf)ဖြင့်ရေးသားသော document များကိုဖွင့်ဖတ်ဖို့ရန် Adobe Acrobat Readerကို install လုပ်ထားဖို့လိုပါတယ်။ ထို့ကဲ့သို့ Installလုပ်ထားမှသာလျှင် .pdf ဖြင့် အဆုံးသတ်သော hyperlink file များပေါ်တွင် click နှိပ်တဲ့အခါတိုင်း Browser Program မှ ဖွင့်ပြ နိုင်ပါလိမ့်မယ်။

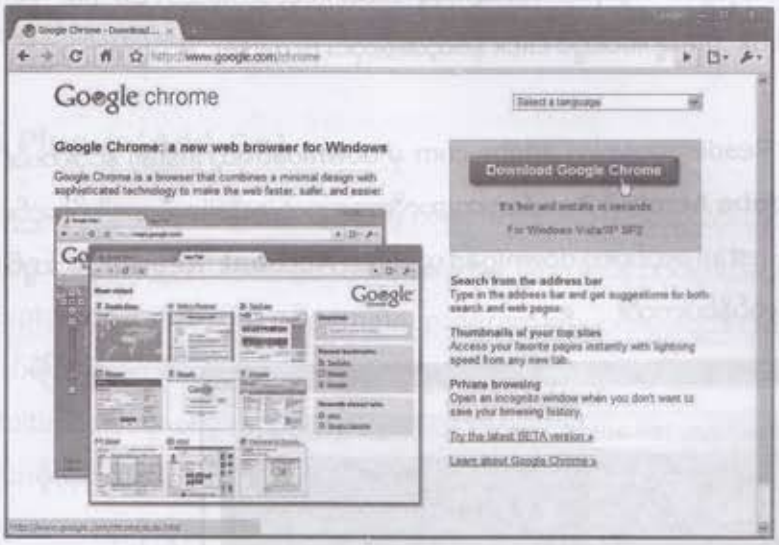
Adobe Acrobat Reader အားwww.adobe.com မှ downloadရယူ install နိုင်ပါတယ်။ Download ပြီးသွားပါက **Adobe Acrobat Reader**အားအလိုအလျောက်installလုပ်ပေးပါလိမ့်မည်။ အကယ်၍ အလိုအလျောက် install မလုပ်ပါက download ယူခဲ့သော **Acrobat Reader** ပေါ်တွင် double clickနှိပ်၍installလုပ်နိုင်ပါတယ်။

❑Java Plug-in

Internet Explorer,Netscape အစရှိသော web browserများအတွင်းမှာရှိတဲ့ applets လို့ခေါ်တဲ့ programများကို Runဖို့ရန် Java plug-inလိုပါတယ်။ appletsဆိုတာ Java language နှင့်ရေးသားထားသော program ငယ်လေးများပဲဖြစ်ပါတယ်။java ဖိုမူရင်းဌာနေ site ကတော့ http://www.java.com/dwonload ပဲဖြစ်ပါတယ်။ မူရင်းဌာနေ site ကနေ download လုပ်လို့မရနိုင်တဲ့အခါ အခြားdownload site ကနေလှည့်ပြီးရှာဖွေdownload ရယူနိုင်ကြပါတယ်။

❑Browser (Google Chrome)

Internet Explorerကဲ့သို့ပင် အင်တာနက်webpage များကို ကြည့်ရှုတဲ့နေရာမှာ အသုံးပြုနိုင်သော freeware programတစ်ခုပင်ဖြစ်ပါတယ်။Chromeကို **http://www.google.com/chrome** မှ download ရယူနိုင်ကြပါတယ်။

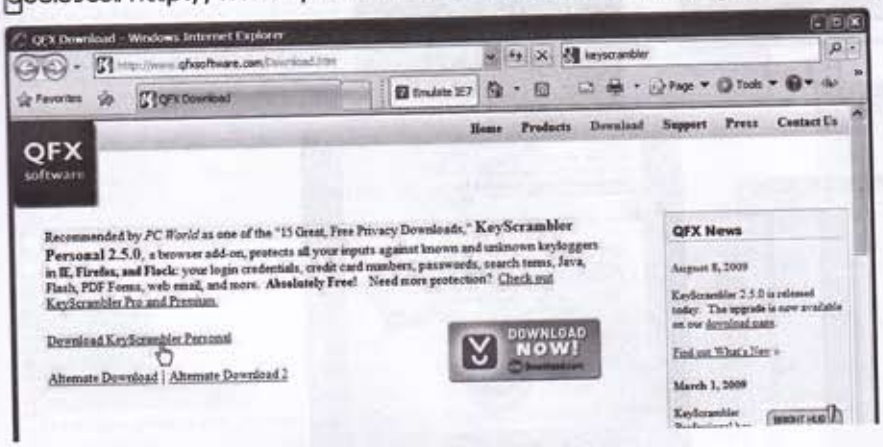


❑Mozilla Firefox

Firefox သည်လည်း browser တစ်ခုပင်ဖြစ်ပြီး http://www.mozilla.org/firefox မှ download ရယူနိုင်ပါတယ်။

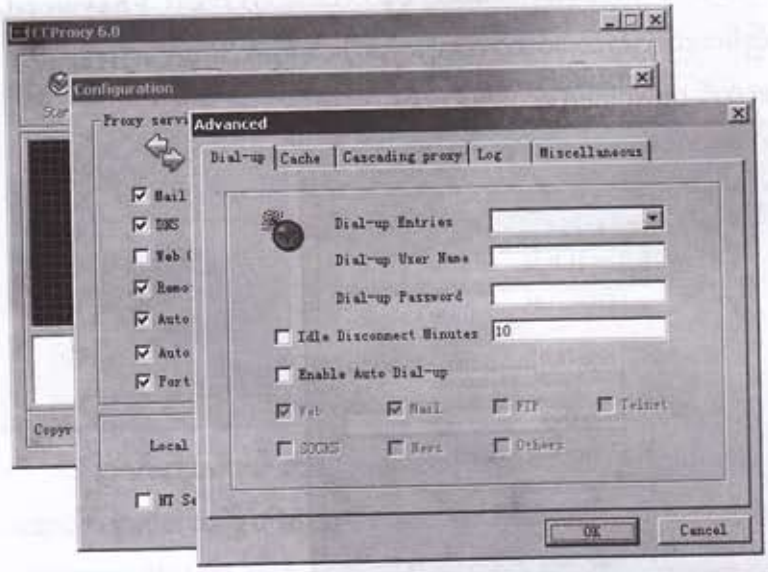
❑KeyScrambler Personal

Keyscrambler သည် Browser plugin တစ်ခုပင်ဖြစ်ပါတယ်။ ဆိုရရင် browser (IE ၊ Firefox) ထဲမှာရိုက်သမျှ URL (address) ၊ username ၊password ၊ search term များကို keylogger(GoldenEye) တို့နှင့် ဖမ်းယူမရနိုင်အောင် encrypt လုပ်ပေးသော plugin တစ်ခုပင် ဖြစ်ပါတယ်။ http://www.qfxsoftware.com/Download.htm မှ download ရယူသုံးနိုင်ပါတယ်။



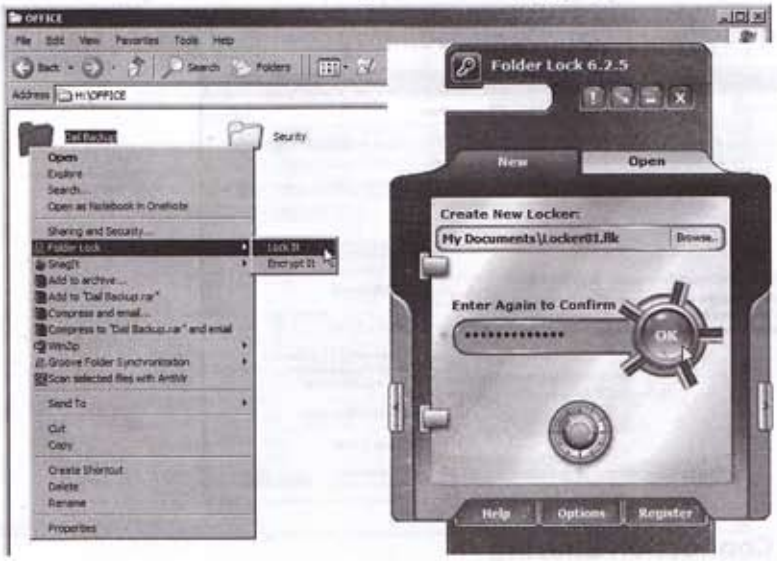
❑CCproxy (Internet Connection Sharing

အင်တာနက်ချိတ်ဆက်ထားသော computerတစ်လုံးရှိ Internet connectionကိုnetwork အတွင်းရှိအခြား ကျန်ကွန်ပျူတာများနှင့် sharing လုပ်၍သုံးစွဲနိုင်သော software ဖြစ်ပါတယ်။ **www.youngzsoft.net/ccproxy**မှ downloadရယူနိုင်ကြပါတယ်။



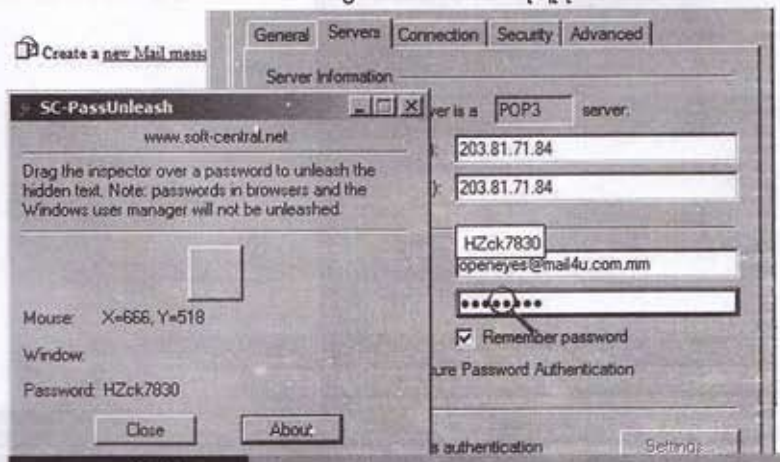
❑Folder Lock

မိမိရဲ့personal fileများ၊ folderများ၊ ရုပ်ပုံများကို မိမိမှလွဲ၍ အခြားသူများအသုံးပြုနိုင်အောင်၊ ဖွင့်မကြည့်နိုင်အောင် password ဖြင့်အကာအကွယ်ပေးနိုင်သော software ပဲဖြစ်ပါတယ်။ **www.newsoftwares.net** မှ download ရယူနိုင်ကြပါတယ်။



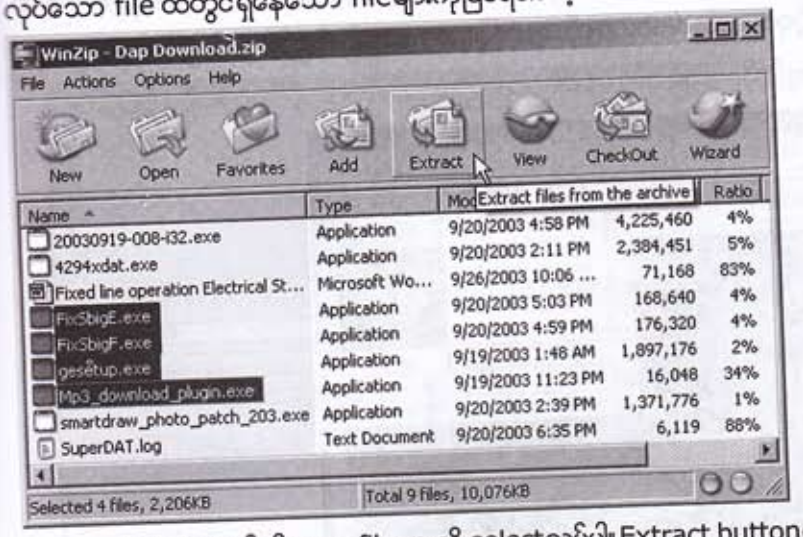
❑ PassUnleash

PassUnleashသည်asterisk(*)ဖြင့်မြင်ရသောpasswordများကိုဖော်ရွေ၍ရအောင်ဆောင်ရွက်ပေးနိုင်သော program တစ်ခုဖြစ်ပါတယ်။ PassUnleash ထဲမှ လူပုံပေါ်တွင် click နှိပ်၍ drag ဆွဲသွားပါကမှန်ဘီလူးပုံပေါ်လာမည်။ မိမိဖော်လိုသော asterisk ပေါ်သို့ မှန်ဘီလူးရောက်တဲ့အခါ **Password** နေရာတွင် password အဖြစ်ထည့်သွင်းထားသော စာလုံးများကို ဖေါ်ပြပါလိမ့်မည်။ **http://www.soft-central.net** တွင် download ရယူနိုင်ပါတယ်။

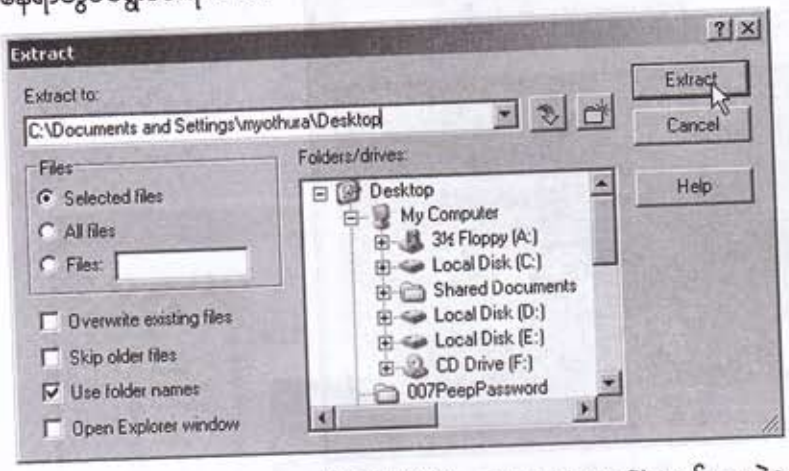


❑Winzip

winrar ကဲ့သို့ပင် file များကို compress လုပ်နိုင်သော program တစ်ခုပဲဖြစ်ပါတယ်။ Winzip ကို www.winzip.com မှ download ရယူနိုင်ပါတယ်။ Winzip ကိုအသုံးပြုရတာ အလွန်ပဲလွယ်ကူပါတယ်။ unzip လုပ်လိုသော zipfile ကို double click နှိပ်၍ဖွင့်လိုက်ပါ။ winzip window ပွင့်လာပြီးမှ လက်ရာ zip လုပ်သော file ထဲတွင်ရှိနေသော file များကိုမြင်ရပါလိမ့်မယ်။



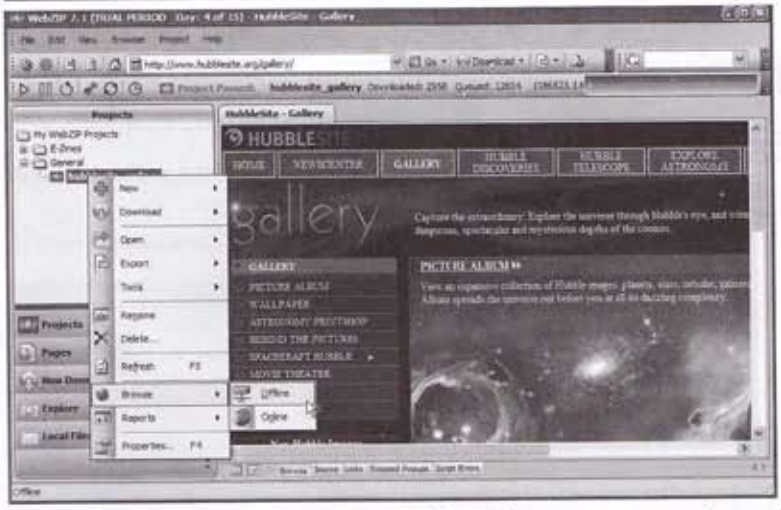
Extract လုပ်လိုသော file များကို select လုပ်ပါ။ Extract button တွင် click တစ်ချက်နှိပ်ပါက ဖိမိ extract လုပ်ရန်ရွေးချယ်ထားသော file များကိုထည့်ထားဖို့ရန် location တစ်ခုကို extract to နေရာတွင်ရွေးပေးရပါမယ်။



Extract button တွင် click နှိပ်ပါက zip archive file လုပ်ထားခဲ့သော file များကိုဖိမိသတ်မှတ်ထားသော folder ထဲသို့ unzip လုပ်ပေးပါလိမ့်မည်။ အလားတူပင် winzip ကိုအသုံးပြုပြီး ဖိမိ file များကို zip လုပ်လိုသော file (သို့) folder ပေါ်တွင် right click နှိပ်ကာ zipfile များအဖြစ်ချုံ့ပစ်နိုင်ပါတယ်။

❑Webzip

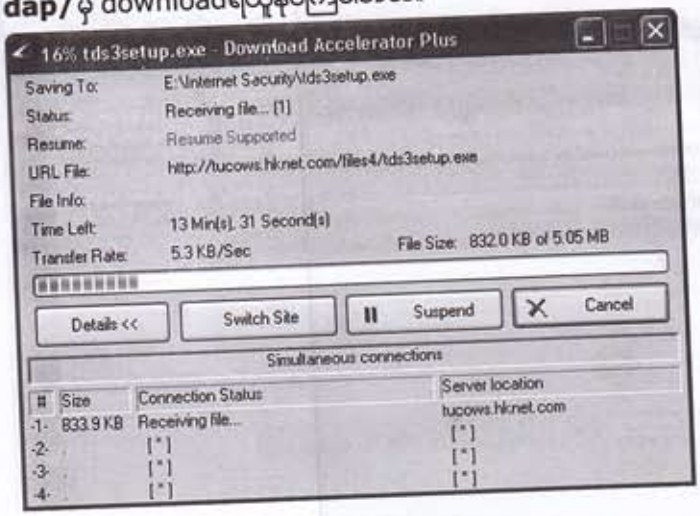
Webzip ကို webpage များ(သို့) website တစ်ခုလုံးကို download လုပ်တဲ့အခါမျိုးမှာ သုံးပါတယ်။ webpage(သို့) website တစ်ခုလုံး download ရယူပြီးတဲ့အခါမှာ အဲဒီ website ထဲမှာရှိတဲ့ image များ၊ audio များနှင့်အခြားသော media file များအားလုံးတို့ဟာ မိမိရဲ့ကွန်ပျူတာထဲရှိ hard disk ထဲသို့ရောက်ရှိလာမှာဖြစ်ပါတယ်။ ဒါကြောင့်ကြိုက်တဲ့နေရာ၊ကြိုက်တဲ့အချိန်မှာ အင်တာနက်နှင့်ချိတ်ဆက်စရာမလိုပဲ offline ပြန်ကြည့်လို့ရပါတယ်။ Webzip ကို အသုံးပြုရတာ အလွန်ပဲရိုးရှင်းလွယ်ကူပါတယ်။ install လုပ်ပြီးသွားပြီး webzip ကိုဖွင့်လိုက်လျှင် သူရဲ့ interface အား အောက်ပါအတိုင်းတွေ့ရပါမယ်။



Webzip က့ဲသို့ပင် website သို့မဟုတ် directory တစ်ခုလုံးကို download လုပ်ရာတွင် အသုံးပြု နိုင်သောအခြား programများမှာ Httrack(www.httrack.com) Webcopier(www.maximumsoft.com) တို့ဖြစ်ပါတယ်။

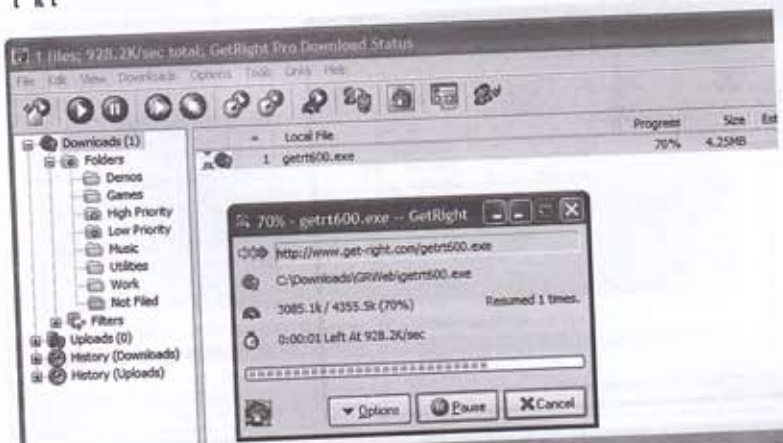
❑ Download Accelerator Plus

နောက်မှာဖေါ်ပြမည့် Internet Download Managerကဲ့သို့ပင် download speed ကိုမြှင့်တင်ပေးနိုင်သလို downloadရယူနေစဉ်အတွင်း connectionပြတ်တောက်သွားတဲ့အခါမှာလည်း အစမှအဆုံးပြန်လည် downloadလုပ်ယူနေစရာမလိုဘဲ ရရှိပြီးသားနေရာမှ ဆက်လက်၍ download ရယူပေးနိုင်သော freeware programတစ်ခုပင်ဖြစ်ပါတယ်။ **http://www.speedbit.com/dap/**မှ downloadရယူနိုင်ကြပါတယ်။



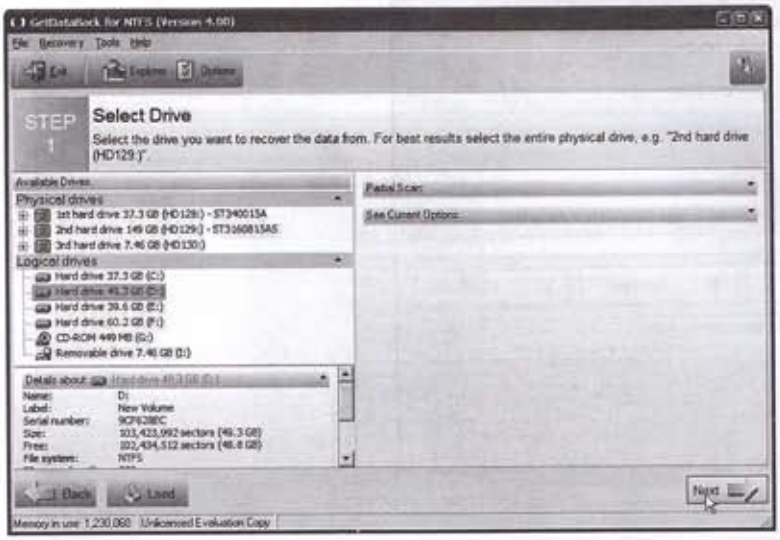
❑ Getright

DAP ကဲ့သို့ပင် download speed ကိုတိုးမြှင့်ပေးနိုင်ပြီး downloadလုပ်နေစဉ်အတွင်း connection ပြတ်သွားပါကလည်း အစမှပြန်လုပ်စရာမလိုဘဲ download ရရှိပြီး သားနေရာမှ ဆက်လက်လုပ်ဆောင်သွားနိုင်သော softwareပင်ဖြစ်ပါတယ်။ **http://www.getright.com**မှ download ရယူနိုင်ပါတယ်။



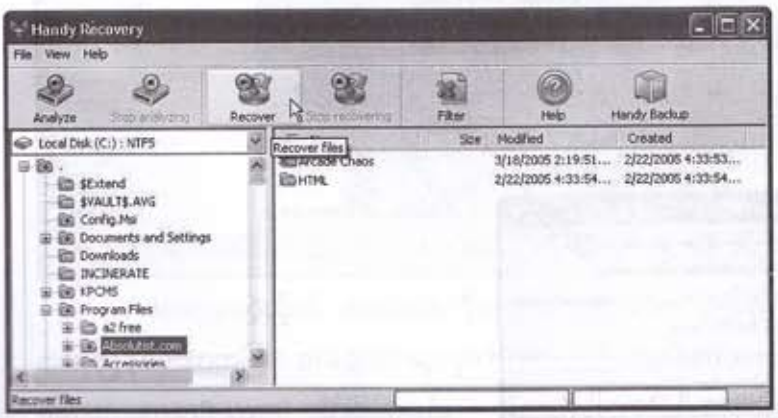
❑ Getdataback

Getdataback သည်မှားယွင်းပြီးဖျက်မိသော file များ၊ data များကိုပြန်လည်ရယူပေးနိုင်သော software program တစ်ခုဖြစ်ပါတယ်။file system အမျိုးအစားပေါ်မူတည်ပြီး getdataback for NTFS နှင့် FAT32 ဟူ၍ program အမျိုးအစားနှစ်ခုရှိပါတယ်။ မိမိ recovery လုပ်လိုသော hard disk ၏ file system ပေါ်မူတည်ပြီး NTFS နှင့် FAT32 တို့ထဲမှ တစ်ခုခုကို ရွေးချယ်အသုံးပြုနိုင်ပါတယ်။ Getdataback ကို **www.runtime.org** မှ download ရယူအသုံးပြုနိုင်ပါတယ်။



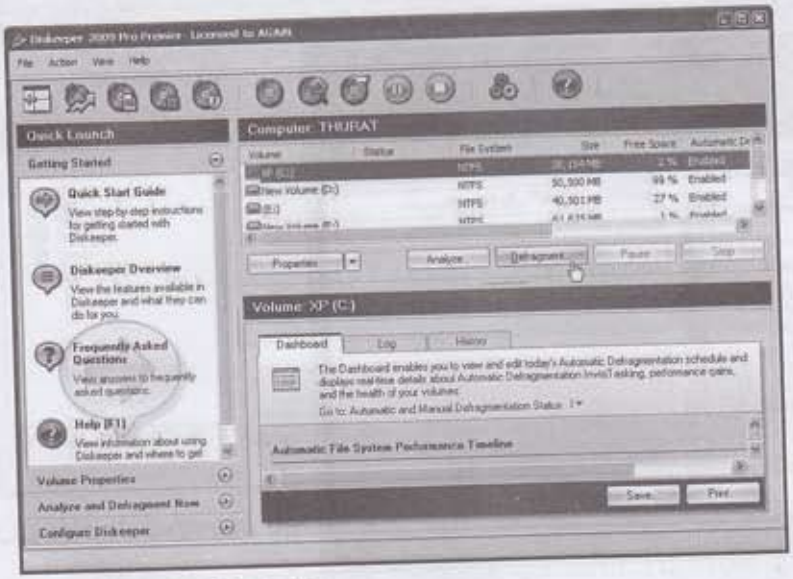
❑ Handy Recovery

Handy Recovery သည်လည်း hard disk များ၊ floppy များပေါ်မှ မတော်တဆမှားယွင်းဖျက်မိသော data များ၊ file များကိုပြန်လည်ရှာဖွေရယူနိုင်သော software တစ်ခုပင်ဖြစ်ပါတယ်။ Handy Recovery ကို **www.handyrecovery.com** မှ download ရယူနိုင်ပါတယ်။



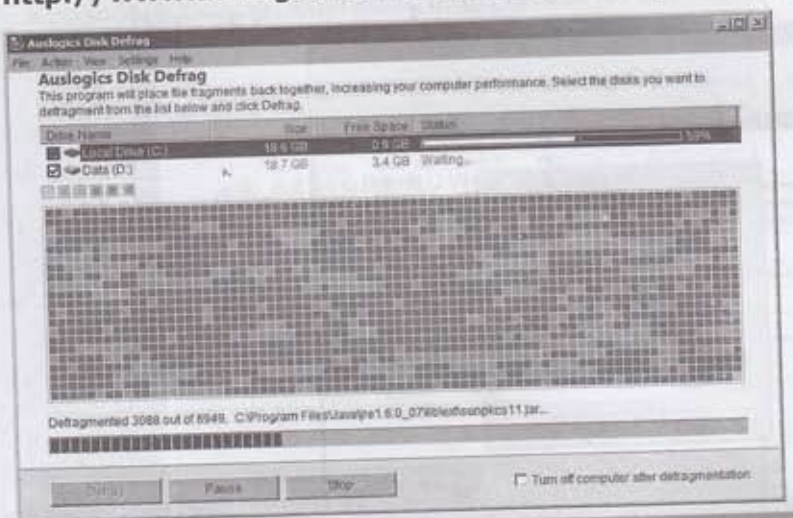
❑ Diskeeper

Disk defragmentation utility တစ်ခုပင်ဖြစ်ပြီး Window တွင်ပါရှိသော disk defragmenter နေရာတွင် အစားထိုးသုံးစွဲသွားနိုင်ပါတယ်။ တစ်ချိန်တည်းတွင် disk drive တစ်ခုထက်မကကို analysis လုပ်နိုင်၊ defrag လုပ်နိုင်ခြင်း ဟူသောအားသာချက်များ ပါရှိပါတယ်။ **http://www.executive.com** မှ download ရယူနိုင်ပါတယ်။



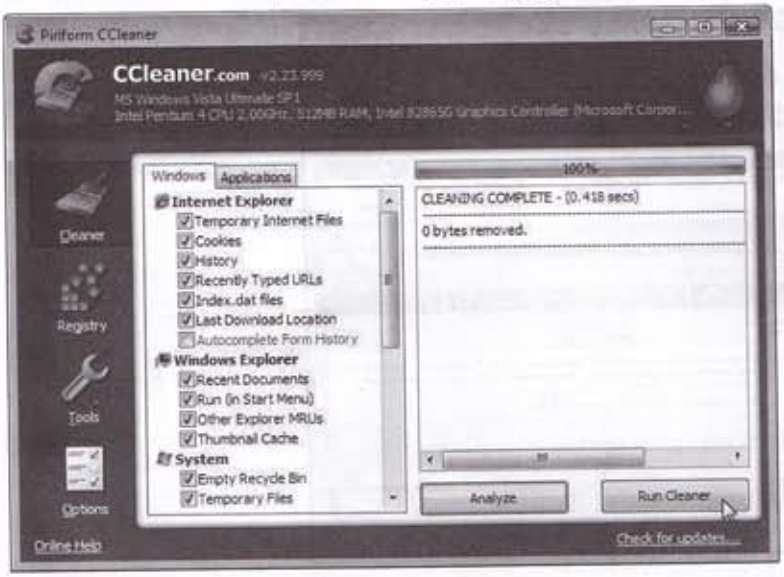
❑Auslogics Disk Defrag

Auslogics Disk Defrag သည်defrag လုပ်ရာတွင် သုံးနိုင်သည့် tool တစ်ခုပင်ဖြစ်ပါတယ်။ အသုံးပြုရလွယ်ကူပြီး ပေါ့ပါးမြန်ဆန်စွာလုပ်ဆောင်နိုင်သည့် အခမဲ့ freeware တစ်ခုလည်းဖြစ်ပါတယ်။ **http://www.auslogics.com/en/software** ကနေ download ရယူသုံးနိုင်ပါတယ်။



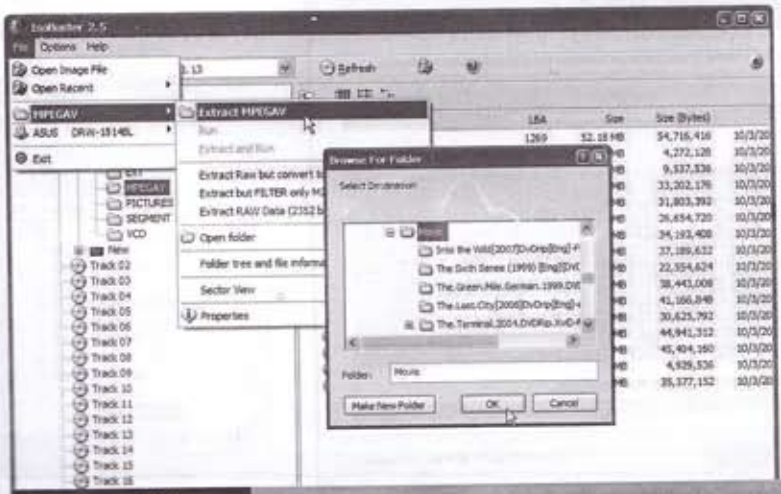
❑CCleaner

CCleaner သည်ကွန်ပျူတာတွင်းမှအသုံးမရှိတော့သော file များ၊ internet history နှင့် temp file များကိုရှင်းလင်းဖယ်ရှားပြီး ကွန်ပျူတာ၏စွမ်းဆောင်ရည်ကို တိုးမြင့်စေနိုင်သော freeware တစ်ခုပင်ဖြစ်ပါတယ်။ဒါ့အပြင် registry error များကိုရှင်းလင်းဖယ်ရှားရန်အတွက်လည်းသုံးနိုင်ပါတယ်။ **http://www.ccleaner.com** မှ download ရယူအသုံးပြုနိုင်ပါတယ်။



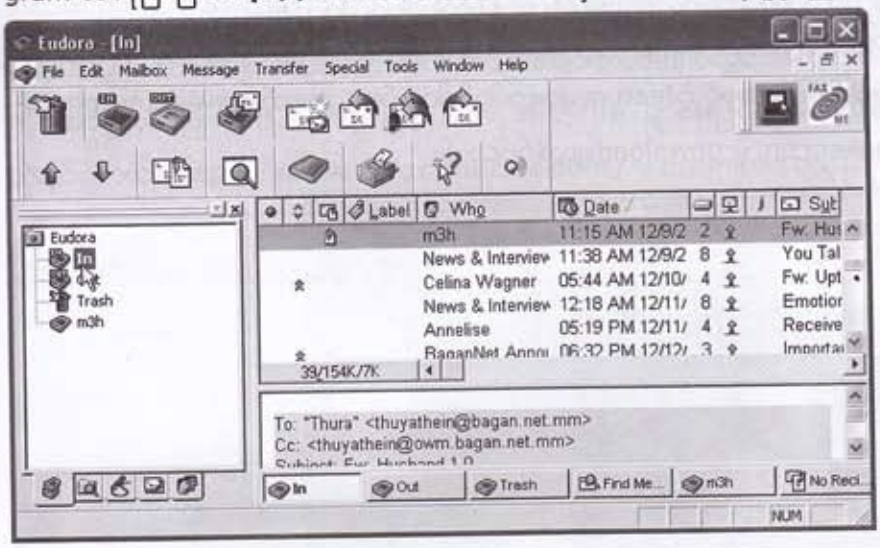
❑IsoBuster

IsoBuster သည်ပုံမှန်အတိုင်းပြန်ဖတ်မရနိုင်တော့သောCD ၊DVD အဟောင်းအပျက်များထဲမှ Document များ၊ image file များအားပြန်လည်ရရှိအောင် ဆယ်ယူပေးနိုင်သော tool တစ်ခုဖြစ်ပါတယ်။ **http://www.smart-projects.net/cdrecovery.php** မှ download ရယူအသုံးပြုနိုင်ပါတယ်။



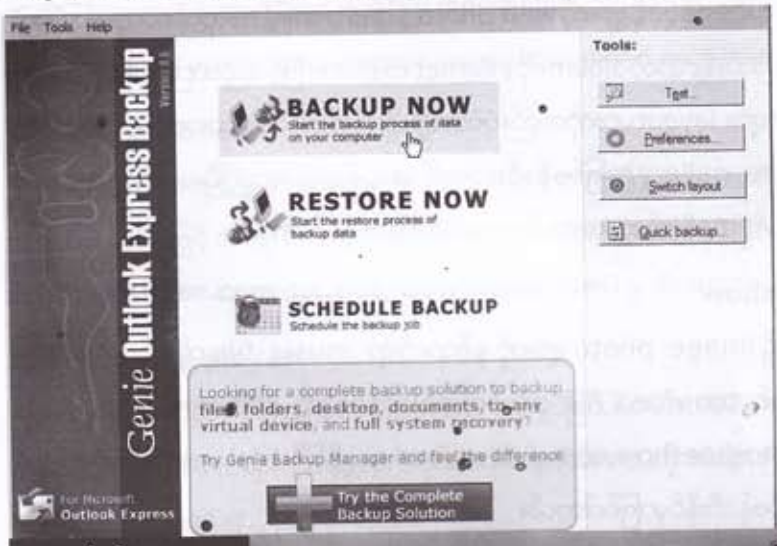
❑ Email client (Euroda)

Outlook Express,Microsoft Outlook တို့ကဲ့သို့ပင် Emaill များပို့လွှတ်ရယူနိုင်ရန် အသုံးပြုနိုင်သော email client programတစ်ခုပင်ဖြစ်ပါတယ်။ Eudrodaသည် shareware program တစ်ခုဖြစ်ပြီး **http://www.eudora.com**မှ download ရယူနိုင်ကြပါတယ်။



❑Outlook Express Backup

OE Backup သည် email message များ၊ setting များ၊ rule များ၊ address book တို့ကို backup လုပ်ကာသိမ်းဆည်းပေးနိုင်သော tools တစ်ခုပင်ဖြစ်ပါတယ်။ အဲဒီ backup လုပ်သိမ်းထားသည့် အထဲက message တွေ၊ address တွေလိုချင်ရင် အချိန်မရွေး Restore လုပ်ကာပြန်လည်ရယူနိုင်ပါတယ်။ **http://www.genie-soft.com/products/oeb/**မှ download ရယူနိုင်ကြပါတယ်။



❑ Acme Photo Screensaver Maker

Trial version အဖြစ် downloadရယူနိုင်တဲ့ professional အဆင့်ရှိတဲ့ softwareတစ်ခု ဖြစ်ပါတယ်။ photo imageများကိုသာမက Mp3၊ waveအစရှိတဲ့ music fileများကိုပါတွဲလျှက် screen saver ထဲထည့်သွင်းအသုံးပြုနိုင်ပါတယ်။ ဒါ့အပြင် ပုံတစ်ခုနှင့်တစ်ခုအကူးအပြောင်းတွင် transition effect များထည့်သွင်းနိုင်ခြင်း၊ ပုံတစ်ခုခြင်းကို caption များထည့်သွင်းနိုင်ခြင်း၊ မိမိစိတ်ကြိုက် background များရွေးချယ်နိုင်ခြင်းအစရှိတဲ့ featureများစွာပါဝင်ပါတယ်။ Acmeကို www.acme-photo-screensaver-maker.com မှ downloadရယူနိုင်ပါတယ်။

❑J Album

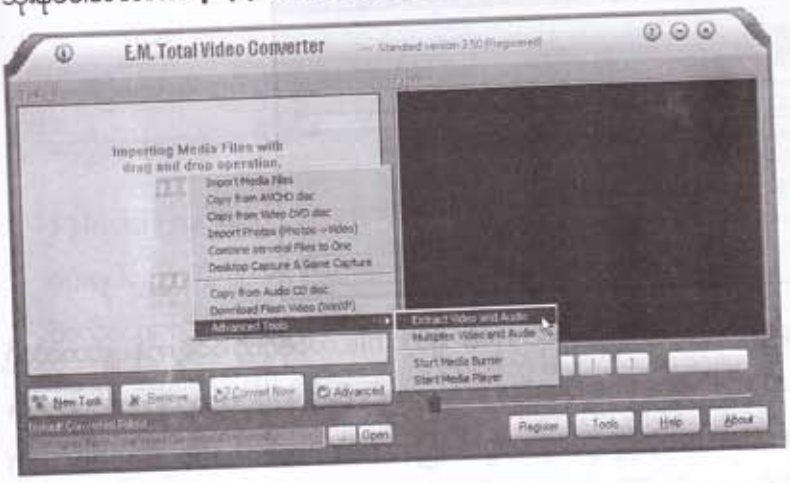
Computer အတွင်းရှိimageပုံများကို web photo album အဖြစ်အလွယ်တကူပြောင်းလဲနိုင်သော freewareပဲဖြစ်ပါတယ်။ရလာတဲ့albumကို internet explorerဖြင့်မည်သည့်ကွန်ပျူတာတွင်မဆိုဖွင့်နိုင်ပြီး color themeများ၊ layoutများကိုလည်းပုံစံအမျိုးမျိုးပြောင်းနိုင်ပါသေးတယ်။ internetရှိ မိမိ website ပေါ်တွင် photo gallery အဖြစ်ဖန်တီးရာတွင် အလွန်အသုံးတည့်ပြီးကောင်းမွန်တာကို တွေ့ရပါမယ်။ http://jalbum.net/သို့သွားရောက် downloadရယူနိုင်ပါတယ်။

❑Digital Photo slide show

ကွန်ပျူတာအတွင်းရှိ image photo များကို နှစ်သက်ရာ music file တို့ဖြင့်ပေါင်းစပ်ပြီး transition effectများပါဝင်သော video file အဖြစ်ပြောင်းလဲနိုင်သည့် softwareပဲ ဖြစ်ပါတယ်။ http://www.digitalphotoslideshow.comမှ download ရယူနိုင်ပြီးtrial versionမှာတော့ ခဲ့ ၅ပုံဖြင့်တစ်မိနစ်စာ videoကိုဖန်တီးနိုင်မှာဖြစ်ပါတယ်။

❑Total Video Converter

မည်သည့် video file အမျိုးအစားကိုမဆို handphone တို့၊ PDA တို့မှာထည့်သွင်းသုံးနိုင်သော video နှင့် audio file (mp4, 3gp, xvid, divx mpeg4 avi, amr audio)များအဖြစ်သို့ပြောင်းပေးနိုင်သော player program တစ်ခုပင်ဖြစ်ပါတယ်။ အဲဒီလို formatများသို့အလွယ်တကူပြောင်းလဲနိုင် သလို CD/DVD burnerအဖြစ်လည်းကောင်း၊ video file များထဲမှaudioချည်းသက်သက်ရအောင် extract လုပ်ကာခွဲထုတ်ပြီး(mp3,ac3,ogg,wav,aac)file များအဖြစ်သို့ပြောင်းတဲ့နေရာမှာလည်း သုံးနိုင်ပါတယ်။ **http://www.effectmatrix.com/** မှ download ရယူနိုင်ကြပါတယ်။



❑ VCD cutter

VCD နှင့် Movie fileများ (MPG, DAT, AVI, MOV, M1V, MPV) တို့နှင့်တွဲသုံးနိုင်သော MPEG playerတစ်ခုအဖြစ်အသုံးပြုနိုင်ပြီး movie fileမှလိုအပ်သော portionကိုလိုသလို cutလုပ်ယူနိုင် တယ်။ **http://www.vcd-cutter.com**မှ download ရယူနိုင်ပါတယ်။

❑ Audio Grabber

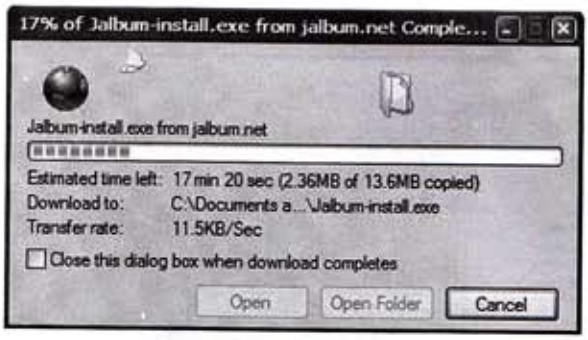
CD အတွင်းမှ သီချင်းများကို MP3 format (သို့) wav format များအဖြစ်သို့ quality ကောင်းကောင်းဖြင့် အလွယ်တကူပြောင်းနိုင်သော software တစ်ခုပဲဖြစ်ပါတယ်။ **http://www.audiograbber.com-us.net/download.html** မှ downloadရယူနိုင်ကြပါတယ်။

❑ VLC media player

VLC သည်freeware audio playerတစ်ခုပဲဖြစ်ပါတယ်။ mp2,mp3, voc,wav,midi,mods အစရှိသော audio file များကိုsupportလုပ်ပေးနိုင်ပါတယ်။ VLCကို **http://www.videolan.org/vlc** မှ download ရယူနိုင်ကြပါတယ်။

Internet Download Manager

Download လုပ်တယ်ဆိုတာ Internet ပေါ်မှာ Fileများကို မိမိရဲ့ကွန်ပျူတာထဲသို့ဆွဲယူခြင်းပဲ ဖြစ်ပါတယ်။ အဲဒီ File တွေဆိုတာဟာ စာသားများ၊အသံများ၊ ရုပ်ပုံ ဗီဒီယိုများ၊သီချင်းများနှင့် program fileများဖြစ်နိုင်ပါတယ်။ Internet Explorerဖြစ်ဖြစ်၊ Netscapeဖြစ်ဖြစ် Browser program တစ်ခုခုကိုအသုံးပြုပြီး file များကို download လုပ်ယူလိုတဲ့ file ပေါ်မှာ click တစ်ချက်နှိပ်လိုက်တာနှင့် Windowထဲမှ filedownload dialogue box ကျလာပါလိမ့်မယ်။



အဲဒီလိုဆွဲယူတဲ့နေရာမှာ ပုံမှန်အားဖြင့်ဆိုရင် 1MB ရှိတဲ့ file တစ်ဖိုင်ကို မိမိရဲ့ကွန်ပျူတာထဲသို့ ရောက်ရှိရန် Modem speed နှင့် Phone line Quality ပေါ်မူတည်ပြီး မိနစ် ၂၀မှ၃၀အထိကြာနိုင်ပါတယ်။ အဲဒါဟာ dialup connection အသုံးပြုသူတွေအတွက်ပြောတာပါ။ Broadband Connection အသုံးပြုသူတွေကတော့အဲဒီလောက်မကြာပါဘူး။ အဲဒါအပြင် download လုပ်ယူနေစဉ်အတွင်း Connection ပြတ်တောက်မှုများနှင့် ကြုံတွေ့ရလေ့ ရှိတဲ့အခါမျိုးမှာ အစကနေပြန်လည် download လုပ်ရတာကိုမကြာခဏာကြုံဘူးကြပါလိမ့်မယ်။

အဲဒီအခက်ခဲနှစ်ခုကို Internet Download Manager ကိုသုံးပြီးဖြေရှင်းနိုင်ပါတယ်။ IDM ဟာ Mirror site search ကိုအသုံးပြုပြီး download speed ကို ၄ဆမှ၅ဆ အထိမြှင့်တင်ပေးနိုင်ပါတယ်။ mirror site ဆိုတာ server တစ်ခုပေါ်မှာရှိတဲ့ file တစ်ခုကိုအခြား serverများပေါ်မှာပါ copy ပွားထည့်ပြီးတင်ထားခြင်းကို ဆိုလိုပါတယ်။ IDM ဟာ download ဆွဲယူမယ့် location ကိုရှာဖွေပြီးသည်နှင့် အနီးဆုံး mirror siteများနှင့်တပြိုင်တည်း Multiple connection ချိတ်ဆက်၍ segmentများခွဲကာ downloadလုပ်ယူပါတယ်။

နောက်တစ်ခုကတော့ resume downloadဆိုတဲ့ featureပဲဖြစ်ပါတယ်။အဲဒီ featureကတော့ download လုပ်နေစဉ်အတွင်း connection ပြတ်တောက်သွားခဲ့ပါက လက်ရှိ download ရယူပြီးတဲ့နေရာမှာရပ်ထားပါတယ်။ နောက်တစ်ကြိမ် connection ပြန်ရလာခဲ့အခါမှာ အစကနေပြန်ဆွဲစရာမလိုဘဲရရှိပြီးသားနေရာကနေဆက်လက် download ဆက်လုပ်ပေးသွားနိုင်ပါတယ်။

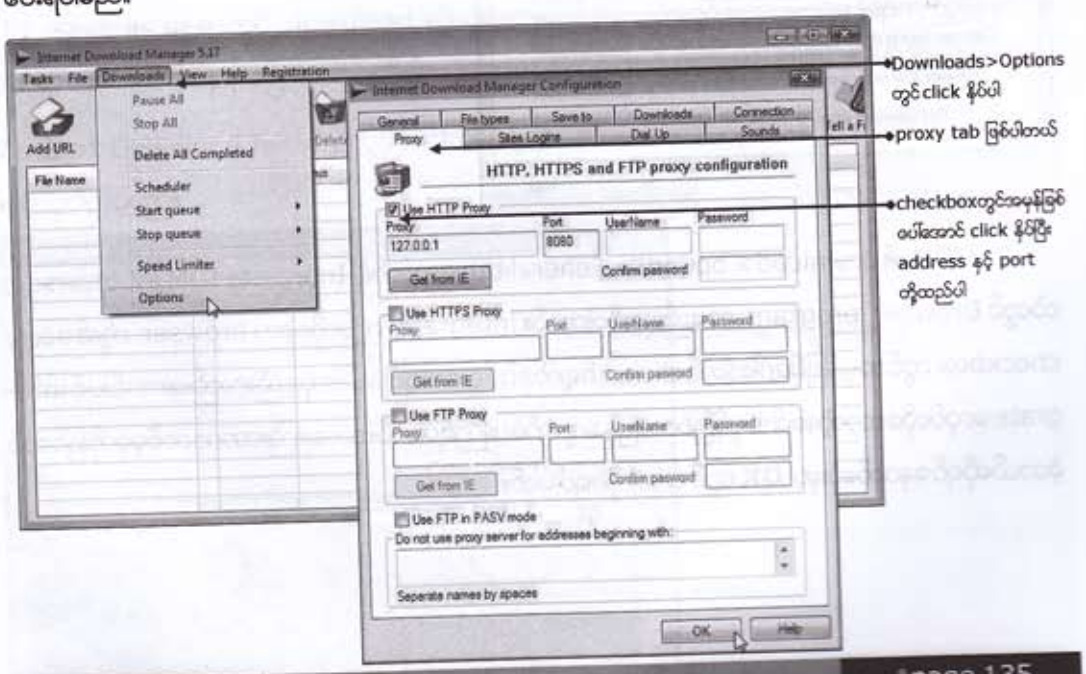
◈ Downloading IDM

IDM အား www.internetdownloadmanager.com/download.html သို့သွားရောက် download လုပ်ယူနိုင်ပါတယ်။ free download ရယူစမ်းသပ်သုံးမည့် IDM သည် feature အပြည့် သုံးခွင့်မပေးဘဲ usage limit ဖြင့်ကန့်သတ်ထားသော demoware တစ်ခုဖြစ်ပါတယ်။ register လုပ်ပြီးမှ သာလျင် IDM ဖြင့်အကန့်အသတ်မရှိdownload ရယူသုံးနိုင်ကြပါတယ်။

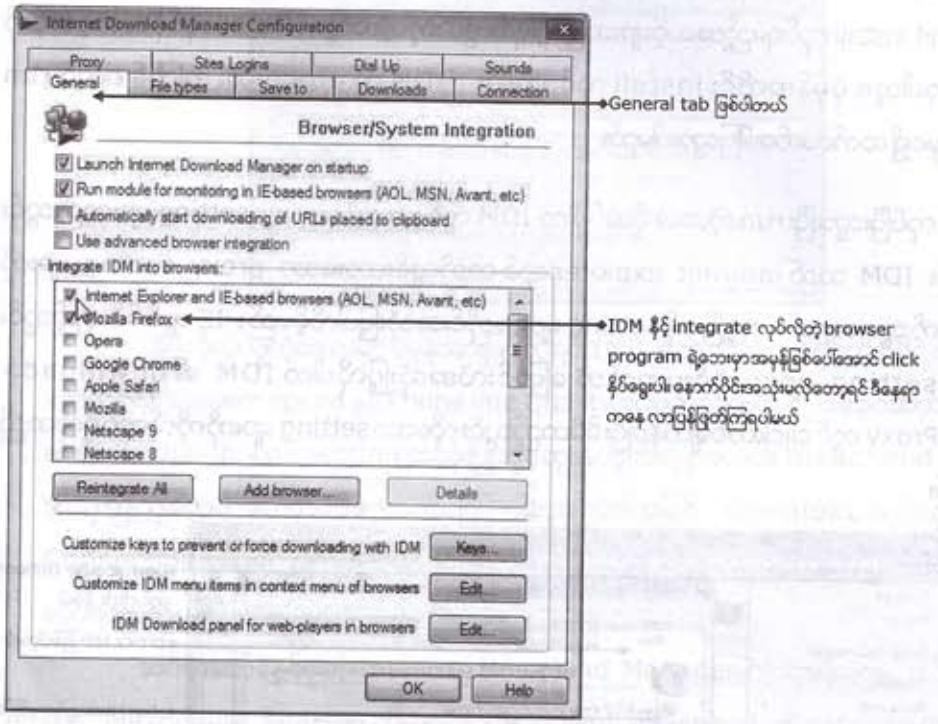
◈ Installing IDM

IDM install လုပ်ရမည့်အဆင့်များသည်ရိုးရှင်းလွယ်ကူတဲ့အတွက် install လုပ်ပုံအဆင့်ဆင့်ကို မဖေါ်ပြတော့ပါဘူး။ ပုံမှန်အတိုင်း install လုပ်သွားပြီး IDM ကို ပထမဦးဆုံး အကြိမ် စတင် run သည့်နေရာမှစ၍ ဆက်လက်ဖေါ်ပြသွားပါမည်။

1) Install လုပ်ပြီးသွားပြီး runတဲ့အခါလိုအပ်ပါက IDM တွင် proxy server setting များထည့်သွင်း ပေးရပါမည်။ IDM သည် internet explorer တွင် ထည့်သွင်းထားသော proxy setting များကို အလိုလျောက် သွားရောက်ဖတ်ရှုပြီး ထို setting များအတိုင်းအသုံးပြုပါလိမ့်မည်။ IE တွင် မိမိထည့်သွင်း ထားသော setting များအတိုင်းမဟုတ်ဘဲ ပြောင်းလဲအသုံးပြုလိုပါက IDM ၏ download> options>Proxy တွင် clickတစ်ချက်နှိပ်ပြီး မိမိထည့်သွင်းလိုသော setting များကို ကိုယ်တိုင်ရိုက်ထည့် ပေးရပါမည်။



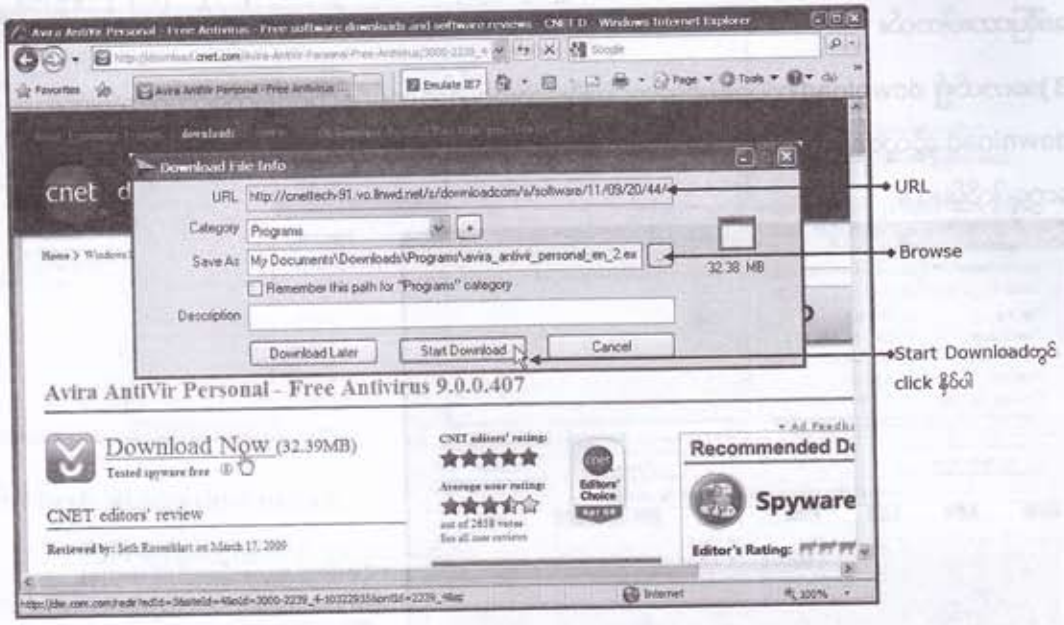
2) proxy setting များကို ထည့်သွင်းခဲ့ပြီးပါက ဘယ် browser နှင့် integration လုပ်မလဲ ဆိုတာ ရွေးပေးပုံကိုကြည့်ရအောင်။ သဘောကတော့ အင်တာနက်မှ download လုပ်ယူသည့် အခါတိုင်း IDM အလိုလျောက်ပွင့်လာပြီး downloadရယူခြင်းများကို လုပ်ဆောင်နိုင်စေရန် ဖြစ်ပါတယ်။ ဥပမာ IE နှင့် integrate လုပ်ထားရင် IE ထဲကနေ dowload တစ်ခုခုဆွဲလိုက်တာနှင့် windows download dialog box အစား IDM ပွင့်လာပြီး download ဆွဲယူပါလိမ့်မယ်။ ဒါပေမယ့် အချို့သော website တွေက IDM ဖြင့် download ဆွဲယူခြင်းကိုခွင့်မပြုဘူး။ အဲဒီလိုအခါမျိုးတွေမှာ integrate လုပ်ထားခြင်းကိုပြန်ဖြုတ်ပေးကြရတယ်။



IDM ၏ download> options>General tab အောက်ရှိ Integrate IDM int browsers ထဲတွင် Browser program အမည်များရှိပါတယ်။ integrate လုပ်လိုသော browser တို့၏ ဘေးမှ checkbox တွင် အမှန်ခြစ်ပေါ်အောင်clickတစ်ချက်နှိပ်ရွေးပေးရပါမယ်။ ထိုနည်းလည်းကောင်းပင် integrate မလုပ်လိုတော့တဲ့အခါအမှန်ခြစ်လာပြန် ဖျောက်ပေးကြရပါမယ်။ အရေးကြီးတာက တစ်ခုခုကိုပြင်ဆင်ခဲ့တယ်ဆိုရင် နောက်ဆုံးမှာ **OK** တွင် click နှိပ်ရပါမယ်။

◈Using IDM

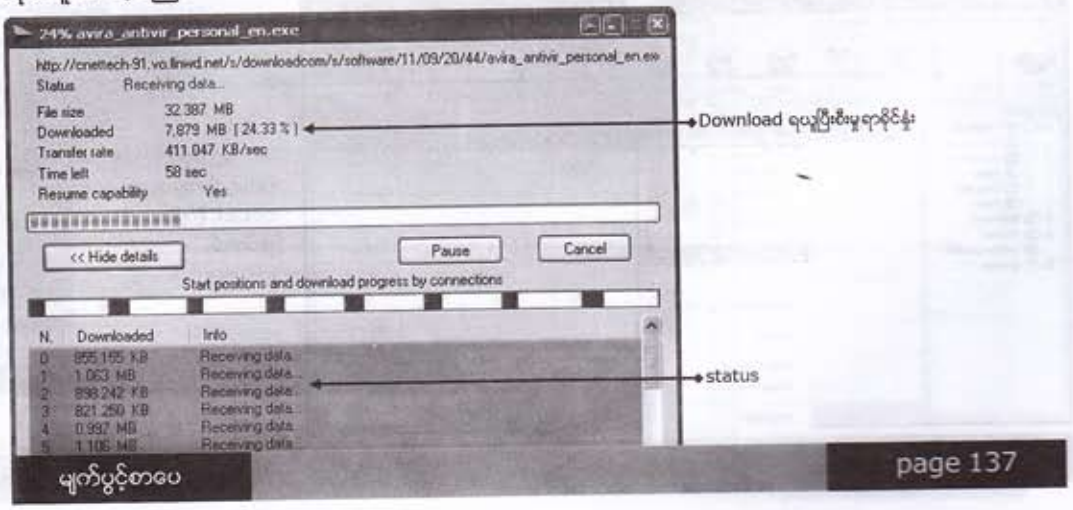
1) IDM အတွက် လိုအပ်သော setting များကို ပြည့်စုံမှန်ကန်စွာဖြည့်စွက်ခဲ့ပြီးပါက အင်တာနက်ပေါ်မှ downloadလုပ်သည့်အခါတိုင်း IDM windows ပွင့်လာပါလိမ့်မည်။



(a) URL တွင် မိမိ downloadဆွဲယူမည့် fileရှိရာနေရာ (URL)ကိုတွေ့ရပါမည်။

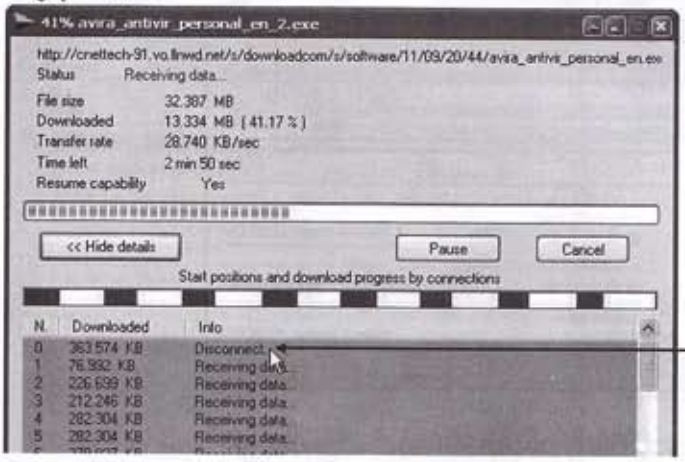
(b) save as နေရာတွင် download ဆွဲယူရလာမည့် file အားသိမ်းထားမည့်နေရာကို ညွှန်ပြထားပါတယ်။ အကယ်၍ နေရာပြောင်းသိမ်းလိုပါက **browse**တွင် click တစ်ချက်နှိပ်ပြီးပြောင်းနိုင်ပါတယ်။

2) Start Download button တွင် clickတစ်ချက်နှိပ်ပါက မိမိကွန်ပျူတာထဲသို့စတင် download လုပ်ယူပါလိမ့်မည်။

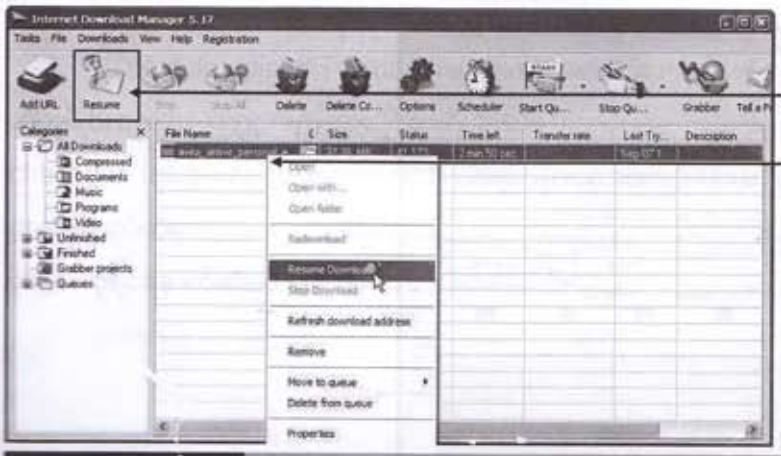


downloadရယူနေတဲ့ IDM interface ထဲက file sizeနေရာတွင် download ရယူမည့် fileဏ်အရွယ်အစား၊ downloaded နေရာတွင် download ရယူပြီးသော ပမာဏ၊ transfer rateတွင် download speedနှင့် time left တွင်ပြီးဖို့ရန်ခန့်မှန်းကြာချိန်တို့ကို ဖေါ်ပြထားပါတယ်။ ဒါ့အပြင် IDM interfaceရဲ့title barထဲမှာလည်း ဘယ်လောက်ပြီးသွားပြီဆိုတာကိုအလွယ်တကူသိနိုင်ရန် ရာခိုင်နှုန်းဖြင့် ဖေါ်ပြထားပါတယ်။

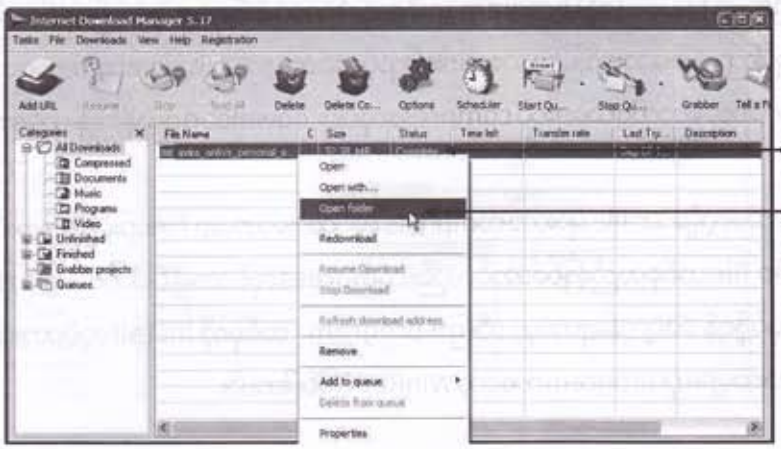
3)အကယ်၍ download လုပ်နေစဉ်အတွင်းမပြီးသေးခင်မှာဘဲ connectionပြတ်တောက်သွားတဲ့အခါ download ဆွဲယူနေသော IDM windows ထဲတွင် disconnectဟူသော error message များကို တွေ့ရပါလိမ့်မယ်။



4) ISP သို့connectionပြန်ယူပါ။ connectionရလာတဲ့အခါ IDM ကိုဖွင့်လိုက်ပါ။ IDM windows ထဲမှာ မိမိ download ဆွဲယူခဲ့သော file အား ရာခိုင်နှုန်းဘယ်လောက်ကူးပြီး သွားပြီဆိုတာကို မြင်ရပါလိမ့်မည်။ ဆက်လက် download လုပ်ရန်အတွက် file nameပေါ်တွင် click တစ်ချက်နှိပ်ပါက **Resume** button သည် activeဖြစ်လာတာကိုတွေ့ရပါမည်။

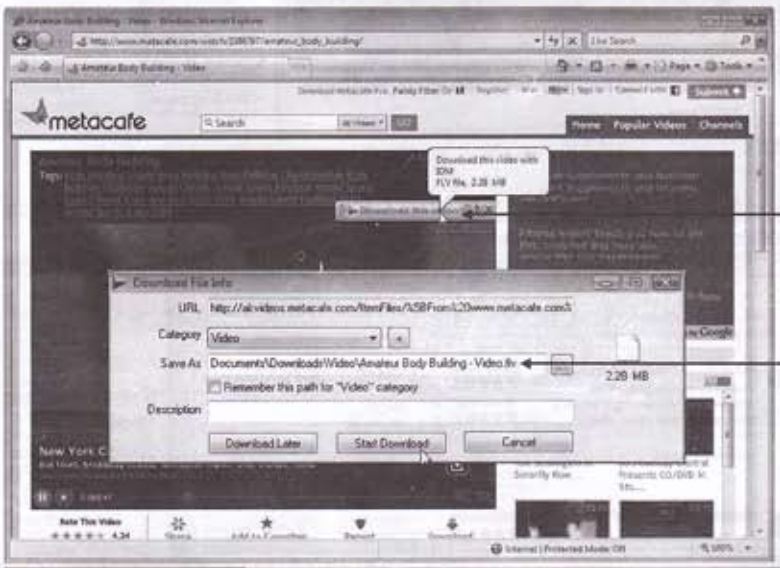


5) Resume button တွင် click နှိပ်ပါက အစဆုံးပြန်လည် download မလုပ်ဘဲမူလရရှိပြီးသားနေရာမှ ဆက်လက် download လုပ်ယူသွားတာကိုတွေ့ရပါလိမ့်မည်။ download ပြီးသွားတဲ့အခါမှာ မိမိဆွဲယူခဲ့တဲ့ file ရဲ့ status နေရာမှာ ရာခိုင်နှုန်းများအစား complete ဆိုတာကို တွေ့ရပါမည်။



◈ Flash Video download

IDM ရဲ့ feature သစ်တစ်ခုက webpage ထဲက flash video တွေကို IDM ဖြင့်တိုက်ရိုက် download ရယူနိုင်ခြင်းဖြစ်ပါတယ်။ webpage ထဲမှာ flash video ပါတယ်ဆိုရင် IDM ကိုယ်စားပြု သင်္ကေတကို တွေ့ရပါမယ်။ **Download this video** တွင် click နှိပ်ကာရယူနိုင်ပါတယ်။ဒီနေရာမှာ အရေးကြီးတာက IDM download box ထဲက Save as နေရာမှ filename သည် မိမိရယူမည့် file ဟုတ် မဟုတ်စစ်ဆေးရပါမယ်။ သေချာပြီဆိုရင် Start download တွင်click နှိပ်ကာရယူနိုင်ပါပြီ။



WinRar

ကွန်ပျူတာများကို အင်တာနက်နှင့် online ချိတ်ဆက်ပြီး file များကို share လုပ်၍ ကွန်ပျူတာ တစ်လုံးမှ တစ်လုံးသို့ ပို့လွှတ်ခြင်း၊ download ရယူခြင်းတို့ဟာ ယနေ့အချိန်မှာတော့ အသုံးများတွင်ကျယ် နေပါပြီ။ အဲဒီလိုအသုံးပြုကြရာမှာ file များ (သို့) program များရဲ့အရွယ်အစားပေါ်များစွာမူတည်နေပါတယ်။ ဆိုရရင် file size ကြီးနေရင်ကြာမယ်၊သေးရင်မြန်မယ်ပေါ့။ ဒါကြောင့် အင်တာနက်ပေါ်မှာ website အတော် များများဟာ file များကို မူလပထမထက်ငယ်အောင် compress လုပ်ပြီး download ရယူနိုင်ရန် တင်ထား လေ့ရှိပါတယ်။

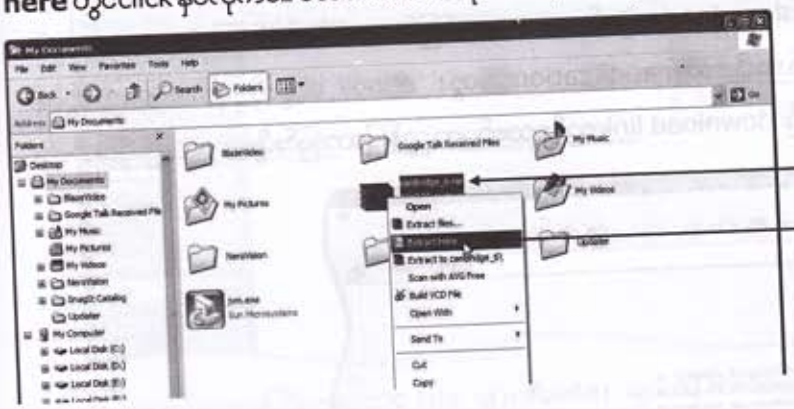
.zip ဖြင့်အဆုံးသတ်လေ့ရှိသော file များဟာ compress လုပ်ထားသော zip file များပဲဖြစ်ပါတယ်။ file များစွာကိုစုပေါင်းပြီး zip file တစ်ခုတည်းဖြစ်အောင်လည်း compress လုပ်ထားနိုင်ပါတယ်။ အဲဒီ zip file များကို unzip ပြန်လုပ်ဖို့ရန် မိမိရဲ့ကွန်ပျူတာမှာ သီးခြား program တစ်ခုကို install လုပ်ထားရန် လိုအပ်ပါတယ်။ ယနေ့အသုံးအများဆုံး program ကတော့ WinRar ပဲဖြစ်ပါတယ်။

Downloading WinRar

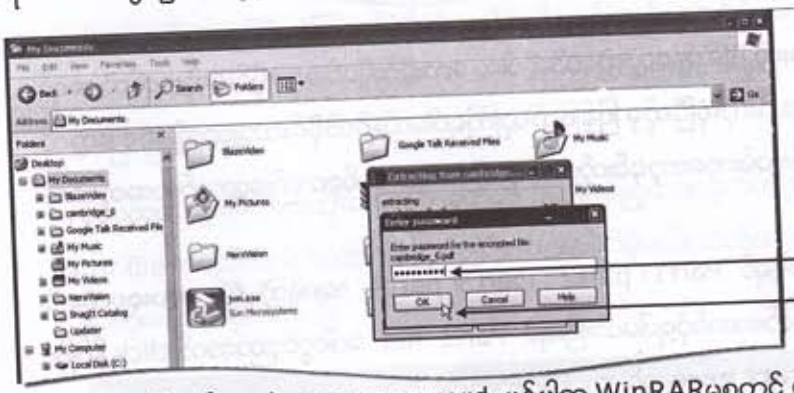
1) Winrar အား download ရယူရန် www.download.com သို့သွားပါ။ Search နေရာတွင် winrar ဟုရိုက်ထည့်ပြီး Go button တွင် click တစ်ချက်နှိပ်ပါ။ download now တွင် click နှိပ်၍ down-load ရယူပါ။

◈ ချုံ့ထားသော **RAR file** အားပြန်ဖြည်ခြင်း

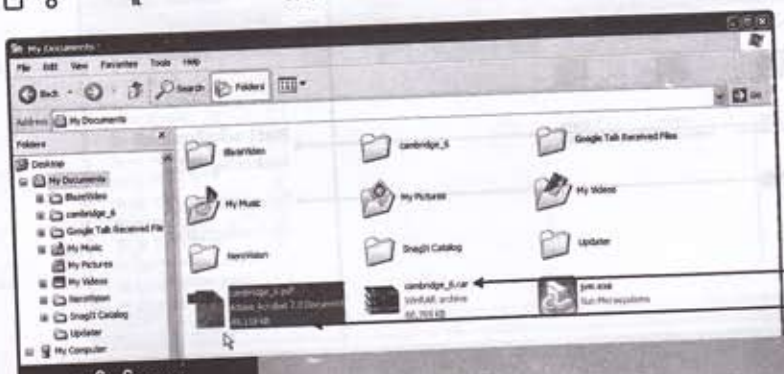
1) Extract လုပ်လိုသော RAR file ပေါ်တွင် ညာဘက် click နှိပ်ပါ။ ကျလာမည့် menu ထဲရှိ **extract here** တွင် click နှိပ်လိုက်ပါ။ စတင် extract လုပ်ပါလိမ့်မယ်။ လိုအပ်ပါက password တောင်းပါလိမ့်မယ်။



2) password ထည့်ပြီးချုံ့ထားသည့် file တွေကို ပြန်ဖြည်တဲ့အခါ ထိုနှိုက်မှုလ password ပြန်ထည့်ပေးရပါတယ်။ ဆွဲစဉ်အခါတုန်းက ကူးယူမှတ်သားထားသည့် password ထည့်ပြီး **OK** တွင် click နှိပ်လိုက်ပါ။

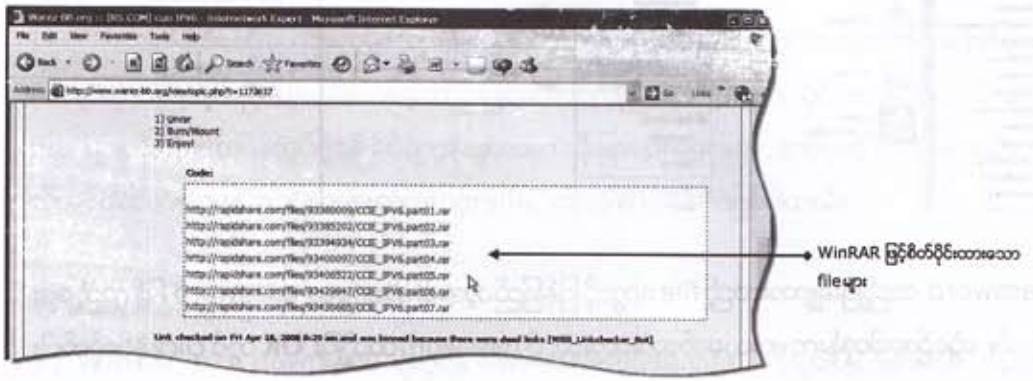


ထည့်သွင်းပေးခဲ့သော password မှန်ပါက WinRAR မှစတင် extract လုပ်ပါလိမ့်မယ်။ ပြီးသွားပါကမူလ RAR file ရှိရာ folder နေရာထဲမှာပင် သုံးနှိုင်ပြီဖြစ်တဲ့ ဖြည်ပြီးသား file ကိုတွေ့ရပါမယ်။



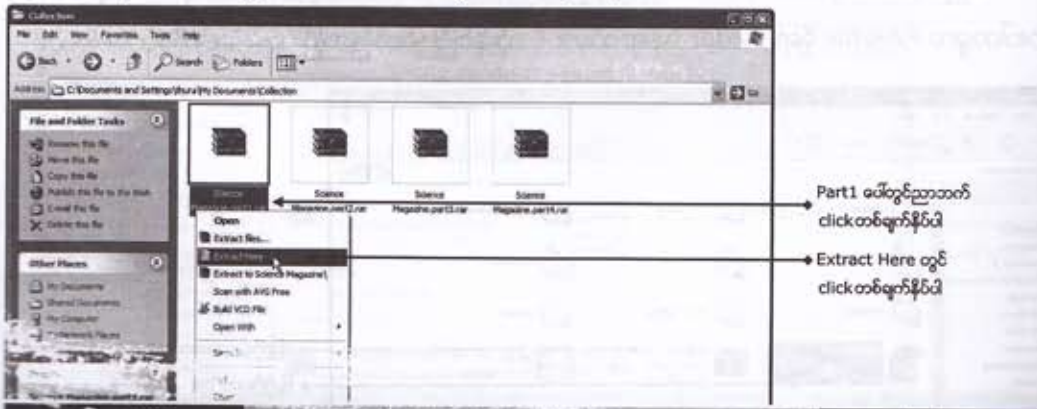
◈ စိတ်ပိုင်းထားသော RAR file များကိုပြန်ဖြည်ခြင်း

WinRar ကို compress လုပ်ရန်တစ်မျိုးတည်းအတွက် မဟုတ်ဘဲ အခြားရည်ရွယ်ချက်ဖြင့်လည်းသုံးနိုင်ပါသေးတယ်။အထူးသဖြင့်မူလအရွယ်ထက်ငယ်အောင်ချုံ့ပြီးသော်လည်း အရွယ်အစားကြီးနေသေးသည့် file တွေကို download ဆွဲရန် အလောတော်ဖြစ်အောင်စိတ်ပိုင်းကြတဲ့နေရာမှာလည်းသုံးကြပါတယ်။သည့်အတွက် အရှိုးသော application တွေ၊ ebook တွေကို download ဆွဲရန် part1,part2,part3...ဆိုပြီး download linkတစ်ခုထက်မကညွှန်ပြထားခြင်းမျိုးတွေလည်းရှိပါတယ်။

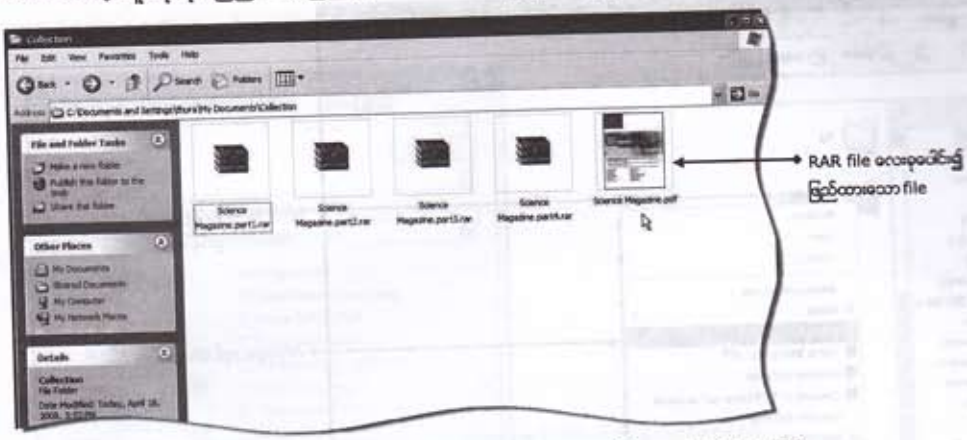


အဲဒီလို စိတ်ပိုင်းထားတဲ့ file မျိုးတွေဆွဲမယ်ဆိုပါက လေးပိုင်းရှိရင် လေးပိုင်းစလုံးစက်ထဲ အရင်ရောက်အောင် ဆွဲရပါမယ်။ အားလုံးစုံပြီဆိုမှ ပြန်ဖြည်ယူကြရပါမယ်။စိတ်ပိုင်းထားသည့် file တွေကို ပြန်ဖြည်ယူရန်အလွယ်ဆုံးနည်းလမ်းကတော့ ၎င်းတို့အားလုံးကို folder တစ်ခုတည်းအောက်မှာအတူတကွထားရှိရပါမယ်။

သဘောက လေးပိုင်းရှိရင် Part1၊ part2 ၊part3၊ part4 အစရှိတဲ့ file လေးခုစလုံးကို folder တစ်ခုထဲအောက်ရောက်အောင်ပို့ရပါမယ်။ပြီးရင် Part1 file ပေါ်တွင် ညာဘက် click နှိပ်ပြီး ကျလာမည့် menu ထဲရှိ **extract here**တွင် clickနှိပ်လိုက်ပါ။



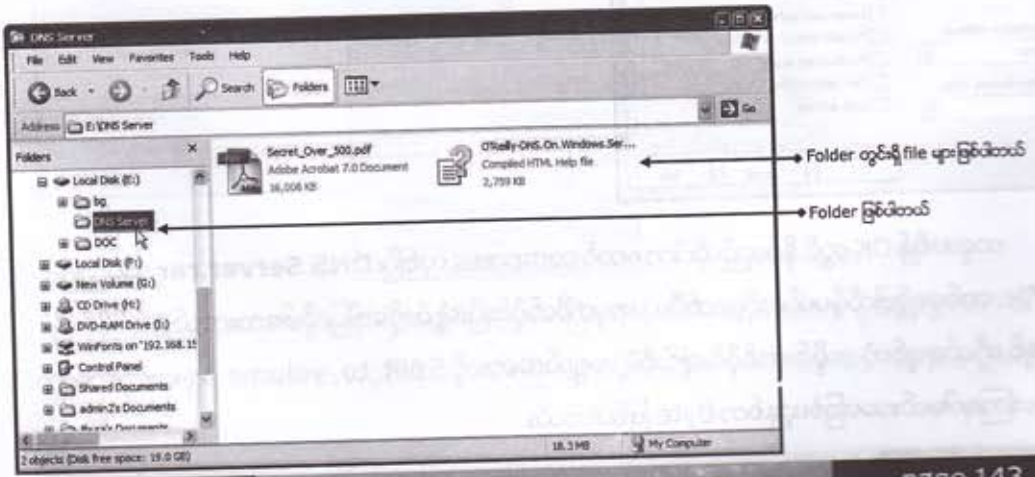
ကျန်သည့် Part2၊Part3၊Part4 တို့ကိုပါအလိုအလျောက်ဆက်ဖြည်သွားပြီးနောက်ဆုံးမှာတော့ အဆင်သင့်ယူသုံးနိုင်ပြီဖြစ်တဲ့ ဖြည်ပြီးသား fileတခုကိုတွေ့ရပါမယ်။



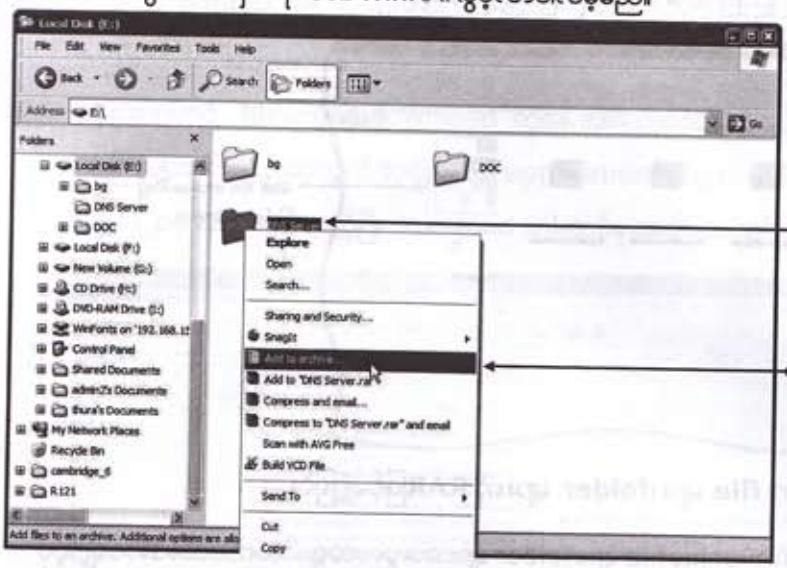
◈ အရွယ်အစားကြီးမားသော file များ၊folder များကို RARဖြင့်ချုံ့ခြင်း

ယခုဆက်လက်ပြီး WinRar ဖြင့် file များ၊ folder များအားမူလအရွယ်ထက်ငယ်အောင်ချုံ့ယူပုံအဆင့်ဆင့်တို့အားဖေါ်ပြသွားပါမယ်။ WinRar ဖြင့်တဖိုင်လ်ချင်းစီကိုချုံ့လိုရုံသလို၊ file တွေကို folder တစ်ခုထဲအောက်စုထည့်ပြီးချုံ့ကြမယ်ဆိုရင်လည်းရပါတယ်။ လုပ်ဆောင်ပုံများမှာလည်းအတူတူပင်ဖြစ်ပါတယ်။ ဒီနေရာမှာတော့ နှစ် ဖိုင်လ် ၊သုံးဖိုင်လ် လောက်ကို folder တစ်ခုထဲအောက်စုထည့်ပြီး ချုံ့ယူပုံများကိုဖေါ်ပြသွားပါမယ်။

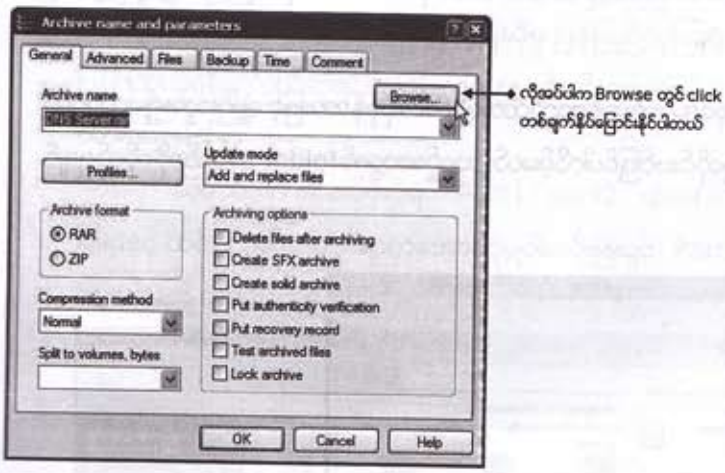
1) ပထမဦးစွာ file များကို folder တခုအောက်မှာစုထည့်ထားလိုက်ပါ။ပုံမှန်အားဖြင့် ချုံ့ပြီးသွား၍ရလာမည့် rar file အမည်သည် folder အမည်တိုင်းပင်ဖြစ်ပါလိမ့်မယ်။ သည့်အတွက် folder အမည်ကို ကိုယ်ရချင်သလိုပေးထားနိုင်ပါတယ်။



2) Compress လုပ်လိုသော folderပေါ်တွင် ညာဘက် click နှိပ်ပါ။ ကျလာမည့် menu ထဲရှိ **Add to Archive** တွင်click နှိပ်လိုက်ပါ။ WinRARဖွင့်လာပါလိမ့်မည်။

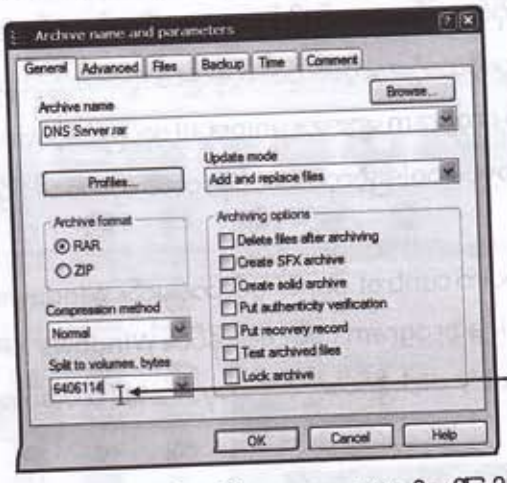


3) Compress လုပ်ပြီး၍ ရလာမည့် rar file နေရာကိုပြောင်းထားလိုပါက Browse တွင်နှိပ်ပြီး ပြောင်းနိုင်ပါတယ်။ ဒီအတိုင်းထားရင်တော့ ခုနက folder နေရာမှာပင်ဖြစ်ပါလိမ့်မယ်။

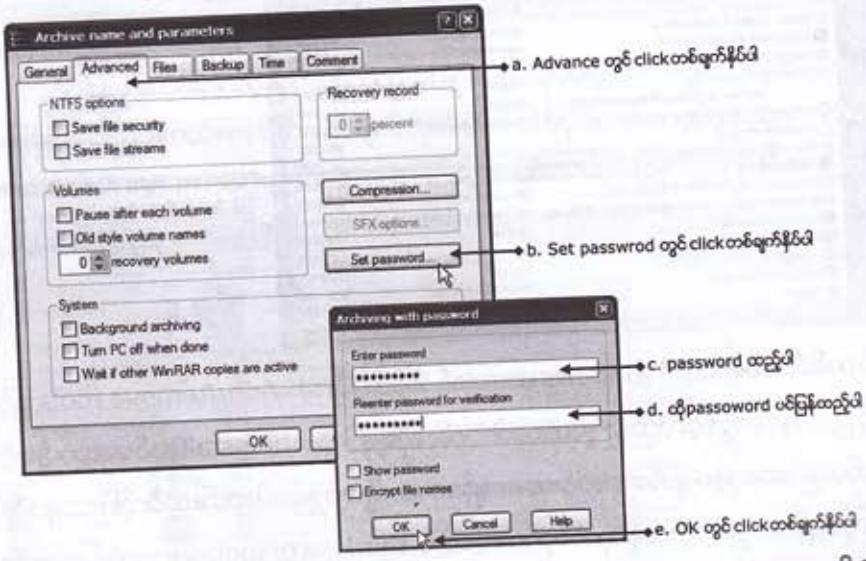


ယခုအချိန် OK တွင် နှိပ်မည်ဆိုပါက စတင် compress လုပ်ပြီး **DNS Server.rar** အမည်ဖြင့် Rar file တစ်ခုရရှိပါလိမ့်မယ်။ သို့သော်ဒီနေရာမှာ စိတ်ပိုင်းပြီးချုံ့ပုံကိုဖေါ်ပြလိုပါသေးတယ်။ စိတ်ပိုင်းပြီး ချုံ့ချင်ရင် ကိုယ်ရချင်တဲ့ အပိုင်းတစ်ပိုင်းချင်းစီရဲ့အရွယ်အစားကို Split to volume နေရာတွင်ထည့် သွင်းပေးကြရပါမယ်။ အခြေခံယူနစ်က Byte ဖြစ်ပါတယ်။

ဥပမာအနေနှင့် ပိုင်းကြည့်ရအောင် ။ မိမိ folder (DNS Server) ရဲ့အရွယ်အစားသည် 18.3MB(19,218,432 Bytes) ဖြစ်ပါတယ်။ ရလာမည့် တစ်ပိုင်းချင်းစီရဲ့အရွယ်ကိုသည် 6MB (6406114 Bytes)ထက်မပိုချင်ရင် ထိုပမာဏကို Split to volumes နေရာတွင်ထည့်ကြရပါမယ်။



နောက်တခါpassword ခံပုံကို ဖေါ်ပြပါဦးမည်။ **Advanced** တွင် Click နှိပ်လိုက်ပါ။ ထို့နောက် **Set password** တွင် Click နှိပ်လိုက်ပါ။password ထည့်ပြီးလျှင် **OK**တွင်Click နှိပ်လိုက်ပါက password box ပျောက်သွားပါလိမ့်မည်။

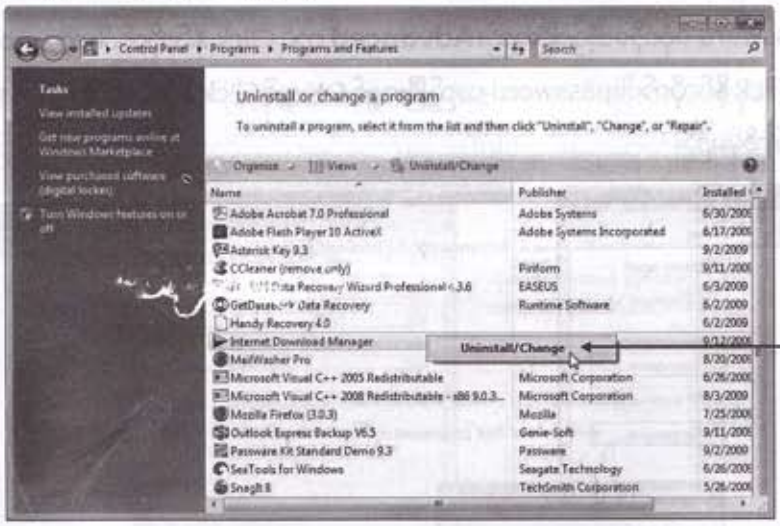


ဒါဆိုရင် compress လုပ်ဖို့အဆင်သင့်ဖြစ်ပါပြီ။ မူလ WinRAR Archive ရှိ**OK** button ပေါ်တွင် click နှိပ်ပါ။ စတင် compressလုပ်ပါလိမ့်မယ်။ ပြီးသွားတဲ့အခါ စိတ်ပိုင်းထားသော rar file များကို တွေ့ကြရပါမယ်။

Your Uninstaller

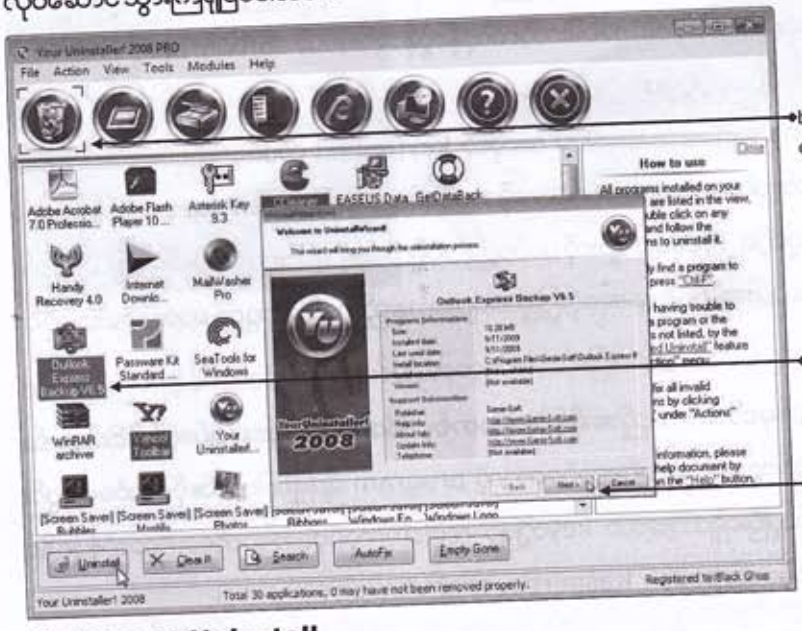
အသုံးပြုသူတို့အနေနှင့် trial period ကာလ ကုန်သွားလို့ပဲဖြစ်ဖြစ် အကြောင်းတစ်ခုခုကြောင့် ဆက်လက် အသုံးမရှိတော့တဲ့ program တွေကို ကွန်ပျူတာထဲကနေ ရှင်းထုတ်ပစ်ဖို့ တနည်းဆိုရရင် uninstall လုပ်ဖို့လိုအပ်ပါတယ်။ အသုံးမရှိဘဲ ဒီအတိုင်းဆက်ထားမယ်ဆိုပါက နေရာပုပ်မယ်။ အချို့ resources (CPU memory၊ hard disk space) တွေကိုယူသုံးနေတဲ့အတွက် ကွန်ပျူတာစွမ်းဆောင်ရည်ကို အနည်းနှင့်အများထိခိုက်စေတတ်ပါတယ်။ အဲဒီလို program များအား uninstall လုပ်ခြင်းကို windows မှာအဆင်သင့်ပါရှိပြီးသားဖြစ်တဲ့ Add/Remove toolsဖြင့်လုပ်ဆောင်နိုင်တယ် ဆိုတာ သိရှိပြီးဖြစ်ကြပါလိမ့်မယ်။

Start > Control Panel တွင် click နှိပ်ပါက control panel ပွင့်လာပါမယ်။ Windows vista သုံးသူတွေက program အုပ်စုထဲရှိ uninstall a program တွင် click နှိပ်ပါ။ Windows XP သုံးသူတွေက Add or Remove programs တွင် double click နှိပ်ပါ။ကွန်ပျူတာမှာ install ထားသော program များရဲ့list ကိုမြင်ရပါမယ်။



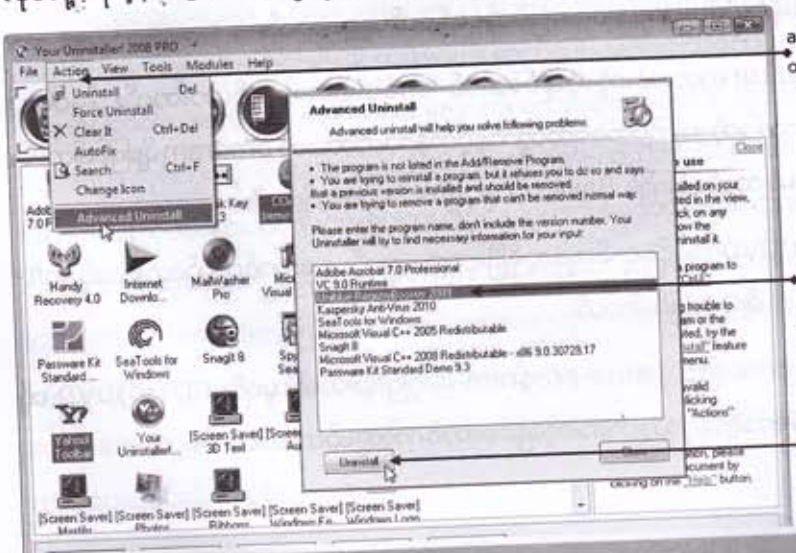
ဒါပေမယ့် တစ်ခါတစ်လေအဲဒီ windows မှာအဆင်သင့်ပါရှိပြီးသားAdd/Remove tools ဖြင့် ဖြေရှင်းလို့မရနိုင်တဲ့ပြဿနာတွေနှင့်လည်းကြုံရတတ်ပါတယ်။ ဆိုရရင် လုံးဝ uninstall လုပ်မရတာမျိုးနှင့် uninstallလုပ်သော်လည်းအကုန်မပျက်ဘဲတိုင်းတစကျန်နေတာမျိုးတွေဖြစ်ပါတယ်။ အဲဒီလိုပြဿနာမျိုးတွေကို uninstallလုပ်ရန်အတွက် သီးသန့်ထုတ်လုပ်ထားသော third Party toolsများအသုံးပြုဖြေရှင်းနိုင်ကြပါတယ်။ programတွေကို uninstallလုပ်တဲ့နေရာမှာ နာမည်အကြီးဆုံးနှင့် အသုံးပြုတဲ့ နေရာမှာ အလွယ်ကူဆုံးtoolsကတော့ Your Uninstaller ဖြစ်ပါတယ်။ **www.ursoftware.com**မှ download ရယူသုံးနိုင်ပါတယ်။

Your Uninstaller အားဖွင့်လိုက်ပါက ကွန်ပျူတာမှာ install ထားသော program များရဲ့ list ကိုမြင်ရပါမယ်။ ဖျက်ထုတ်လိုသော program တစ်ခုပေါ်တွင် ရွေးချယ် click နှိပ်ပြီး **Uninstall** button တွင် click နှိပ်ပါ။ Uninstaller wizard ကျလာမည်။ ပေါ်လာသောညွှန်ကြားချက်များအတိုင်း လိုက်ပါ လုပ်ဆောင် သွားကြရုံဖြစ်ပါတယ်။



Advance Uninstall

ပုံမှန်နည်းလမ်းဖြင့်လွယ်လွယ်ကူကူ uninstall လုပ်မရနိုင်တာမျိုးတွေကို advanced uninstall ဖြင့်ဖြေရှင်းနိုင်ကြပါတယ်။ စနစ်တကျမဖျက်ထုတ်ခဲ့ဘဲ တစ်ပိုင်းတစ်စကျန်နေသည့်အတွက် reinstall လုပ်လို့မရတဲ့ program တွေကို ဒီfeature ဖြင့် အရင်ရှင်းလင်းပြီး ပြန်လည် install လုပ်နိုင်ပါတယ်။



Type of Cracks

အခြို့ software တွေကို ကွန်ပျူတာမှာ Install လုပ်ပြီးတစ်ပတ်တန်သည်၊ တစ်လတန်သည် အသုံးပြုသွားတဲ့အခါ ဆက်လက်အသုံးပြု၍ မရတော့ပါ။ အချို့ကျပြန်တော့ Install ပြီး၍ စသုံးစဉ်ကာလ ကတည်းကိုက အချို့သော Feature တွေကို အသုံးပြု၍မရပါဘူး။ အဲဒီလို အပြည့်အဝအသုံးချမရနိုင်တာ တွေကို Function ပြည့်သုံးချင်တယ်(သို့) အစမ်းကာလကုန်လွန်သွားသည့် softwareတွေကို ဆက်သုံး ချင်သေးရင် register လုပ်ခိုင်းလေ့ရှိပါတယ်။

Registerလုပ်ဖို့ရန် software version အလိုက် key(ဝါ)text codeများရှိရပါမယ်။ အဲဒီtext codeတို့ကို softwareထုတ်လုပ်ရောင်းချသူ vendor တို့ထံမှ ဝယ်ယူကြရပါတယ်။ Registerလုပ်ခိုင်းခြင်း ရဲ့အဓိကရည်ရွယ်ချက်က သူတို့ရဲ့ Productများကို ဝယ်ယူခြင်းမရှိဘဲ သုံးပြုခြင်းမှကာကွယ်ရန်ဖြစ်ပါတယ်။ ကာကွယ်တားဆီးပုံ နည်းလမ်းအမျိုးမျိုးမှ အသုံးပြုမှုအများဆုံးနည်းလမ်း တွေက အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

Time Limit - သတ်မှတ်ထားသည့်အချိန်ကာလတစ်ခုထိအောင်သာအလုပ်လုပ်နိုင်ပါတယ်။ ကျော်သွားရင်အလုပ်မလုပ်တော့တဲ့ program မျိုးဖြစ်ပါတယ်။ ပိုက်ဆံပေးသွင်း ဝယ်ယူပြီးရရှိထားသော keyတို့ဖြင့် registerလုပ်မှသာ ဆက်လက်အသုံးပြုရနိုင် ပါလိမ့်မယ်။ ဥပမာ- Kaspersky trial Version

Demo Limit - Feature အချို့ကိုသာ အသုံးပြုနိုင်အောင် enable လုပ်သော program မျိုးဖြစ်ပါတယ်။ အထူးသဖြင့်တကယ့်အရေးအကြီးဆုံး(သို့) အသုံးအတည့်ဆုံး Featureကိုသုံးမရနိုင်အောင် disableလုပ်ထားလေ့ရှိပါတယ်။ Feature အားလုံး သုံးနိုင်တဲ့ full versionအဖြစ်သို့ရရန် ဝယ်ယူရပါတယ်။

Usage Limit - Featureအားလုံးကိုသုံးနိုင်အောင် enableတော့လုပ်ထားတယ်။ ဒါပေမယ့် အသုံးပြုတဲ့အကြိမ်အရေအတွက်နှင့်ကန့်သတ်ထားတဲ့ programမျိုးဖြစ်ပါတယ်။ ဥပမာ ဘယ်နှစ်ကြိမ် Save လုပ်ခွင့်ရှိတယ်ဆိုတာမျိုးပေါ့။

Copy Protection (Retail software) - CD/DVDတို့ဖြင့်ရောင်းချလေ့ရှိပြီးcopyကူးလို့မရအောင်ကွယ်ထားသည့် software မျိုးတွေဖြစ်ပါတယ်။

Disc Protection - အများအားဖြင့် game program တွေဖြစ်ပါတယ်။ မူရင်း CD(သို့)DVD တို့ driveထဲရှိနေမှသာ ကစားလို့ရနိုင်အောင်ကာကွယ်ထားပါတယ်။

Dongle Protection- Dongleလို့ခေါ်တဲ့ encryption device ကို USB (သို့) parallel port တစ်ခုခုမှာတပ်ဆင်ထားမှသာလျှင် program ကို အသုံးပြု၍ရပါတယ်။ ထို program ကိုဖြုတ်လိုက်တာနှင့် programသည် အလုပ်မလုပ်တော့ပါ။

ဒါတွေက software ထုတ်လုပ်ရောင်းချသူတွေက သူတို့ရဲ့ productများကိုဝယ်ယူခြင်းမရှိပဲ အသုံးပြု၍မရနိုင်အောင် ကာကွယ်ရန်အတွက် အသုံးပြုလေ့ရှိသော နည်းလမ်းများထဲက အသုံးပြုမှု အများဆုံး နည်းလမ်းအချို့ဖြစ်ပါတယ်။

◈ Understanding Crack

Crack လုပ်တယ်ဆိုတာက ရှေ့မှာဖော်ပြခဲ့တဲ့ usage Limit,time limitအစရှိတဲ့ကန့်သတ်ချက်များအား ဖယ်ရှားခြင်းဖြစ်ပါတယ်။ Vendorတွေဘက်က ကာကွယ်တားဆီးတဲ့နေရာမှာ နည်းလမ်းအမျိုးမျိုး သုံးကြသလို Crackလုပ်ဖို့ရန်အတွက်ကလည်း နည်းလမ်းများစွာရှိပါတယ်။

1) Serial codes (Serials)

အလွယ်ကူဆုံး Crack အမျိုးအစားဖြစ်ပါတယ်။ Serial ဆိုတာက trial ၊demo အစရှိတဲ့ကန့်သတ်ချက်များကို ဖယ်ရှားဖို့ရန် software ထုတ်လုပ်ရောင်းချသူတွေမှ ထုတ်ပေးသော text code များဖြစ်ပါတယ်။ serial key ၊product key လို့လည်းခေါ်ကြပါတယ်။ ဆိုရရင်ယခုလက်ရှိtrial အနေနှင့် activate လုပ်သုံးနေတဲ့ kaspersky2010 ကို key ထည့်လိုက်ရင် ရက် ၃၀စာ ကန့်သတ်ထားသည့် time limitကိုဖယ်ရှားလိုက်ခြင်းဖြစ်ပါတယ်။ဒီနေရာမှာ တစ်ခုသိထားသင့်တာကအင်တာနက်ကနေ free downloadဆွဲယူထားသည့် kaspersky Installer ပဲဖြစ်ဖြစ်၊ ဝယ်ယူထားသည့် CD ထဲမှာပါတဲ့ kaspersky Installer ပဲဖြစ်ဖြစ်အားလုံးဟာအတူတူပဲ။ ဝယ်တယ်ဆိုတာကအဲဒီ CD အိတ်ပေါ်မှာပါတဲ့ key (ဂါ) text code ကိုဝယ်ယူရခြင်းဖြစ်တယ်ဆိုတာကိုတော့ သဘောပေါက်ထားသင့်ပါတယ်။ အချို့ softwareတွေမှာကျတော့ keyတစ်ခုတည်းမဟုတ်ဘဲ username နှင့် product key ဆိုပြီး အတွဲလိုက် ထည့်ပေးရခြင်းမျိုးတွေရှိပါတယ်။

ဒါတွေကို manufacturer တွေကမပေးဘဲ ဘယ်လိုရနိုင်သလဲဆိုတော့ ကျွမ်းကျင်သည့် Cracker များက Crackလိုသော softwareတို့ရဲ့ registration Algorathm ကိုနားလည်သဘောပေါက်အောင် လေ့လာပြီးကောင်းစွာအလုပ်လုပ်တဲ့ တနည်းဆိုရရင် ကန့်သတ်ချက်များကို ဖယ်ရှားနိုင်တဲ့ key များ၊ text codeများကို ဖော်ထုတ်နိုင်ကြပါတယ်။ဤတွင်မှ ဝယ်ယူမှသာရနိုင်တဲ့ key များအတိုင်းကောင်းစွာအလုပ်လုပ်တဲ့ text codeများကို အင်တာနက်ကနေဖြန့်ဝေလေ့ရှိသည့်အတွက်မဝယ်ပဲရရှိနိုင်ကြပါတယ်။

Vendorတွေကလည်း အဲဒီလို keyများထွက်နေပြီဆိုတာခြေရာခံမိရင် ၄င်းတို့ကို blacklistထဲထည့်လေ့ရှိပါတယ်။သည့်အတွက်နောက် Version အသစ်ထွက်လာတဲ့အခါဖြစ်စေ၊ Update လုပ်တဲ့အခါဖြစ်စေ blacklist key ဖြင့်အလုပ်လုပ်နေသော program များသည် ဆက်လက်အလုပ်မလုပ်တော့ပါ။

အနှစ်ချုပ်ရရင် registerလုပ်ရန်အတွက် ၄င်းsoftwareနှင့် သက်ဆိုင်သော text code(serial) ရှိရပါမယ်။ ၄င်း serialတွေကိုအောက်ဖော်ပြပါ file formatနှစ်ခုဖြင့်ရရှိနိုင်ကြပါတယ်။

a) Text file

b) Keygen file

❑Text file

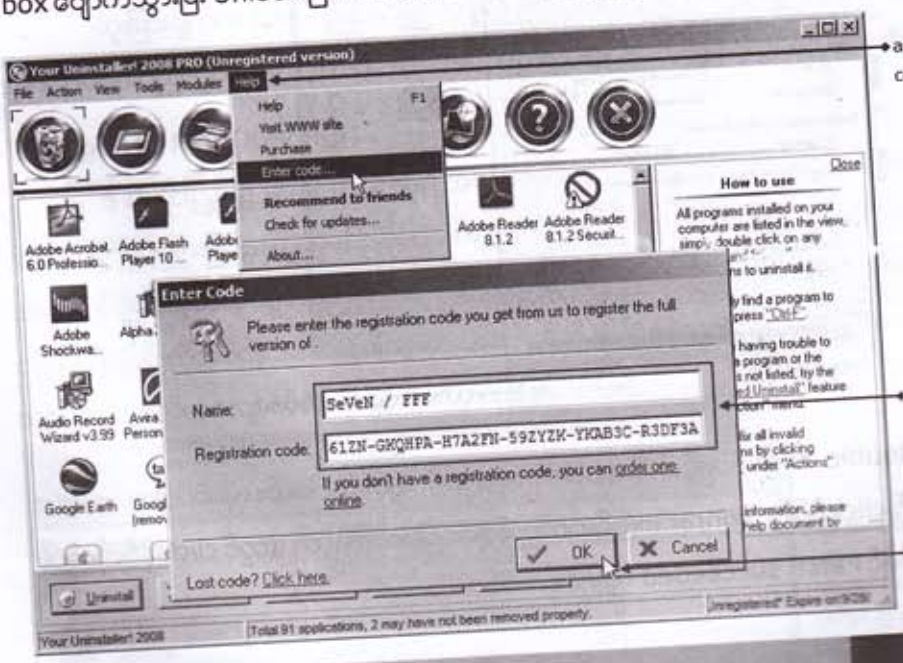
သက်ဆိုင်ရာ software နှင့်အတူ text fileပါလာရင်တော့ အရှင်းဆုံးဖြစ်ပါတယ်။အများအားဖြင့် key.txt ၊ serial.txt ဆိုတဲ့အမည်မျိုးတွေဖြင့်လာလေ့ရှိပါတယ်။ ထို file တွေကို double click နှိပ်ဖွင့်လိုက်ရင် notepad ဖြင့်ပွင့်လာပြီး register လုပ်ဖို့ရန် လိုတဲ့ serial(text code)တွေကို အလွယ်တကူရရှိနိုင်ပါလိမ့်မယ်။

❑Keygen

keygen ရဲ့အဓိပ္ပါယ်က key generator ဖြစ်ပြီး exe file များပင်ဖြစ်ပါတယ်။ CDkey ၊ serial number ၊ activation number ၊ license code များထုတ်ပေးနိုင်သော programတစ်မျိုးလို့လည်း ခေါ်နိုင်ပါတယ်။ ၎င်း keygen fileကို double click နှိပ်ဖွင့်၍ပွင့်လာတဲ့အခါ ရှေ့ဘာဆက်လုပ်ရမလဲ ဆိုတာကို အလွယ်တကူသိနိုင်ကြပါလိမ့်မယ်။ တစ်ခါတစ်လေအမည်တစ်ခု(သို့) အချက်အလက်တစ်ခု (ဥပမာ - emailလိပ်စာ) ထည့်သွင်းပေးရတာမျိုးတွေလည်းရှိပါတယ်။ ပြီးလျှင် Generate (အခြားစာလုံး လည်းဖြစ်နိုင်ပါတယ်) ကို click နှိပ်တဲ့အခါ registerလုပ်ဖို့လိုအပ်တဲ့ serial key ၊ product key များ ရရှိပါလိမ့်မယ်။

❑Key(text code) ထည့်သွင်းcrack ပုံများ

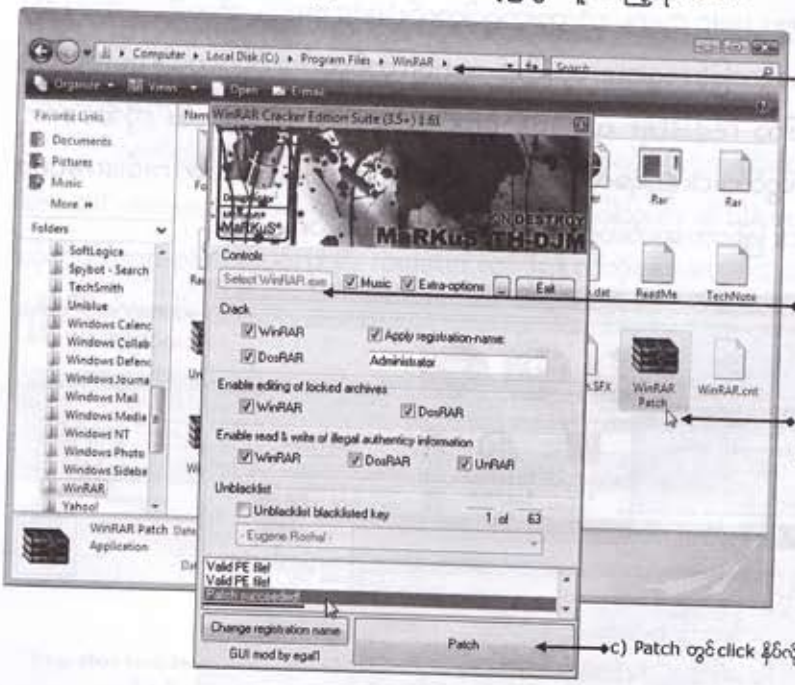
software အတွက်လိုအပ်တဲ့ key(text code)တွေရှိပြီဆိုရင် စတင် unlockလုပ်လို့ရပါပြီ။ အချို့သော programတွေကို စဖွင့်စဉ်မှာကတည်းကိုက registration လုပ်ဖို့တောင်းဆိုတတ်ပါတယ်။ အချို့ကအဲဒီလိုမတောင်းပါဘူး။ Help menu ထဲသွားရှာရပါတယ်။ Help menu ထဲမှာ Register (သို့) Activate(သို့) Unlockအစရှိသဖြင့် registerလုပ်ဖို့ရန် option တစ်ခုခုပါလေ့ရှိပါတယ်။ ၎င်း option တစ်ခုခုပေါ်မှာ click နှိပ်ပါက register လုပ်ဖို့ရန် box တစ်ခုပွင့်လာပါလိမ့်မယ်။ လိုအပ်သော keyများထည့်သွင်းပြီး OKတွင် clickနှိပ်ရလေ့ရှိပါတယ်။ ထည့်သွင်းခဲ့တဲ့ key မှန်ပါက registration box ပျောက်သွားပြီး Unlock ဖြစ်ကာ ဆက်လက်အသုံးပြုရသွားပါလိမ့်မယ်။



Patch file

Patch ဆိုတာက crack လုပ်မည့် software program ထဲက Registry နှင့်ဆိုင်တဲ့ code တွေကိုပြောင်းလဲပစ်ဖို့ရန် ဦးတည်လုပ်ဆောင်တဲ့ program ငယ်လေးတစ်ခုပင်ဖြစ်ပြီး၊ ရလဒ်အနေနှင့်ကတော့ crackလုပ်ခံရတဲ့ software အား သူကိုယ်သူ register လုပ်ပြီးသားလို့အထင်ရောက်သွားစေကာ demo၊ time limit များကို ဖယ်ရှားစေပါလိမ့်မယ်။ Patch.exe၊ software_Patch:exe၊ Crack.exeဆိုတဲ့ အမည်များဖြင့်လာလေ့ရှိပါတယ်။

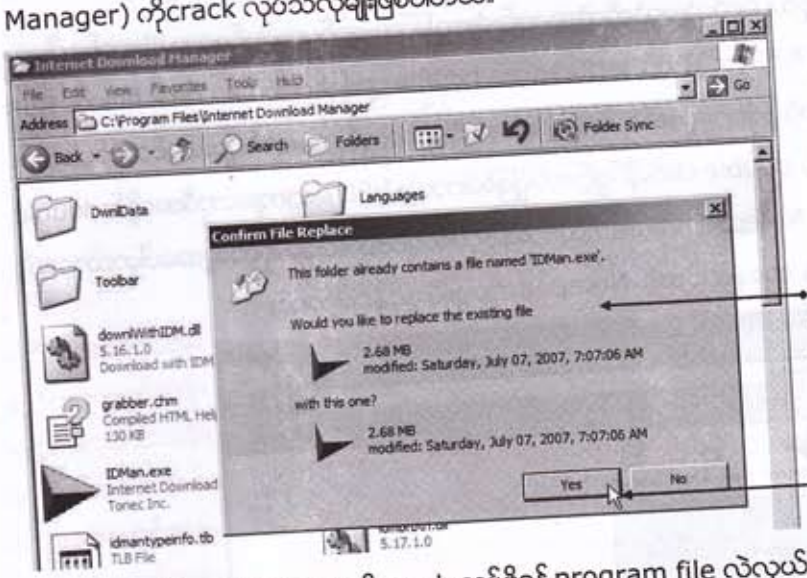
Patchမလုပ်ခင် ပထမဦးဆုံးသိထားရမှာက မိမိ crack လိုသော programနှင့်ဆိုင်သော file တွေသည်ကွန်ပျူတာထဲက ဘယ် drive၊ ဘယ် folder အောက်မှာရှိသလဲဆိုတာဖြစ်ပါတယ်။ အများအားဖြင့် C:\program file\program name ဖြစ်ပါတယ်။ ဥပမာ Window XP မှာ WinRaR ကို Install ပါက ၄င်းနှင့်ဆိုင်သော program file တွေရှိရာနေရာသည် C:\program file\Winrarဖြစ်ပါလိမ့်မယ်။ Window Vista မှာတော့ Computer ▶ Local Disk (c:) ▶ Program Files ▶ WinRAR ဖြစ်ပါလိမ့်မယ်။ Patch fileကို၄င်း folder ထဲသို့ဦးစွာကူးထည့်ရပါမယ်။



ပြီးလျှင်double click နှိပ်ဖွင့်ပါက crack program ပွင့်လာပါမယ်။ လိုအပ်ပါက select WinRar.exe တွင် clickနှိပ်ပြီး Winrar.exeရှိရာကိုညွှန်ပေးရပါမယ်။Patch itတွင် click နှိပ်လိုက်ပါ။ အောင်မြင်တယ်ဆိုရင် Patch succeeded လို့မြင်ရပါလိမ့်မယ်။

Cracked.exe

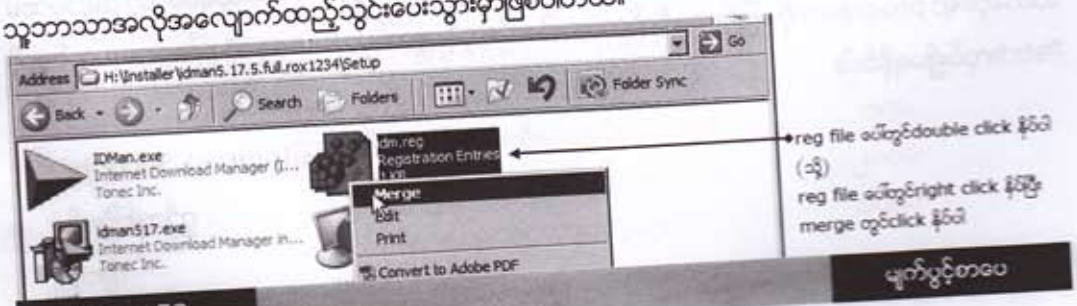
Cracked ဆိုတာ crack လုပ်ထားပြီးသား program file တစ်ခုပင်ဖြစ်ပါတယ်။ မိမိသုံးလိုတဲ့ software ကိုပုံမှန်အတိုင်း Install လုပ်ရမယ်။ Install ပြီးသွားရင် program fileတွေထဲက .exe (သို့) .bat fileတစ်ခုခုကို အဆင်သင့် crack လုပ်ထားပြီးသား file နှင့်လဲလှယ်ထည့်သွင်းပေးရပါတယ်။ ပြီးတဲ့အခါအဲဒီ program သည် register လုပ်ပြီးသားဖြစ်သွားပါမယ်။ ဥပမာ IDM(Internet Download Manager) ကိုcrack လုပ်သလိုမျိုးဖြစ်ပါတယ်။



ထူးခြားချက်က IDM ကို crack လုပ်ဖို့ရန် program file လဲလှယ်ရုံတစ်ဆင့် တည်းနှင့် မရဘူး။ serial key ထည့်သွင်းခြင်း (သို့) reg file အားdouble click နှိပ် run ခြင်းထပ်မံလုပ်ပေးဖို့လိုအပ်ပါတယ်။

Registry File (key file)

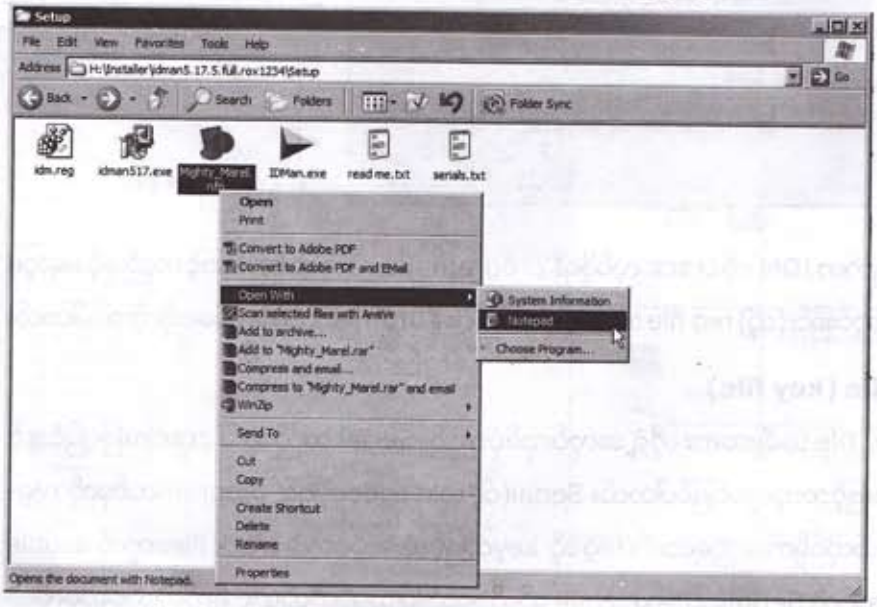
ဒီ crack file အမျိုးအစား တို့ရဲ့အလုပ်လုပ်ပုံသည် Serial ထည့်သွင်း crackဖြေရှင်းနှင့် သဘောတရားအားဖြင့် အတူတူပင်ဖြစ်ပါတယ်။ Serial(ဂါ) text codeတို့ဖြင့် programတစ်ခုကို register လုပ်ဖို့ရန် ကိုယ်တိုင်ရိုက်ထည့်ရတယ်။ reg သို့ keyတို့ဖြင့်ဆုံးလေ့ရှိတဲ့ ဒီ crack fileတွေကို double clickနှိပ်ရုံဖြင့် လိုအပ်တဲ့ Serial(ဂါ)text code တို့ကို အသုံးပြုသူတို့ကိုယ်တိုင် ရိုက်ထည့်စရာမလိုဘဲ သူဘာသာအလိုအလျောက်ထည့်သွင်းပေးသွားမှာဖြစ်ပါတယ်။



ယခုဆိုရင် crack လုပ်ပုံအမျိုးမျိုးနှင့် ၄င်းတို့အားအသုံးပြုပုံများကို အကြမ်းမျဉ်းသဘောပေါက်ခဲ့ပြီ ဖြစ်ပါလိမ့်မယ်။သူတို့ကို မှန်မှန်ကန်ကန်သုံးနိုင်အောင် မသုံးခင်မှာအောက်ဖော်ပြပါအချက်အချို့ကို သတိပြုလိုက်နာဖို့အရေးကြီးပါတယ်။

1) crack file အပါအဝင်အင်တာနက်မှ download ဆွဲယူခဲ့သော fileများအားအသုံးမပြုခင် Antivirus programဖြင့် မဖြစ်မနေစစ်ဆေးကြရပါမယ်။

2)crack fileတို့နှင့်အတူဘယ်လိုသုံးမလဲဆိုတဲ့အကျဉ်းချုံးညွှန်ကြားချက်များပါဝင်သော fileတစ်ခုပါလေ့ ရှိပါတယ်။အများအားဖြင့် NFO(သို့)Txt file(Readme.txt)file များဖြစ်ပါတယ်။ crack fileကိုမ Run ခင်၊ဒီ NFO(သို့) txt fileကိုမဖြစ်မနေဖတ်ရပါမယ်။အရေးကြီးသောညွှန်ကြားချက်များပါဝင်တတ်ပါတယ်။ txt fileကတော့ရှင်းတယ် double clickနှိပ်ဖွင့်ဖတ်ရုံဖြစ်ပါတယ်။ NFO တွေကျတော့ဒီအတိုင်း double clickနှိပ်ဖွင့်ဖတ်လို့မရဘူး Notepad programထဲကနေဖွင့်ဖတ်ရင်ဖတ်။ဒါမှမဟုတ်သူအပေါ်မှာညာဘက် clickနှိပ်ကာ Open with ကနေတစ်ဆင့် Notepadကိုရွေးပြီးဖွင့်နိုင်ပါတယ်။



3) patchလုပ်မယ်(သို့)အဆင်သင့် crackလုပ်ထားပြီးသား fileတို့နှင့်လဲမယ်ဆိုရင်တော့ ဦးစွာပထမ သက်ဆိုင်ရာ program ကိုမဖြစ်မနေပိတ်ထားရပါမယ်။ကွန်ပျူတာမှာ Runနေတဲ့ program တစ်ခုကို Patchလုပ်၍မရနိုင်ပါ။

Internet Security

. . . . ဤတွင်ပြီး၏

မျိုးသူရ

INTERNET Security

မျိုးသူရ

- Virus များအား ရှာဖွေရှင်းလင်းနည်းများ
- Virus Definiction အသစ်များ Update လုပ်နည်းများအကြောင်း
- လျှို့ဝှက်ထောက်လှမ်းနိုင်သောနှင့် Spy Software များအကြောင်း
- Computer Virus ဆိုတာဘာလဲ၊ ဘယ်လိုပြန့်နှံ့သွားကြသလဲ
- Virus ကာကွယ်နိုင်သော Software အသုံးပြုနည်းများ
- Virus အန္တရာယ်ကာကွယ်နိုင်မည့် Avira နှင့် KasperSky Software
- Hacker များနှင့် Introder များရန်မှ ကာကွယ်ပေးနေသည့် Firewall များအကြောင်း
- မလိုလားအပ်သော Mail များရှင်းလင်းတားဆီးခြင်း၊ Window Registry လုပ်ခြင်း

မျိုးသူရ

openeyes@mail4u.com.mm