အင်တာနက် သုံးစွဲသူများ အတွက် အသိပေးချက် ၈ ချက်

ယခုအခါ သတင်းအချက်အလက်များကို ၂၄ နာရီ၊ ၇ ရက်လုံး ရယူနိုင်သော အင်တာနက်ကို ကွန်ပျူတာဖြင့် ချိတ်ဆက်မှုများ ကျယ်ပြန့်စွာ သုံးစွဲလာကြပါသည်။ အင်တာနက်သည် သတင်းအချက်အလက် ရယူသူနှင့် လေ့လာသူများအတွက် အလွန်အဖိုးမဖြတ်နိုင်သော ဆက်သွယ်ရေး အသုံးအဆောင် ပစ္စည်းတစ်ခုဖြစ်ပါသည်။

သို့သော်လည်း၊ အချို့ကျွမ်းကျင်သူများသည် အင်တာနက်မှတစ်ဆင့် ရာဇဝတ်မှုများနှင့် နှောင့်ယှက်မှုများကို လုပ်ဆောင်လာကြပါသည်။ ရာဇဝတ်မှုများအနေဖြင့် ခွင့်ပြုချက်မရဘဲ ကွန်ပျူတာအတွင်း ဝင်ရောက်ကြည့်ရှုခြင်းနှင့် ကိုယ်ရေးအချက်အလက်များကို ခိုးယူခြင်း၊ ကိုယ်ပွား ရယူအသုံးပြုခြင်း၊ ဆိုက်ဘာနည်းအားဖြင့် တိုက်ခိုက်ခြင်းများအထိ လုပ်ဆောင်လာပါသည်။

အောက်တွင်ဖော်ပြထားသော အချက်အလက်များသည် ဆိုက်ဘာ လုံခြုံမှုနှင့် ပတ်သက်သော အလေ့အကျင့်များအတွက် အခြေခံအချက်များ ဖြစ်ပါသည်။ ထိုအလေ့အကျင့်များဖြင့် ဆိုက်ဘာနည်းဖြင့် ကျူးလွန်သော ရာဇဝတ်မှုများကို ကာကွယ်နိုင်မည်ဖြစ်ပါသည်။

ဆိုက်ဘာလုံခြုံမှုအတွက် နည်းလမ်းတစ်ခု သို့မဟုတ် ဖြေရှင်းချက်တစ်ခုဖြင့် မလုံလောက်ပါ။ ထိုအလေ့အကျင့်များကို သုံးစွဲခြင်းဖြင့် အင်တာနက် သုံးစွဲမှုပုံစံများနှင့် နည်းပညာဖြေရှင်းချက်များက လုံခြုံစိတ်ချရသော အင်တာနက်သုံးစွဲမှု ဖြစ်လာနိုင်ပါသည်။

၁။ တန်ဖိုးကြီးသော ကိုယ်ရေးအချက်အလက်များကို ကာကွယ်ပါ။

ကိုယ်ရေးအချက်အလက်များဖြစ်သော အီးမေးလိပ်စာ၊ စကားဝှက်များ နှင့် ဝက်ဘ်ဆိုဒ်သုံးစွဲမှု မှတ်တမ်းများကို ရယူခြင်း၊ လေ့လာခြင်းအားဖြင့် များစွာသော အနှောင့်အယှက်များ ပေးနိုင်ပါသည်။ အရေးကြီးသော အချက်အလက်များကို ရယူရန်အတွက် အီးမေးလ်များ ပေးပို့ခြင်း၊ ဝက်ဘ်ဆိုဒ်များသို့ ဝင်ရောက်စေခြင်းနှင့် ဆွဲဆောင်မှုများ ပြုလုပ်ခြင်းဖြင့် ခိုးယူနိုင်ပါသည်။

- အရေးကြီးသော သင့်ကိုယ်ရေးအချက်အလက်များကို အခြားသူများအား မပေးမိအောင် ဆင်ခြင်ပါ။
- အင်တာနက်သုံးစွဲပြီးတိုင်း သုံးစွဲမှုမှတ်တမ်းများအားဖျက်ပါ။
- အလွန်အကျွံ မက်လုံးပေးသော အီးမေးလ်များနှင့် ဝက်ဘ်ဆိုဒ်များကို ရှောင်ကျဉ်ပါ။
- မေးမြန်းလာသော မေးခွန်းများအား ဂရုတစိုက်ဖတ်ပြီး ဖြေကြားပါ။ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို မပေးပါနှင့်။
- ကိုယ်ရေးအချက်အလက်နှင့် စကားဝှက်များကို စာအုပ်တွင် ရေးသားခြင်း၊ ဖုန်းလိုင်းမှ ပြောဆိုခြင်းကို ရှောင်ကျဉ်ပါ။

၂။ အွန်လိုင်းတွင် ဆက်သွယ်သူများအား သိအောင်လုပ်ပါ။

အခြားသူများမှ ပေးပို့လာသော အီးမေးလ်များတွင် ပါဝင်သော ဝက်ဘ်ဆိုဒ်များတွင် စွဲဆောင်မှုများအပြည့်ဖြင့် လာရောက်ကြည့်ရှုစေပါလိမ့်မည်။ ထိုအီးမေးလ်များ စာရင်းတွင် ပါဝင်လိုက်ခြင်း (သို့) ဝက်ဘ်ဆိုဒ်တွင် မှတ်ပုံတင်လိုက်ခြင်းဖြင့် အမှားအီးမေးလ်များ ပို့ခြင်း ခံရသော သားကောင် ဖြစ်သွားပါမည်။ တခါတရံ ကိုယ်ရေးအချက်အလက်များကို ခိုးယူခြင်းများလည်း လုပ်ဆောင်နိုင်ပါသည်။ အွန်လိုင်းတွင် ဆက်သွယ်သောသူ အားလုံးကို သိအောင်ကြိုးစားပါ။ မသိသောသူများကို ဖိတ်ခေါ်ခြင်းနှင့် အချက်အလက်များ ဝေငှသုံးစွဲခြင်း ရှောင်ကျဉ်ပါ။

- ကွန်ပျူတာကို သူစိမ်းများအား ဝေငှသုံးစွဲစေခြင်း။ ဖိုင်များကို ကူးယူစေခြင်းကို ရှောင်ကျဉ်ပါ။
- သူစိမ်းတစ်ဦးအား ကွန်ပျူတာကို စိတ်တိုင်းကျ လုပ်ဆောင်နိုင်မည့် အခွင့်အရေးမပေးပါနှင့်။
- မလိုအပ်သောအီးမေးလ်များ မဝင်ရောက်စေရန် အီးမေးလ် လိပ်စာကို မိတ်ဆွေများသာပေးခြင်း။
- သူစိမ်းများမှ အချိန်မှန်အီးမေးလ် ပို့လာသောအခါ မလိုအပ်ပါက ပယ်ဖျက်ရန်ဟု သတ်မှတ်ပေးရန်တွင် ထည့်သွင်းရပါမည်။
- သေချာစွာမသိသော အီးမေးလ်လိပ်စာသို့ စာမပြန်ပါနှင့်။ တွဲဆက်ဖိုင်များပို့တိုင်း အမြဲတမ်း စီစစ်ပါ။
- ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို အီးမေးလ်နှင့် ပြန်မပို့ပါနှင့်။
- အခမဲ့ပေးဆော့ဖ်ဝဲများ (Free Software) နှင့် ဖိုင်များသိုမှီးထားသော နေရာများ (File Hosting)ကို သေချာစွာ စိစစ်ပြီးမှ သုံးပါ။
- တိုက်ရိုက်ပြော စကားဝိုင်း (Instant Messangers) များမှ ကိုယ်ရေးအချက်အလက်များနှင့် ဖိုင်များကို မဝေငှပါနှင့်။

၃။ ကွန်ပျူတာလုံခြုံမှုရှိရေး ဆော့ဖ်ဝဲများထည့်သွင်းပါ။

ကွန်ပျူတာကို တိုက်ခိုက်နိုင်သော ဗိုင်းရပ်စ်၊ ထရိုဂျန်နှင့် အခြားဆော့ဖ်ဝဲများစွာရှိပါသည်။ ထိုတိုက်ခိုက်မှုများသည် တစ်ဦးတစ်ယောက်ကို ရည်ရွယ်တိုက်ခိုက်ခြင်းမျိုးမှသည် အများကိုရည်ရွယ်၍ တိုက်ခိုက်ခြင်းများအထိ ရှိနိုင်ပါသည်။ မိနစ်တိုင်းတွင် ဗိုင်းရပ်အသစ်၊ တိုက်ခိုက်မှု အသစ်များနှင့် ဆော့ဖ်ဝဲပြဿနာများ ပေါ်ပေါက်နေပါသည်။ ကွန်ပျူတာ လုံခြုံမှုရှိစေရေးတွင် ဆော့ဖ်ဝဲများ တပ်ဆင်ရုံသာမက ထိုဆော့ဖ်ဝဲ များ၏ နောက်ဆုံးမူကွဲများကို ပြောင်းလဲတပ်ဆင်ထားရန်လည်း လိုအပ်ပါသည်။

- ဗိုင်းရပ်နှိမ်နင်းရေးဆော့ဖ်ဝဲ တပ်ဆင်ပါ။ အမြဲတမ်းနောက်ဆုံးမူကွဲဖြင့်သုံးပါ။
  - http://support.microsoft.com/kb/49500 - http://en.wikipedia.org/wiki/List_of_antivirus_software
- ပြင်ပမှ အဆက်မပြတ် တိုက်ခိုက်မှုများကို ကာကွယ်နိုင်ရန် Firewall ကိုသုံးပါ။ ကွန်ရက်သုံးစွဲမှုများကို စိစစ်ပါ။
  - http://www.zyra.org.uk/firewall.htm
- ကွန်ပျူတာတွင်း ထောက်လှမ်းသော ပရိုဂရမ်များ မဝင်ရောက်နိုင်စေရန် Anti-spyware ပရိုဂရမ်များထည့်သွင်းပါ။
  - http://en.wikipedia.org/wiki/Anti-spyware#Anti-spyware_programs

၄။ အသုံးပြုသော ဆော့ဖ်ဝဲများ အဆင့်မြှင့်ခြင်း ပုံမှန်လုပ်ပါ။

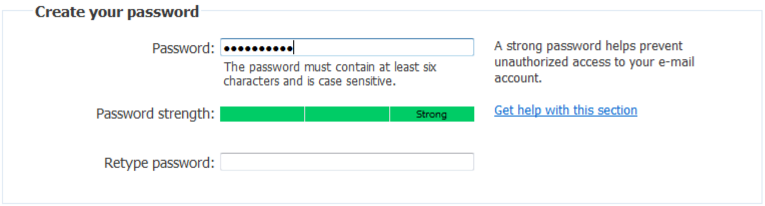
အသုံးပြုသောဆော့ဖ်ဝဲများနှင့် စက်မောင်းနှင်မှုစနစ် (Operating System) တွင် မှားယွင်းမှုများ ပါဝင်နေသည်ကို အနှောင့်အယှက် ပေးနိုင်သော ကျွမ်းကျင်သူများ (သို့) ဟက်ကာများမှ အမြဲစောင့်ကြည့်နေကြပါသည်။ ကွန်ရက်အခြေပြု သုံးစွဲနေသော ဆော့ဖ်ဝဲများနှင့် ဆက်စပ်သော ဝက်ဘ်ဆိုဒ်များတွင် ချို့ယွင်းချက်များ ရှိနေပါက တိုက်ခိုက်သူများမှ ဝင်ရောက်တိုက်ခိုက်မည်ဖြစ်သည်။

- လုံခြုံမှုများ ပြင်ဆင်ပေးထားသည့် ဆော့ဖ်ဝဲ မူကွဲအသစ်များကို ရယူတပ်ဆင်ပါ။
- လုံခြုံရေးနှင့် ပတ်သက်သော နည်းပညာအသစ်များ၏ အားသာချက်များကို လေ့လာအသုံးပြုပါ။
- အခမဲ့ရသော ဆော့ဖ်ဝဲများကို သုံးစွဲပါက နောက်ဆုံးမူကွဲကို ရယူသုံးစွဲပါ။
- ဗိုင်းရပ်စ် အသစ်များ နှင့် တိုက်ခိုက်မှုအသစ်များကို ကာကွယ်နိုင်သော ဆော့ဖ်ဝဲများကို ရှာဖွေအသုံးပြုပါ။

၅။ စိတ်ချယုံကြည်ရသော စကားဝှက်များနှင့် စကားဝှက် စိစစ်မှုကို သုံးပါ။

စကားဝှက်များကို ကွန်ပျူတာဝင်ရောက်ရန်နှင့် ဆော့ဖ်ဝဲနှင့် ဝက်ဘ်ဆိုဒ်များ ဝင်ရောက်ရာတွင် သုံးစွဲကြရပါသည်။ အထူးသဖြင့် အီးမေးလ် တစ်ခုနှင့် စကားဝှက်တစ်ခုသည် လူတိုင်းအတွက် အရေးကြီးသော ကိုယ်ရေးအချက်အလက်အဖြစ် ဆိုက်ဘာကမ္ဘာတွင် သတ်မှတ် လာကြသည်။ စကားဝှက်မေ့ခြင်း၊ ပျောက်ဆုံးခြင်း၊ အလွယ်မှတ်လွယ်သော စကားဝှက်များကို ပေးမိခြင်းတို့သည် စကားဝှက်ပေါ်အခြေခံသော ပြဿနာများဖြစ်ကြသည်။ စကားဝှက်သုံးစွဲသူတိုင်းအတွက် ကောင်းသော အလေ့အကျင့်များမှာ

- မှတ်ရမလွယ်ကူသော၊ အဘိဓာန်တွင် မပါဝင်သော၊ ဂဏန်းများပါဝင်သောနှင့် အခြားသင်္ကေတများ ပေါင်းစပ်ထားသော ၈ လုံးထက် များသော စာလုံးတွဲ ပေးသင့်ပါသည်။
- အမည်၊ မွေးသက္ကရာဇ်၊ အမည်၊ asdf၊ admin၊ abcd၊ 1234 နှင့် အလွန်တိုသော စကားဝှက်များကို ရှောင်ရှားပေးသင့်ပါသည်။
- စကားဝှက်များကို အခြားသူများအားပေးခြင်း၊ ဝေငှသုံးစွဲခြင်းများကို ရှောင်ကျဉ်သင့်ပါသည်။
- စက်ရုံမှ ထုတ်စဉ်မှ သတ်မှတ်ပေးလိုက်သော စကားဝှက်များကို ပြောင်းလဲသုံးစွဲသင့်ပါသည်။
- စကားဝှက်ကို တစ်ခြားသူသိလျှင်သော်၎င်း၊ အပတ်စဉ်/လစဉ် ပြောင်းလဲသုံးစွဲသင့်ပါသည်။
- စကားဝှက်တစ်ခုကို နေရာစုံတွင် သုံးစွဲခြင်းကို ရှောင်ကျဉ်သင့်ပါသည်။
- အသုံးပြုသူအမည်နှင့် တူညီသော စကားဝှက်ကို ရှောင်ကျဉ်သင့်ပါသည်။
- မိမိကိုယ်တိုင် ပြန်လည်မှတ်မိလွယ်နိုင်သော စကားဝှက်ကို ဖန်တီးသင့်ပါသည်။
- စကားဝှက်များကို စီမံခန့်ခွဲနိုင်သော စနစ်များသုံးစွဲသင့်ပါသည်။
- အခြားသူများ စကားဝှက် ထည့်သွင်းခြင်းကို စောင့်ကြည့်ခြင်းနှင့် ကိုယ်တိုင် ကြည့်ခံရခြင်း မရှိအောင် ရှောင်ကျဉ်သင့်ပါသည်။
- စကားဝှက်သုံးစွဲသောအခါ https စိစစ်မှုမှတဆင့် သုံးစွဲပါက ပိုမိုသင့်လျော်ပါသည်။
- အောက်တွင်ပြထားသည့်အတိုင်း စကားဝှက် အဆင့်ခိုင်မာသည့်အထိထည့်သွင်းရန်လိုအပ်ပါသည်။



၆။ အရေးကြီးသော ဖိုင်များကို ပွားယူထားပါ။

ပြီးပြည့်စုံသော လုံခြုံစိတ်ချရသည့် ကာကွယ်မှုစနစ် မရှိနိုင်ပါ။ ကုသခြင်းထက် ကာကွယ်ခြင်းက ပိုကောင်းပါသည်။ ကွန်ပျူတာတွင်မူ ကာကွယ်ခြင်းထက် စိတ်ချရသောနေရာတွင် ပွားထားခြင်းက ပိုကောင်းပါသည်။ သုံးစွဲနေသော ကွန်ပျူတာမှ အရေးကြီးသော ဖိုင်များကို သင့်တော်သောနေရာတစ်ခုတွင် ကူးပွားထားခြင်း၊ ရွှေ့ပြောင်းနိုင်သော မီဒီယာများတွင် ကူးပွားထားခြင်းနှင့် အခြားဆက်စပ်မှုမရှိသော ဒေသတွင် သိမ်းဆည်းထားခြင်း စသော နည်းလမ်းများဖြင့် လုပ်ဆောင်နိုင်ပါသည်။ ကူးပွားထားခြင်းကို လုပ်ဆောင်ပါက အခြားသူများ ရယူနိုင်ခြင်း မရှိစေရန် စကားဝှက်များ သတ်မှတ်ခြင်းနှင့် ခွင့်ပြုချက်ဖြင့်သာ ဖတ်နိုင်သော (Encryption) နည်းများ အသုံးပြုပြီး ကူးပွားထား သင့်ပါသည်။

၇။ အမှားဖြစ်နိုင်သော နည်းလမ်းများကို သင်ယူမှတ်သားပါ။

လုံခြုံစိတ်ချရသော စနစ်ကို တည်ဆောက်ထားသော်လည်း တိုက်ခိုက်မှုများက ရှိနေဦးမည်ဖြစ်ပါသည်။ တိုက်ခိုက်မှုအများစုသည် လုံခြုံမှု အသိပညာအားနည်းခြင်း၊ ကိုယ်ရေးအချက်အလက်များ ရယူခြင်းနှင့် အခြား ဆွဲဆောင်သောနည်းလမ်းများဖြင့် သုံးစွဲသူကို အခြေပြု တိုက်ခိုက်လာကြပါသည်။ တိုက်ခိုက်နိုင်သည့်နည်းလမ်းများနှင့် ခိုင်မာသော လုံခြုံရေးစည်းမျဉ်းများကို သင်ယူမှတ်သားခြင်းတို့ကို နေရာ တိုင်းတွင် လုပ်ဆောင်ရန်လိုအပ်ပါသည်။ သုံစွဲသူ အချင်းအချင်း အတွေ့အကြုံများ ဖလှယ်ရန်လိုအပ်ပါသည်။ အမှားဖြစ်နိုင်သော နည်းလမ်းများစွာ ရှိပါသည်။ ထိုနည်းလမ်းများကို http://www.microsoft.com/security/default.mspx တွင် ရယူလေ့လာနိုင်ပါသည်။

၈။ ဆိုက်ဘာတိုက်ခိုက်ခံရသောအခါ မည်သို့ပြုလုပ်ရမည်ကို ကြိုတင်ပြင်ဆင်ပါ။

အင်တာနက်ကွန်ရက် သုံးစွဲသူများသည် လွယ်ကူသောလုပ်ငန်းစဉ်များကို လုပ်ဆောင်နိုင်သောကြောင့် လုံခြုံမှုအားနည်းချက်ကြောင့် ဝင်ရောက်တိုက်ခိုက်ခြင်း ခံရနိုင်ပါသည်။ ထိုကြောင့် အခြားဖြစ်ခဲ့သော လုံခြုံမှုအမှားများ၊ အားနည်းချက်များကို လေ့လာခြင်းဖြင့် ရှောင်ရှား နိုင်မည်ဖြစ်ပါသည်။ တိုက်ခိုက်ခြင်းခံနေရသလား ဆိုတာကို စိစစ်နိုင်သော တိကျသော နည်းလမ်းမရှိပါ။ ဖြစ်ခဲ့ဖူးသော အမှားအယွင်းများ သို့မဟုတ် ပုံမှန်လုပ်ဆောင်မှုများမှ သွေဖယ်နေမှသာ တိုက်ခိုက်ခြင်းကို သိရှိနိုင်ပါသည်။ မိသားစုဝင်များနှင့် လုပ်ငန်းခွင်တွင် တိုက်ခိုက်ခံရ သောအခါ မည်သို့လုပ်ဆောင်ရမည်ကို အသိပေးထားရန်လိုအပ်ပါသည်။

- တိုက်ခိုက်ခြင်းခံရသည်ဟု ယူဆပါက လက်ရှိ ဆက်သွယ်မှုများကို ရပ်ပါ။
- ကွန်ပျူတာကို ဗိုင်းရပ်နှိမ်နင်းသော ဆော့ဖ်ဝဲနှင့် စိစစ်ပါ။
- Firewall ကို သေချာစွာ စိစစ်၍ အဆင့်မြှင့်ပါ။
- နောက်တကြိမ် မတိုက်ခိုက်နိုင်ရန် ပြင်ဆင်ဆောင်ရွက်ပါ။

လက်တွေ့အသုံးချအစီအစဉ်

၁။ ဝက်ဘ်ဆိုဒ်များကို အသုံးပြု၍ ဖြတ်ကျော်လွှားခြင်း။

(က) ရှာဖွေရေး ဝက်ဘ်ဆိုဒ်များမှ ခေတ္တမှတ်ထားသော စာမျက်နှာများကိုကြည့်ခြင်း။

(ခ) ဖိုင်များပြောင်းရွှေ့ခြင်းကို ဖိုင်သို့လှောင်သော ဝက်ဘ်ဆိုဒ်များ အသုံးပြုခြင်း။

(ဂ) တဆင့်ခံကြည့်နိုင်သော ဝက်ဘ်ဆိုဒ်များမှ ကြည့်ခြင်း။

(ဃ) တဆင့်ခံကြည့်နိုင်သော ဝက်ဘ်ဆိုဒ်များ စာရင်း။

၂။ ဆော့ဖ်ဝဲထည့်သွင်းအသုံးပြု၍ ဖြတ်ကျော်လွှားခြင်း။

(က) Ultrasurf တပ်ဆင်အသုံးပြုခြင်း။

(ခ) Your-freedom တပ်ဆင်အသုံးပြုခြင်း။

၃။ Internet Explorer နှင့် Mozilla တွင် Proxy Server ရှာဖွေနည်း။

၄။ အင်တာနက်ကဖီးတွင် ကွန်ပျူတာအသုံးပြုစဉ် ဆောင်ရန်၊ ရှောင်ရန်များ။

(က) စကားဝှက်များနှင့် အချက်အလက်မှတ်တမ်းများ မကျန်ပါစေနှင့်။

(ခ) ဝက်ဘ်ဆိုဒ်ဝင်ရောက်သော ကိုယ်ရေးအချက်အလက်များ ပြင်ပကွန်ပျူတာတွင် မှတ်သားခြင်းကို ရှောင်ကျဉ်ပါ။

(ဂ) အရေးကြီးသော အချက်အလက်များကို မှတ်သားရန် မိုဘိုင်းဒစ်ကိုအသုံးချပါ။

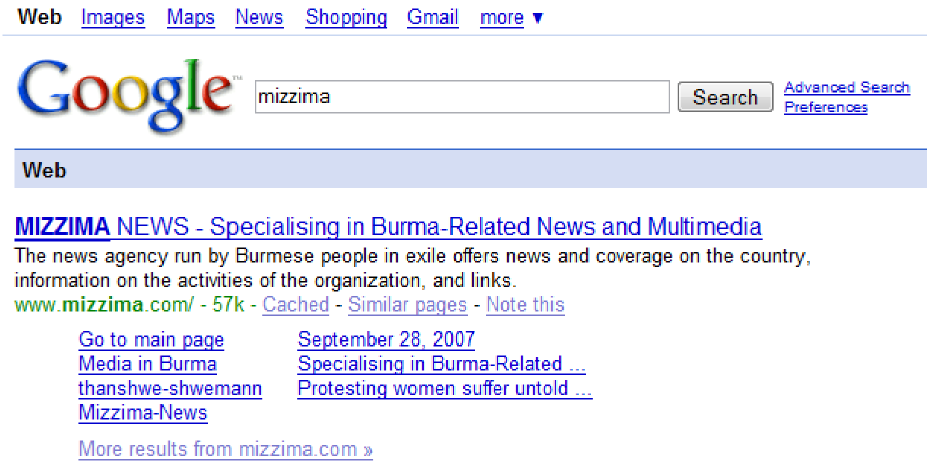
(ဃ) ရိုက်နှိပ်သောကီးများမှတ်တမ်းတင်သောစနစ်ကို ရှောင်ရှားနိုင်ရန် ကာကွယ်ပါ။

၁။ (က) ရှာဖွေရေးဝက်ဘ်ဆိုဒ်များမှ ခေတ္တမှတ်ထားသော စာမျက်နှာများကိုကြည့်ခြင်း။

ရှာဖွေရေး ဝက်ဘ်ဆိုဒ်များသည် ဝက်ဘ်စာမျက်နှာများကို လွယ်ကူစွာ ပြန်လည်ပြသနိုင်ရန် ခေတ္တသိမ်းဆည်း ထားကြပါသည်။ ဥပမာ အားဖြင့် google.com တွင် mizzima ဆိုသောစကားလုံးကို ရှာပါ။ ထိုအခါ ရှာဖွေရရှိသော အချက်အလက်များကို တွေ့ရမည်ဖြစ်သည်။ Cached ဆိုသော စကားလုံးကို ရှာပါ။ ကြည့်ရှုလိုသော ပိတ်ဆို့ထားသည် ဝက်ဘ်ဆိုဒ်ကို အလွယ်ဆုံး နည်းလမ်းဖြင့် ကြည့်ရှုနိုင်ပါမည်။

အဆင့် - ၁

အဆင့် - ၂



အဆင့် - ၃

၁။ (ခ) ဖိုင်များပြောင်းရွှေ့ခြင်းကို ဖိုင်သိုလှောင်သော ဝက်ဘ်ဆိုဒ်များ အသုံးပြုခြင်း။

Web Site	Max File Size (MB)	Storage Capacity (GB)	Sign Up (Uploading)
www.mediafire.com	100	Unlimited	No
www.fileden.com	50 (free)/1000 (paid)	1 (free)/15 (paid)	Yes
www.filefactory.com	300	100 (free)/500 (paid)	No
www.yousendit.com	100	Unlimited	No
quicksharing.com	500	Unlimited	No

filefactory

quicksharing

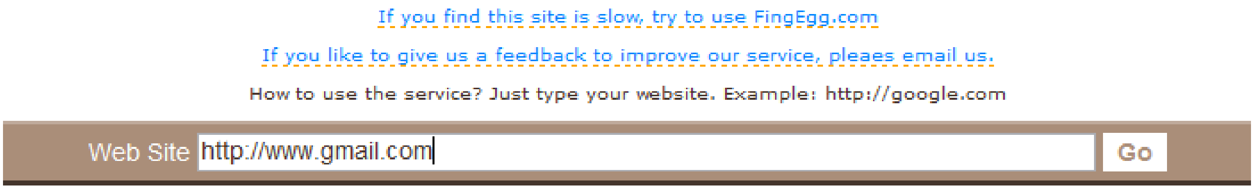
YouSendIt

www.mashable.com/2007/07/28/online-storage/ အခြားဖိုင်သိုလှောင်သော ဝက်ဘ်ဆိုဒ်များကို တွေ့ နိုင်ပါသည်။

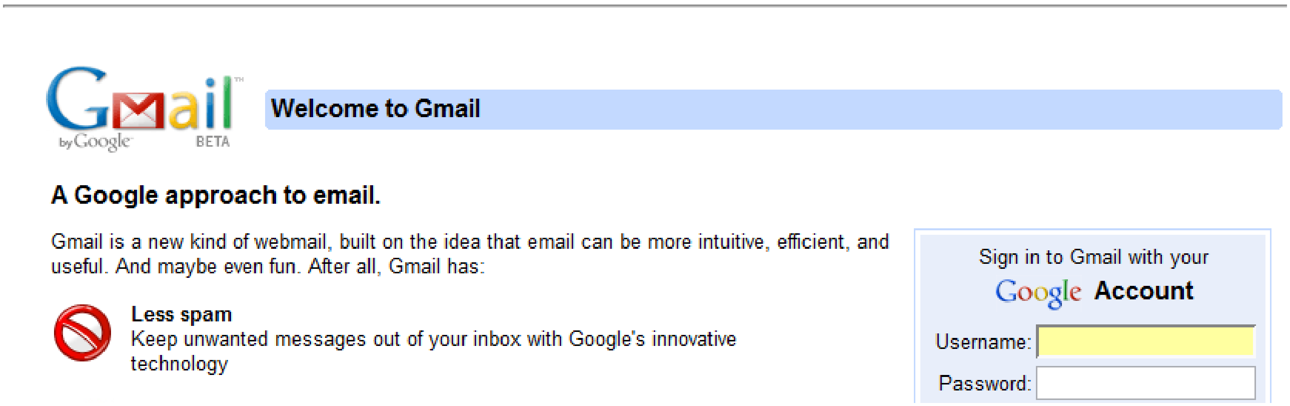
၁။ (ဂ) တဆင့်ခံကြည့်နိုင်သော ဝက်ဘ်ဆိုဒ်များမှ ကြည့်ခြင်း။

အချို့ သောဝက်ဘ်ဆိုဒ်များကိုမူ တဆင့်ခံကြည့်နိုင်သော ဝက်ဘ်ဆိုဒ်များမှသာ ကြည့်ရှုနိုင်မည်ဖြစ်ပါသည်။ တဆင်ခံ ဝက်ဘ်ဆိုဒ်များမှ ကြည့်ရှုနိုင်သော နည်းလမ်းမှာ အလွန်လွယ်ကူသော်လည်း မကြာခဏ ပိတ်ဆို့ခြင်းကို ခံရနိုင်သည်။ နည်းစံရာကို မေးမြန်းခြင်းဖြင့် ကြည့်ရှုနိုင်သော တဆင့်ခံ ဝက်ဘ်ဆိုဒ်ကို သိရှိနိုင်သည်။ ဥပမာ အားဖြင့် google တွင် Proxy ဆိုသော စာလုံးကို ရှာဖွေခြင်းဖြင့် ဝက်ဘ်ဆိုဒ်အသစ်များကို ရှာဖွေတွေ့နိုင်သည်။ http://www.unipeak.com သည် အောက်တွင် ဖော်ပြထားသည့်အတိုင်း ဝက်ဘ်ဆိုဒ်လိပ်စာ ထည့်သွင်းသောနေရာ ပေါ်လာမည်။ ဝက်ဘ်ဆိုဒ်လိပ်စာကို ထည့်သွင်းပြီး ဆက်သွားပါက မိမိအလိုရှိသော ဝက်ဘ်ဆိုဒ်သို့ လွယ်ကူစွာ ရောက်ရှိနိုင်မည်ဖြစ်ပါသည်။

အဆင့် - ၁



အဆင့်-၂



၁။ (ဃ) တဆင့်ခံကြည့်နိုင်သော ဝက်ဘ်ဆိုဒ်များ စာရင်း။

anonymouse.ws/
www.proxyking.net/
www.anonymousindex.com
www.hidemyass.com/
www.proxy7.com/
www.proxyfoxy.com/
www.78y.net/
www.75i.net/
www.dzzt.com/
www.proxyguy.com/
www.GamesProxy.com
www.proxyz.be/
www.antifw.tk
www.proxyhero.com/
www.proxydrop.com/
www.proxydrop.net/
www.proxydrop.biz/
www.proxydrop.info/
www.proxydrop.org/
www.prx1.com/
www.ninjaproxy.com/
www.shadowsurf.com/
www.famous5.net/
www.no1proxy.com/
ProxySpy.com
www.theproxy.be/
www.newproxy.be/
www.smartproxy.net/
ProxyPrince.com
PimpMyIP.com
OhMyProxy.com
www.UnBlockMySpace.com
www.ProxyForAll.com
www.MyProxySurfer.com
www.ProxyCat.com
www.ProxyDetective.com
www.indianproxy.com
www.proxybrowsing
www.ProxyPi.com
www.proxyjet.com
www.justhide.com
www.anonymization.net/
www.guardster.com/
www.proxyweb.net/
webwarper.net/
www.megaproxy.com/
www.amegaproxy.com/
www.w3privacy.com/
www.anonymizer.ru/
www.the-cloak.com/
www.pureprivacy.com/
proxify.com/
www.urlencoded.com/
www.snoopblocker.com/
www.long999.com/
www.psurf.net
www.phproxy.info/
www.proxy121.com/
www.userbeam.de/
www.calcmaster.net/
www.myshield.com/
www.silentsurf.com/cgi-bin/nph-index.cgi
www.bigate.com/cgi-bin/bigate/b/k/k/
www.misterprivacy.com/begin_anonymous_surfing.htm
www.siatec.net/proxyanonymizer
www.idzap.com/
www.safegatetech.com/
www.breiter.ch/
www.rrdb.org/rrdbproxy.php?l=en
proxy.decodes.biz/
proxy.mxds.ch/
www.spondoo.com/
search.sicomm.us/
filter2005.com/
www.kproxy.com/
www.websitereactor.org/cgi-bin/001/nph-.pl
www.goproxing.com/
anonycat.com/
www.spynot.com/
www.merletn.org/anonymizer
www.cgi-proxy.net/
www.proxymouse.com/
www.theunblocker.tk/
www.betaproxy.com/
www.letsproxy.com/
www.freeproxysurf.info/
www.mysticproxy.com/
www.proxywave.com/
www.vtunnel.com/
www.proxysnail.com/
www.freeproxy.ca/
basic.3proxy.com/
www.privatebrowsing.com/
www.hackingtruths.org/proxy
www.xanproxy.be/
www.ipsecret.com/
www.proxyanon.com/
www.anonproxy.info/
www.proxysafe.com/
www.strongproxy.com/
www.boredatschool.net/
www.ukproxy.com/
www.simpleproxy.com/
www.phproxy.org/
surfonym.com/
geoepker.hu/freeproxy/
www.browseatwork.com/
www.ipblocker.info/
www.boredatwork.info/
www.anonymousurfing.info/
www.browsingwork.com/
www.freeproxyserver.org/
www.browseany.com/
www.browsesecurely.com/
IEproxy.com/
www.sneak3.po.gs/
www.proxytastic.com/
www.freewebproxy.org/
www.thecgiproxy.com/
www.hide-me.be/
www.anotherproxy.com/
www.proxy77.com/
www.surf-anon.com/
www.free-proxy.info/
www.theproxysite.info/
www.proxyify.info/
www.concealme.com/
browseschool.info/
browsework.info/
browsingschool.info/
browsingwork.info/
browsingschool.com/
www.proxyindex.com/
www.gobyproxy.com/
www.proxifyme.com/
www.proxyghost.com/
www.spysurfing.com/
www.unblockthis.com/
www.proxyserver7.com/
www.daveproxy.co.uk/
www.tntproxy.com/
www.neoproxy.net/
www.bypassbrowser.com/
www.procksie.com/
www.httproxy.com/
www.cgiproxy.info/
www.proxy-sock.com/
www.proxygeek.com/
www.datadefense.org/
www.hideyour.info/
www.howto.pro/
www.collegeproxy.com/
www.demonproxy.com/
www.satanproxy.com/
www.hidingyou.com/
www.intelliproxy.com/
www.fireprox.com/
www.h0h0h0.com/firewall/
www.katedrala.cz/
www.browseatwork.net/
www.2255.info/
www.vproxy.be/
www.boxproxy.com/
www.nopimps.com/
www.fsurf.com/
www.proxylord.com/
roachhost.com/hp/
www.freepr0xy.com/
www.proxypop.com/
proxy.winidn.com/
www.cloax.net/
www.proxy247.com/
www.traceless.com/
www.stealth-ip.net/
www.proxywhip.com/
www.proxy-surf.net/
www.videoeditors.info/proxy/
www.blockmy.info/
www.proxychatroom.com/
www.teenproxy.com/
www.totalupload.com/surf/
www.proxene.com/
www.fileshack.us/proxy.php
www.cloaker.ca/
www.proxified.net/
www.mrreid.net/

၂။ (က) Ultrasurf တစ်ဆင့်အသုံးပြုခြင်း။

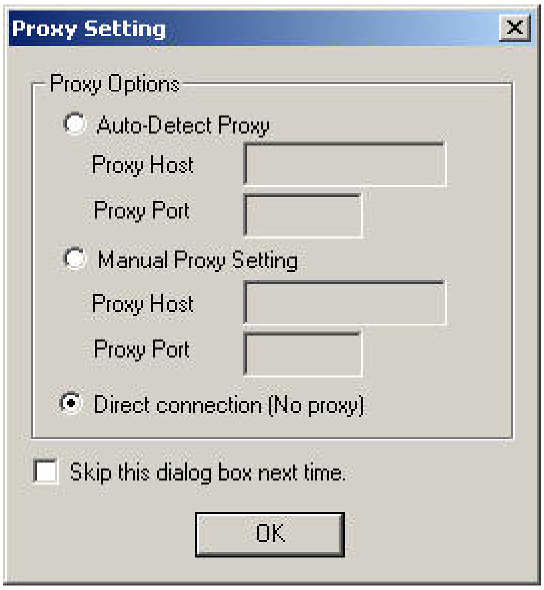
Ultrasurf ကို အသုံးပြုနိုင်ရန် အတွက် ယခုစီဒီတွင် ထည့်သွင်းထားပါသည်။ u.exe ကို software directory တွင်ရှာပါ။ သို့မဟုတ် နောက်ဆုံးထုတ် ဆော့ဖ်ဝဲကို ရယူလိုပါက www.wujie.net/downloads/ultrasurf/u.zip တွင် ရယူနိုင်သည်။

အဆင့် - ၁

u.exe icon ကိုဖွင့်ပါ။

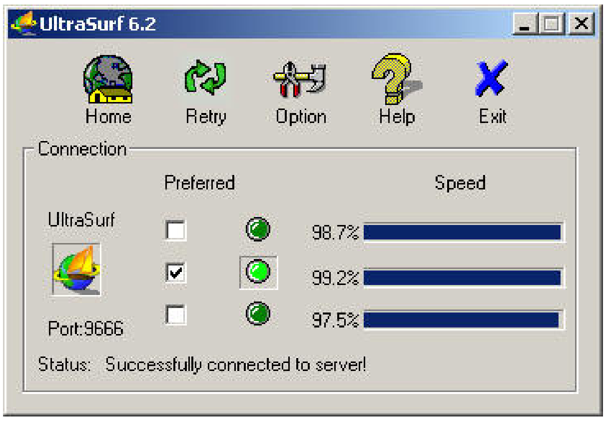
အဆင့် - ၂

Proxy Setting တွင် မိမိသုံးစွဲသော အင်တာနက်ပံ့ပိုးသူမှ ပေးသောစာသား သို့မဟုတ် ဂဏန်း များ ထည့်သွင်းရန်။ Internet Explorer တွင် ထည့်သွင်းပြီးဖြစ်ပါက အလို အလျောက် ထည့်သွင်းပေးပါသည်။



အဆင့် - ၃

မြန်နှုန်းကိုရှာဖွေပြီး အကောင်းဆုံးတစ်ခုဖြင့် ဆက်သွယ် ပေးမည်ဖြစ်သည်။ မိမိကြိုက်ရာ ရွေးချယ်ခြင်းကို Option တွင် ပြင်ဆင်နိုင်သည်။

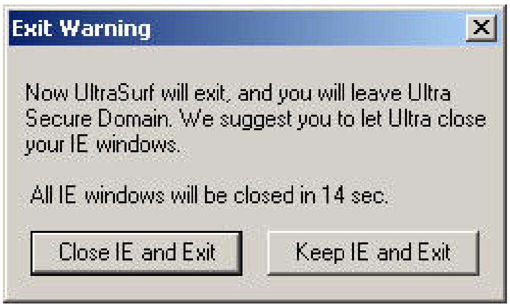


အဆင့် - ၄

ညာဖက်ထောင့်တွင် သော့ခလောက်ပုံ ပေါ်လာပါမည်။

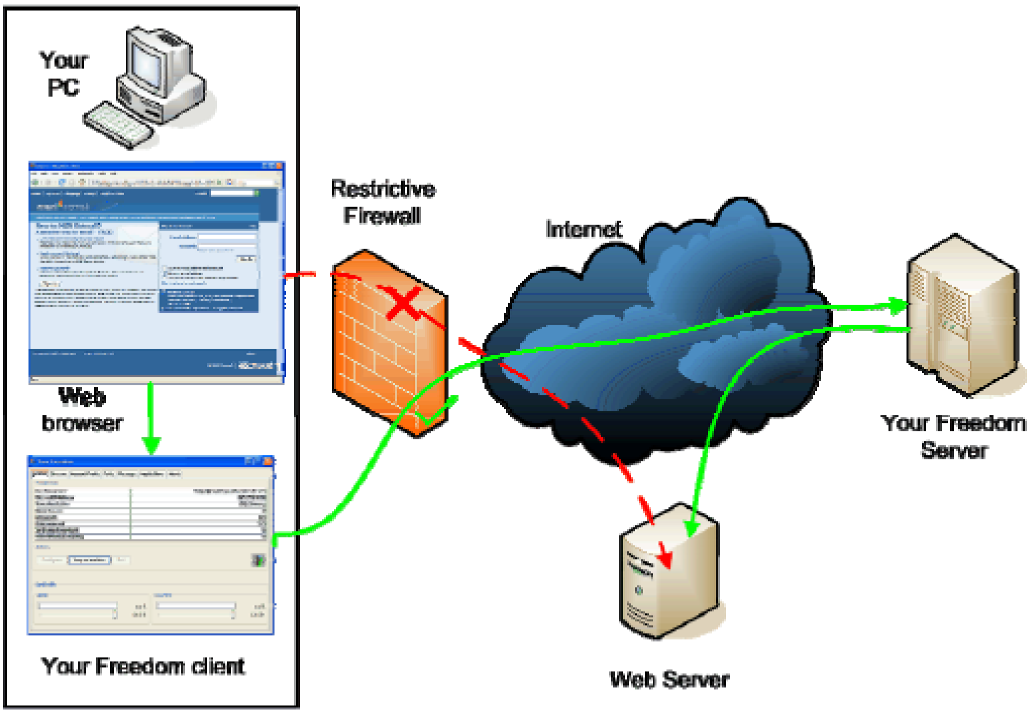
အဆင့် - ၅

Exit ကိုနှိပ်ပါက လက်ရှိသုံးစွဲနေသော Internet Explorer ပိတ်ရန်တောင်းဆိုပါမည်။



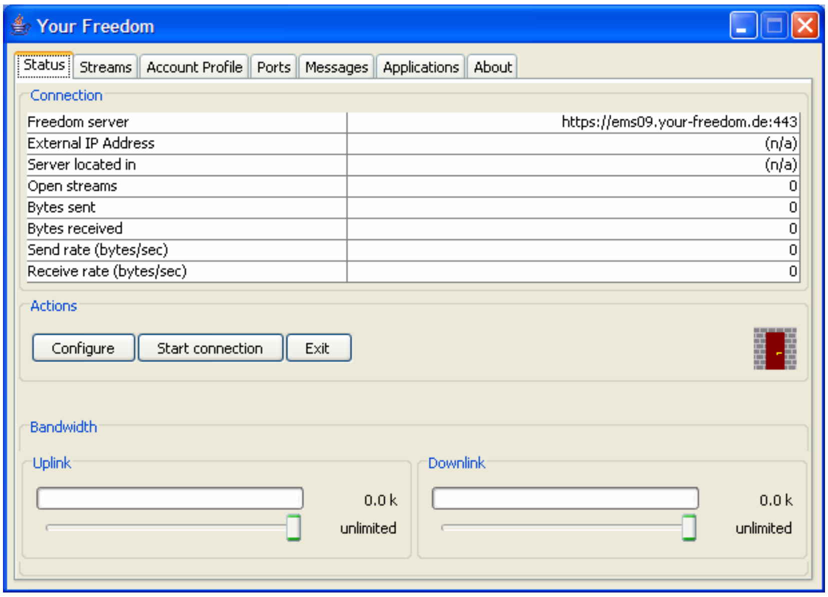
၂။ (ခ) Your-freedom တပ်ဆင်အသုံးပြုခြင်း။

Your-Freedom ကိုအသုံးပြုနိုင်ရန် အတွက် ယခုစီဒီတွင်ထည့်သွင်းထားပါသည်။ freedom-20080314-01.exe ကို software directory တွင်ရှာပါ။ မူကွဲအသစ် ဆော့ဖ်ဝဲကို ရယူလိုပါက www.your-freedom.net/index.php?id=3 တွင်ရယူနိုင်သည်။ ထိုဆော့ဖ်ဝဲကို အသုံးပြုနိုင်ရန်အတွက် သုံးစွဲသူအမည်နှင့် စကားဝှက် ဦးစွာရှိထားရန်လိုအပ်ပါသည်။ ၎င်းတို့ ဝက်ဘ်ဆိုဒ်တွင် အသင်းဝင်ပုံစံ ထည့်သွင်းခြင်း သို့မဟုတ် ပြင်ပတွင် ရောက်ရှိနေသူ တစ်ဦးဦးထံသို့ အကူအညီ တောင်းခံခြင်းဖြင့် အခမဲ့ရရှိနိုင်ပါသည်။



အဆင့် - ၁

Configure ကို နှိပ်ခြင်းဖြင့် အစီအစဉ် သတ်မှတ်ချက်များကို ပထမဦးစွာ ဖြည့်သွင်းပေးရန် လိုအပ်ပါသည်။

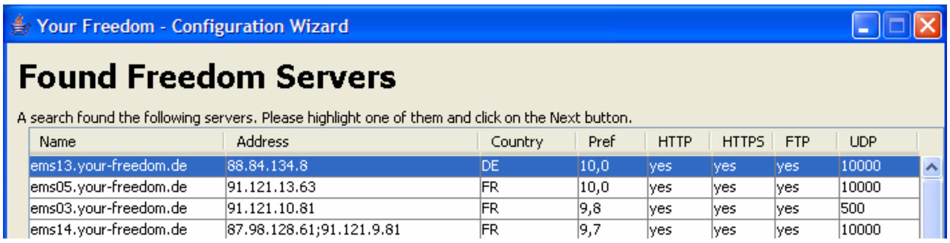


အဆင့် - ၂

လက်ရှိအသုံးပြုနေသော Proxy Server ကိုထည့်သွင်းပါ။ Internet Explorer နှင့် Mozilla တွင် Proxy Server ရှာဖွေနည်းကို ဖော်ပြထားသည်။

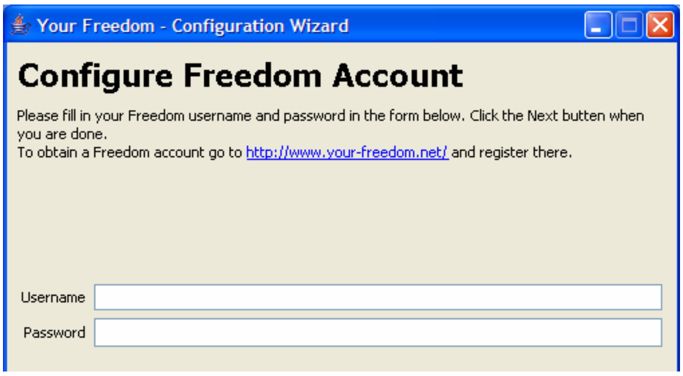
အဆင့် -၃

ထို့နောက် အသုံးပြုနိုင်သော Freedom Server များကိုရှာဖွေပါမည်။



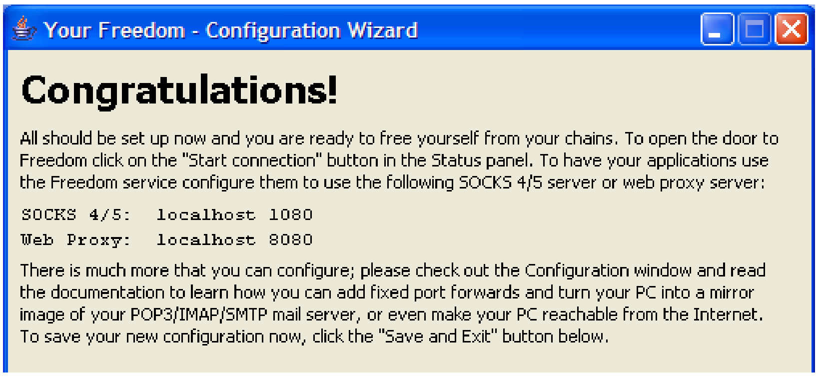
အဆင့် - ၄

မိမိတွင်ရှိသော သုံးစွဲသူအမည်နှင့် စကားဝှက် ကိုထည့်သွင်းရန် လိုအပ်သည်။



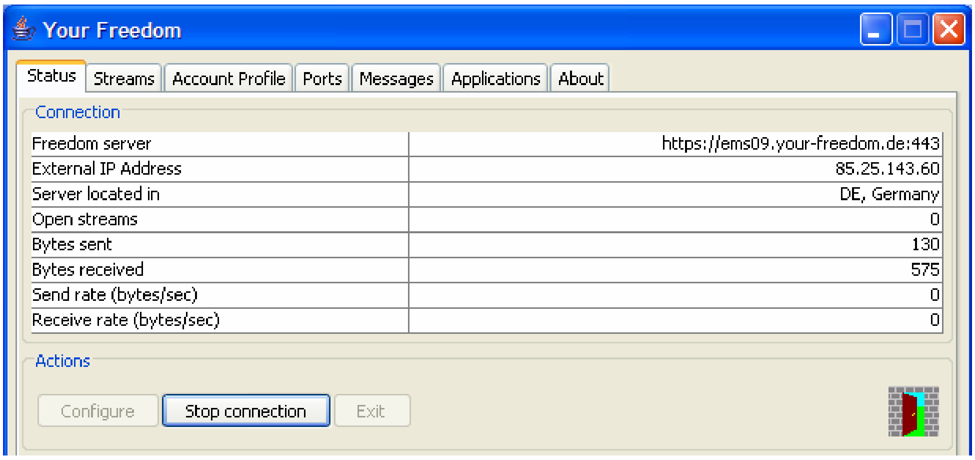
အဆင့် - ၅

နောက်ဆုံးတွင် သုံးစွဲနိုင်သော အခြေအနေနှင့် သတ်မှတ်ချက်များကို အောက်ပါအတိုင်းဖော်ပြပေးမည်။



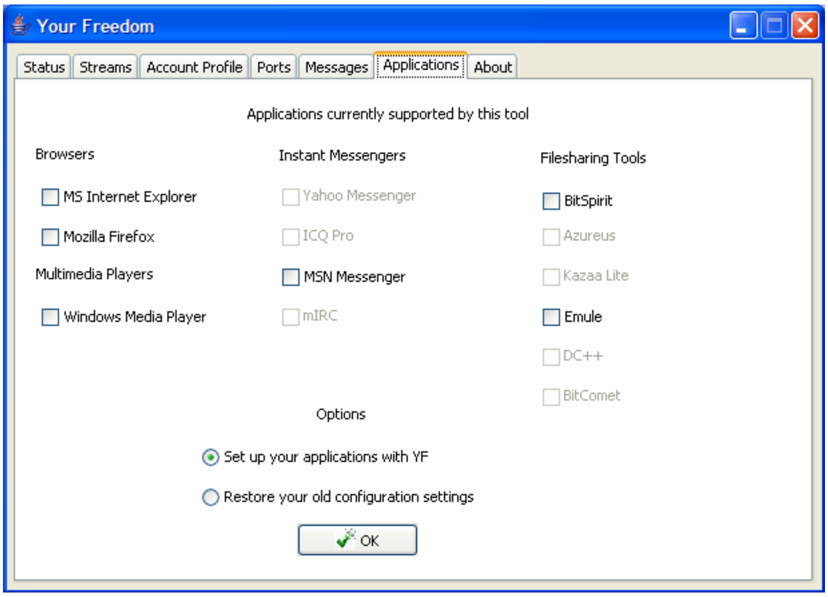
အဆင့် - ၆

Start connection ကိုနှိပ်ခြင်းဖြင့် ညာဖက်အလယ်ပိုင်းတွင် တံခါးပွင့်နေသောပုံပေါ်လာမည်။ အင်တာနက် ကျော်လ ားမှု စတင်သုံးစွဲနိုင်သော အခြေအနေဖြစ်ပါသည်။ Stop connection ကိုနှိပ်ခြင်းဖြင့် သုံးစွဲမှုများ ရပ်တန့်နိုင်သည်။



အဆင့် - ၇

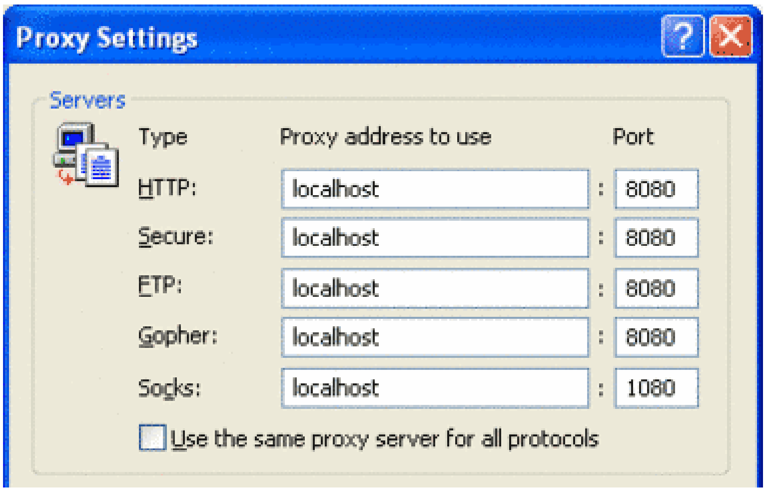
သုံးစွဲလိုသော ဆော့ဖ်ဝဲများကို ရွေးချယ်နှိပ်ခြင်းအားဖြင့် ပိတ်ဆို ခြင်းများကို ကျော်လွှားနိုင်မည်။



၃။ Internet Explorer နှင့် Mozilla တွင် Proxy Server ရှာဖွေနည်းကို ဖော်ပြထားသည်။

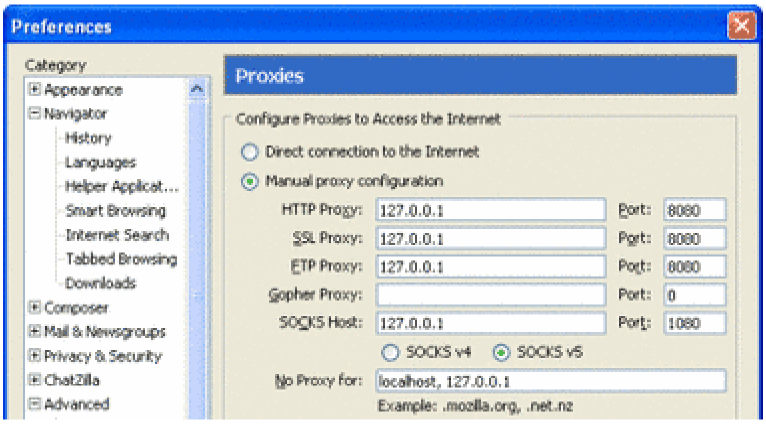
Internet Explorer တွင် Proxy Server ရှာဖွေနည်း။

Internet Explorer ကို ဖွင့်ပါ။
Select: Tools --> Internet Options
Click on "Connections" Tab, then click on "LAN Settings".



Mozilla တွင် Proxy Server ရှာဖွေနည်း။

Mozzila Firefox ကိုဖွင့်ပါ။
Select: --> Edit --> Preferences
Click on "Advanced" and then on "Proxies".



၄။ အင်တာနက်ကဖီးတွင် ကွန်ပျူတာအသုံးပြုစဉ် ဆောင်ရန်၊ ရှောင်ရန်များ။

(က) စကားဝှက်များနှင့် အချက်အလက်မှတ်တမ်းများ မကျန်ပါစေနှင့်။

FireFox : Tools > Clear Private Data ကို ဖွင့်ခြင်း သို့မဟုတ် Ctrl+Shift+Del ကို တွဲနှိပ်ခြင်းဖြင့် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များ ရှင်းနိုင်သည်။

ဝင်ရောက်ခဲ့သော ဝက်ဘ်ဆိုဒ်များမှ ထွက်ခဲ့ရန်လိုအပ်သည်။ မထွက်ခဲ့ပါက နောက်မှ ရောက်လာသူတစ်ဦးမှ သုံးစွဲခြင်း ပြုလုပ်နိုင်သည်။

(ခ) ဝက်ဘ်ဆိုဒ် ဝင်ရောက်သော ကိုယ်ရေးအချက်အလက်များ ပြင်ပကွန်ပျူတာတွင် မှတ်သားခြင်းကို ရှောင်ကျဉ်ပါ။

Internet Explorer : တွင် သုံးစွဲသူ၏ အမည်နှင့် စကားဝှက်ကို မှတ်တမ်း တင်ထားထားသော စနစ်ကို မှတ်သားခြင်းရှောင်ကျဉ်ပါ။

(ဂ) အရေးကြီးသော အချက်အလက်များကို မှတ်သားရန် မိုဘိုင်းဒစ်ကိုအသုံးချပါ။

ပြင်ပနေရာတွင် အင်တာနက်သုံးစွဲသောအခါ အရေးကြီးသော အချက်အလက်များကို မှတ်သားကူးယူရန်အတွက် မိုဘိုင်းဒစ်ကို အသုံးပြုသင့်ပါသည်။ ထိုအပြင် အင်တာနက် ဖွင့်ကြည့်သော ဆော့ဖ်ဝဲများကိုလည်း မိုဘိုင်းဒစ်မှ သုံးစွဲနိုင်သော ဆော့ဖ်ဝဲများဖြင့် သုံးစွဲပါက ပိုမိုသင့်လျော်ပါသည်။ ထိုဆော့ဖ်ဝဲများကို Portable Application ဟုလည်း ခေါ်ပါသည်။ http://portableapps.com/apps/internet/ တွင် ရယူအသုံးပြုနိုင်ပါသည်။

(ဃ) ရိုက်နှိပ်သောကီးများ မှတ်တမ်းတင်သောစနစ်ကို ရှောင်ရှားနိုင်ရန် ကာကွယ်ပါ။

အချို့သော အင်တာနက်ဆိုင်များတွင် ရိုက်နှိပ်သောကီးများ မှတ်တမ်းတင်သော စနစ်ကို တပ်ဆင်ထားနိုင်ပါသည်။ စကားဝှက်များနှင့် အရေးကြီးအချက်အလက်များ ရိုက်သွင်းရန် လိုအပ်သောအခါတွင် အများမသိနိုင်ရန် အကာအကွယ် လိုအပ်ပါသည်။ ထိုသို့ ကာကွယ်နိုင်ရန် on screen keyboard ကိုသုံးပါ။

http://www.aplin.com.au/?page_id=246 တွင် အခမဲ့ရနိုင်သော on screen keyboard ကို အသုံးပြုရိုက်သွင်းပါ။