# တရားမဂင် ဂင်ရောက်ခံရခြင်းမှ ကာကွယ်ခြင်းအစီအမံ

ASEAN · JAPAN
Information Security Awareness

တရားမဂင်ဂင်ရောက်ခံရခြင်းဆိုသည်မှာ···

တရားမဂင်ဂင်ရောက်ခံရခြင်းဆိုသည်မှာ ၁၃-၂-၂ဂဂဂ နေ့ထုတ်ပြန်ထားသော"Unauthorized

Pdf Prepared By: Heavenly Moe

Access Prohibition Law" (*1) အရ ကွန်ပျူတာအသုံးပြုသူများ၏ ကွန်ပျူတာများအတွင်းသို့ မမှန်ကန်သော၊တရားမဝင်သောနည်းလမ်းများဖြင့်ဝင်ရောက်ခြင်း (သို့) ထိုကဲ့သို့ တရားမဝင်နည်းလမ်းများကို အားပေးသော လုပ်ဆောင်ချက်များကိုခေါ်ပါသည်။

・ ကွန်ပျူတာ၏ OS နှင့် Application (သို့) Hardware အတွင်းရှိစနစ်အားနည်းမှု (Security Hole) (*2) ကိုအ သုံးပြု၍ ကွန်ပျူတာ၏ Access Control (*3) စနစ်ကိုကျော်ဖြတ်၍ ကွန်ပျူတာများအတွင်းသို့ ဝင်ရောက်ခြင်း။

・ အသုံးပြုသူတစ်ဦး၏ ID နှင့် Password များကို (*4) ထိုသူ၏ခွင့်ပြုချက်မပါဘဲ ခိုးယူသုံးစွဲခြင်း။ (အယောင်ဆောင်လုပ်ရပ်)

・ အသုံးပြုသူတစ်ဦး၏ ID နှင့် Password များကို ထိုသူ၏ခွင့်ပြုချက်မပါဘဲအခြားသူတစ်ဦး (တတိယလူ) ကိုပေးခြင်း။

ဤအစီအမံစာအုပ်သည်ကွန်ပျူတာအသုံးပြုသူများအတွက်သာ ရည်ရွယ်ပါသည်။

ဤစာအုပ်တင်ဖော်ပြထားသောတရားမဝင်ဝင်ရောက်ခံရခြင်းမှ ကာကွယ်ခြင်းနည်းလမ်းများ သည် ကုမ္ပဏီ Network များတွင်အသုံးပြုရန်အတွက် မလုံလောက်သောကြောင့် အထူးဂရုပြုပါ။

ဥပမာ။ အောက်ပါဖြစ်ရပ်များ...

・ လွယ်ကူသော Password များ၏ မထင်မှတ်ဖွယ်အန္တရာယ်။

ကွန်ပျူတာအသုံးပြုသူ A သည် အင်တာနက်လေလံကိုအသုံးပြု၍ Baseball ကဒ်များကိုရောင်းချသူတစ်ဦးဖြစ်သည်။ ၎င်းသည်အင်တာနက်လေလံ၏ Login တွင် passwordမမေ့စေရန် အတွက် သူ၏အမည်ကို password အဖြစ်အသုံးပြုခဲ့သည်။ တနေ့တွင်အင်တာနက်လေလံ Login လုပ်စဉ်တွင် Invalid Password ဟူသောစာတန်းပေါ်လာပြီး ဝင်ရောက်၍ မရနိုင်တော့ပါ။ A သည် မိမိကိုယ်တိုင်

Passwordပြောင်းလဲခြင်းမပြုခဲ့သည့်အတွက် ကုမ္ပဏီထံသို့ ဆက်သွယ်မေးမြန်း ရာတွင် သူ၏ Password ကို တစုံတစ်ဦးကပြောင်းလဲထားကြောင်းသိရပါသည်။A သည် လွယ်ကူသော Password ကိုအသုံးပြုခဲ့သဖြင့် ခိုးယူသူများကအလွယ်တကူသိရှိ ခိုးယူနိုင်ခြင်းဖြစ်ပါသည်။

・ အင်တာနက်နှင့်အချိန်ပြည့် ချိတ်ဆက်ထားခြင်း၏ မထင်မှတ်ဖွယ်အန္တရာယ်။

ကွန်ပျူတာအသုံးပြုသူBသည်CATVအင်တာနက်စနစ်ကိုအသုံးပြုသူဖြစ်သည်။လစဉ်ပေးဆောင်ရသောနှုန်းထားမပြောင်းလဲသည့်အတွက် သူ၏ ကွန်ပျူတာကို အင်တာနက်နှင့်အချိန်ပြည့် ချိတ်ဆက်ထားခဲ့သည်။ B ၏ ကွန်ပျူတာသည်လုံခြုံမှုစနစ်အားနည်းနေပြီး Microsoft update ကိုလည်းပြုလုပ်ခြင်းမရှိပါ။ တစ်နေ့တွင် B သည် ISRC (Information Security Response Center)မှ သည်အစိုးရအဖွဲ့အစည်းများကို တိုက်ခိုက်နေသဖြင့် အင်တာနက်အသုံးပြုခြင်းကို ရပ်ဆိုင်းရန်အကြောင်းကြားခြင်းခံရသည်။ ထို့နောက်Bအသုံးပြုနေသော ကွန်ပျူတာသည် အင်တာနက်မှ ဖြတ်တောက်ခြင်းခံရသည်။ B သည် မိမိ၏လုံခြုံမှု စနစ်အားနည်းနေသော ကွန်ပျူတာကို အင်တာနက်နှင့်အချိန်ပြည့် ချိတ်ဆက်ထားခဲ့သည့်အတွက် သတိမပြုမိချိန်အတွင်း တိုက်ခိုက်သူများ၏ ခိုးယူခံရခြင်းဖြစ်သည်။

・ ကြိုးမဲ့စနစ်သုံးခြင်း၏
မထင်မှတ်ဖွယ်အန္တရာယ်။

ကွန်ပျူတာအသုံးပြုသူC၏မိသားစုများတွင် ကိုယ်ပိုင်ကွန်ပျူတာများရှိကြသည်။Cသည်မိမိတို့၏အခန်းအတွင်းမှကိုယ်စီ ကွန်ပျူတာများ အသုံးပြုနိုင်ရန်အတွက်ကြိုးမဲ့စနစ်ကိုဂယ်ယူခဲ့သည်။ C ၏ မိသားစုများသည် ကြိုးမဲ့စနစ်၏ ညွှန်ကြားချက်များကိုမဖတ်ဘဲအသုံးပြုခဲ့ကြသည်။ တစ်နေ့တွင် Cမိသားစုများသည် အွန်လိုင်းမှဂိမ်းကစားနေစဉ် မိမိတို့၏ကွန်ပျူတာနှေးလာသည်ဟု ခံစားမိခြင်း၊Hard disk အတွင်းမှ မိမိတို့ထည့်သွင်းထားခြင်းမရှိသော Data များပေါ်လာခြင်းများကိုတွေ့ရပါသည်။ တစ်နေ့တွင် Credit ကဒ်ကုမ္ပဏီမှ အွန်လိုင်းဈေး

ဝယ်ထားခြင်းအတွက်ပြေစာတစ်ခုရောက်ရှိလာ သည်။ သို့သော် ၄င်းသည် C မိသားစုမှဝယ်ယူထားခြင်းမဟုတ်ပေ။ ထို့နောက် C မိသားစုသည် အွန်လိုင်းဈေးဝယ်ရန်အတွက် Credit ကဒ်နံပါတ်ကိုမိမိတို့ ကွန်ပျူတာတွင်ထည့်သွင်းခဲ့ကြောင်းသတိပြုမိခဲ့သည်။လုံခြုံမှုစနစ်ကာကွယ်မထားသော ကြိုးမဲ့စနစ် မှတဆင့် တိုက်ခိုက်သူများ၏ခိုးယူခံရခြင်းဖြစ်သည်။
ထိုကဲ့သို့ လွယ်ကူသော Password ကိုအသုံးပြုခြင်း၊ လုံခြုံမှုစနစ်ကိုပြင်ဆင်မထားခြင်း၊ ဝင်ရောက်မှုကို ကာကွယ်မထားခြင်းစသည်တို့ကြောင့် တိုက်ခိုက်သူများ၏ တရားမဝင် ဝင်ရောက်ခြင်းအန္တရာယ်များရှိနိုင်ပါသည်။ အင်တာနက်အသုံးပြုသူမည်သူမဆို ထိုကဲ့သို့အဖြစ်အပျက်များရင်ဆိုင်တွေ့ရှိနိုင်ပါသည်။ အောက်တွင်ဖော်ပြထားသော အခြေခံလုံခြုံမှုစနစ်များကို လိုက်နာ၍အင်တာနက်ကို အသုံးပြုပါ။

၁။ Security Patches များကို အသုံးပြုပါ။ (ကျူးကျော်မှုများကို တုံ့ပြန်ခြင်း)

Window၊ Macintosh၊ Linux စသည့် OS (Operating System)၊ Internet Explorer၊Firefoxစသည့်Browserများနှင့်အခြားသော ဆော့ဖ်ဝဲလ်များသည် လုံခြုံမှုစနစ်အားနည်းခြင်းကိုဖြစ်ပေါ်စေနိုင်ပါသည်။ ထိုကဲ့သို့ လုံခြုံမှုစနစ် အားနည်းခြင်းကို SecurityHoles (သို့) စနစ်အားနည်းခြင်းဟုခေါ်ဆိုပါသည်။ အကယ်၍သင်သည် စနစ်အားနည်းသော OS (သို့) Application ကိုအသုံးပြုပါက ဗိုင်းရပ်စ်များဝင်ရောက်နိုင်ခြင်း၊တရားမဝင် ဝင်ရောက်ခံရခြင်းများဖြစ်နိုင်ခြင်း၊ သင့်ကွန်ပျူတာအတွင်းမှအချက်အလက်များ ပျောက်ဆုံးခြင်း (သို့) ခိုးယူခံရခြင်းများ စသည့်အန္တရာယ်များရှိပါသည်။ ထိုအန္တရာယ်များကိုကာကွယ်နိုင်ရန် SecurityHolesကိုဖယ်ရှားပေးသော ပြင်ဆင်မှုများ(SecurityPatches)ကိုအသုံးပြုရပါမည်။၄င်းတို့သည်စနစ်အားနည်းခြင်းကိုကာကွယ်ပေးသော ဆော့ဖ်ဝဲလ် ပရိုဂရမ်များဖြစ်သည်။ Window အသုံးပြုသူသည် Microsoft Update ကိုပုံမှန်ပြုလုပ်ခြင်း (သို့) အလိုအလျောက် Update လုပ်ခြင်း စနစ်ကိုထားရှိရပါမည်။ Microsoft ကုမ္ပဏီမှ OS (Operating Systems) နှင့် IE (Internet Explorer) နှင့် Office တို့၏ Patches ကိုအသုံးပြုနိုင်ပါသည်။

■ Microsoft Update

http://www.update.microsoft.com/microsoftupdate/v6/

Microsoft Update အသုံးပြုနည်းကို အောက်ဖော်ပြပါ Website တွင် လေ့လာပါ။

■ Microsoft Update

အသုံးပြုပုံ။

http://www.microsoft.com/japan/protect/computer/updates/mu.mspx

၂။ Password ၏လုံခြုံမှုကို လျစ်လျူမပြုသင့်ပါ။ (ခိုးယူခံရခြင်းမှကာကွယ်ခြင်း)

အသုံးပြုသူ၏ ID နှင့် Password များကို Information Systems (Services) မှမိမိကိုယ်ပိုင်ဖြစ်ကြောင်း သက်သေပြခြင်းကို လုပ်ဆောင်ပါသည်။ အများအားဖြင့် အသုံးပြုသူ၏ ID သည် Information System မှ အသုံးပြု တစ်ဦးချင်းအတွက် သတ်မှတ်ပေးထားသော်လည်း Passwordသည် အသုံးပြုသူ၏ ကိုယ်ပိုင်ဖြစ်သည့်အတွက် (မိမိကိုယ်တိုင်) ပြောင်းလဲရပါမည်။ သင်၏အသုံးပြုသူID နှင့်Passwordကိုခိုးယူသုံးစွဲခြင်းခံရပါကခိုးယူသူကသင့် အနေဖြင့် InformationSystem သို့ဝင်ရောက်နိုင်ပါမည်။ ထိုမှတဆင့်သင်မသိဘဲသင့်အနေဖြင့် အွန်လိုင်းဘဏ်စနစ်မှငွေများကို တရားမဝင်ထုတ်ယူခြင်း၊ အင်တာနက် လေလံမှတဆင့် ပစ္စည်းများ ဝယ်ယူခြင်းစသည် တို့ကိုပြုလုပ်နိုင်ပါသည်။

ထို့ကြောင့်သင်၏အသုံးပြုသူ ID နှင့် Password သည်သင်ကိုယ်ပိုင်ဖြစ်သည့်အတွက် ရိုးရှင်းလွယ်ကူသော Password ကိုမသုံးရန်နှင့်အခြားမည်သူမှမသိစေရန် မကြာခဏပြောင်းလဲခြင်းများပြုလုပ်ရန် လိုအပ်ပါသည်။

Password ဥပမာများ:

(1) စာလုံးကြီး၊ စာလုံးသေး၊ ကိန်းဂဏန်း၊ သင်္ကေတများပေါင်းစပ်အသုံးပြုပါ။
သင်္ကေတများ (!၊ #) ကိန်းဂဏန်းများ၊ စာလုံးများ ပေါင်းစပ်အသုံးပြုပါ။

(2) Password အရှည်များကို အသုံးပြုပါ။
အနည်းဆုံး ၈လုံးအထက်

(3) တစ်ခြားသူများမသိနိုင်သောမိမိမှတ်မိနိုင်သော Password ကို အသုံးပြုပါ။
အဓိပ္ပါယ်မရှိသော စာလုံးအတွဲများကိုအသုံးပြုပါ။

Password ခိုးယူခံရခြင်းမှကာကွယ်နည်းများ

(1) Password ကိုမကြာခဏပြောင်းလဲပေးပါ။
(2) စာရွက်ပေါ်တွင်ချမရေးရ။
(3) ကွန်ပျူတာတွင်မှတ်သားထားခြင်းမပြုရ။
(4) အခြားမည်သူမှမသိစေရ။

၃။ အင်တာနက်နှင့် ချိတ်ဆက်ရာတွင် လိုက်နာရမည့်အချက်များ(ကျူးကျော်မှုကို ကာကွယ်ခြင်း)

နေအိမ် (သို့) ရုံးခန်းမှ အင်တာနက်နှင့် ချိတ်ဆက်လိုသောအခါချိတ်ဆက်သောနည်းလမ်းပေါ်မူတည်၍ သင့်ကွန်ပျူတာကို အခြားအသုံးပြုသူတစ်ဦးမှတရားမဝင် ဝင်ရောက်ခြင်းများပြုလုပ်နိုင်ပါသည်။

အကယ်၍သင်သည်ဖုန်းလိုင်းမှအင်တာနက်နှင့်Modemကိုအသုံးပြုပါကသင့်ကွန်ပျူတာကိုအင်တာနက်နှင့်တိုက်ရိုက်ချိတ်ဆက်ခြင်းဖြစ်သည့်အတွက် အင်တာနက်မှအခြားအသုံးပြုသူတစ်ဦး၏
တရားမဝင်ဝင်ရောက်နိုင်ခြင်းရာနှုန်းများပါသည်။ထို့ကြောင့် သင့်ကွန်ပျူတာ၏လုံခြုံမှုစနစ်ကို စစ်ဆေး ခြင်း (သို့) လုံခြုံမှုစနစ်ကာကွယ်ခြင်းဆော့ဝဲလ်ကို အသုံးပြုပါ။ (နောက်ပိုင်းတွင်ဖော်ပြထားသည့်အတိုင်း) အကယ်၍သင်သည် ADSL(သို့)DSLModemကိုအသုံးပြုပါကအင်တာနက်မှသင့်ကွန်ပျူတာကိုအခြားအသုံးပြုသူတစ်ဦး၏တရားမဝင်ဝင်ရောက်နိုင်ခြင်းရာနှုန်းနည်းပါသည်။ အဘယ်ကြောင့်ဆိုသော် ထိုစနစ်များတွင်
တရားမဝင်ဝင်ရောကခြင်းကိုကာကွယ်ထားသော Router လုပ်ဆောင်ချက်များ ပါဝင်သောကြောင့်ဖြစ်သည်။ သို့သော် Modem Setting လွဲချော်နေပါက တရားမဝင် ဝင်ရောက်နိုင်ခြင်းများ ရှိနိုင်ပါသည်။ ထို့ကြောင့်
သင့်ကွန်ပျူတာ၏လုံခြုံမှုစနစ်ကို စစ်ဆေးခြင်း (သို့) လုံခြုံမှုစနစ်ကာကွယ်ခြင်းဆော့ဝဲလ်ကို အသုံးပြုပါ။
(နောက်ပိုင်းတွင်ဖော်ပြထားသည့်အတိုင်း)

အကယ်၍သင်သည်CATV နှင့် Optical Fiber (သို့) VDSLModemကို အသုံးပြုပါက သင့်ကွန်ပျူတာနှင့်
အင်တာနက်ကြားတွင် ကြားခံပစ္စည်းမရှိသည့်အတွက် အင်တာနက်မှအခြားအသုံး ပြုသူတဦး၏ တရားမဝင်
ဝင်ရောက်နိုင်ခြင်း ရာနှုန်းမြင့်မားပါသည်။ ထို့ကြောင့်Router(သို့)Firewall စနစ်ကိုအသုံးပြုသင့်ပါသည်။
သို့သော်၄င်းစနစ်များ၏ တပ်ဆင်မှုလွဲချော်နေပါက တရားမဝင် ဝင်ရောက်နိုင်ခြင်းများရှိနိုင်ပါသည်။ အကယ်၍
သံသယဖြစ်ပါက သင့်ကွန်ပျူတာ၏လုံခြုံမှုစနစ်ကိုစစ်ဆေးခြင်း (သို့) လုံခြုံမှုစနစ်ကာကွယ်ခြင်း ဆော့ဝဲလ်ကို
အသုံးပြုပါ။(နောက်ပိုင်းတွင်ဖော်ပြထားသည့်အတိုင်း)

အကယ်၍သင်သည် အများသုံးကြိုးမဲ့အင်တာနက် LAN စနစ် (သို့) Business Hotelမှ
အင်တာနက်စနစ်ကိုအသုံးပြုပါက သင့်ကွန်ပျူတာကို အင်တာနက်မှအခြားအသုံးပြုသူတစ်ဦး၏ တရားမဝင်
ဝင်ရောက်နိုင်ပါသည်။အဘယ်ကြောင့်ဆိုသော် ထိုစနစ်များတွင် အသုံးပြုသူများစွာ ပါဝင်သောကြောင့်ဖြစ်သည်။

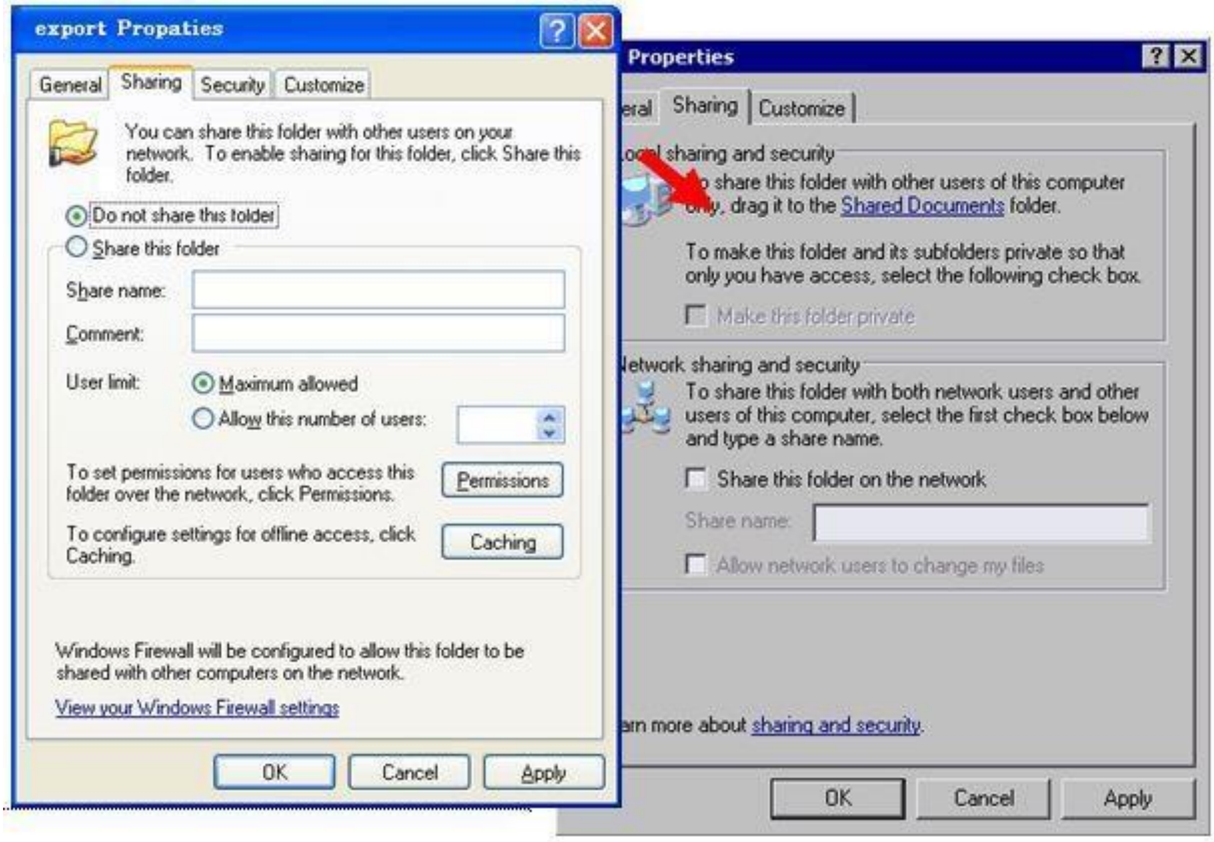
ထို့ကြောင့် သင့်ကွန်ပျူတာ၏လုံခြုံမှုစနစ်ကို စစ်ဆေးခြင်း (သို့) လုံခြုံမှုစနစ်ကာကွယ်ခြင်းဆော့ဖ်ဝဲလ်ကို အသုံးပြုပါ။(နောက်ပိုင်းတွင်ဖော်ပြထားသည့်အတိုင်း)

၄။ တရားမဝင် ဝင်ရောက်ခြင်းမှကာကွယ်နည်းများ ■

## ဖိုင်ဖလှယ်ခြင်းစနစ်ကို Disable ပြုလုပ်ပါ။

အကယ်၍ သင့်ကွန်ပျူတာသည် Business Hotel မှစနစနင့် ချိတ်ဆက်အသုံးပြုသောအခါ Window ၏ My Network မှ အခြားအင်တာနက်အသုံးပြုသူများ၏ ကွန်ပျူတာFolderများကိုတွေ့ရပါမည်။ ထိုအင်တာနက် နင ချိတ်ဆက်ထားသော ကွန်ပျူတာများအချင်းချင်းအကြား Folder များဖလှယ်နိုင်ခြင်းကြောင့်ဖြစ်သည်။ မိမိကွန်ပျူတာတွင်းသို့ ဝင်ရောက်နိုင်ရန် ဖိတ်ခေါ်ထားသကဲ့သို့ဖြစ်သည်။ ထို့ကြောင့် အသုံးပြုသူများစွာ ဝင်ရောက်အသုံးပြုနိုင်သောကြောင့်အင်တာနက်နှင့် ချိတ်ဆက်သောအခါ သင့်ကွန်ပျူတာ၏ Folder Sharing ကို Disableပြုလုပ်ပါ။

ဘယ်ဘက်ရှိပုံသည် Folder Sharing လုပ်နိုင်သောအခါ ဖော်ပြသောပုံဖြစ်သည်။Folder ကိုညာကလစ်နှိပ်၍ 'n [Property] 'n [Sharing] ကိုကလစ်နှိပ်ပါက Folder ၏ Property Window ပေါ်လာပါမည်။အကယ်၍သင်သည် Windows XP Professional Edition ကို အသုံးပြုပါက ဘယ်ဘက်ရှိပုံ အတိုင်း ပေါ်လာ ပါမည်။ အကယ်၍သင်သည် Windows XP Home Edition ကို အသုံးပြုပါက ညာဘက်ရှိပုံအတိုင်း ပေါ်လာပါမည်။ (ထို Window ၂ မျိုးသည် အနည်းငယ်ကွဲပြားနေပါမည်။)

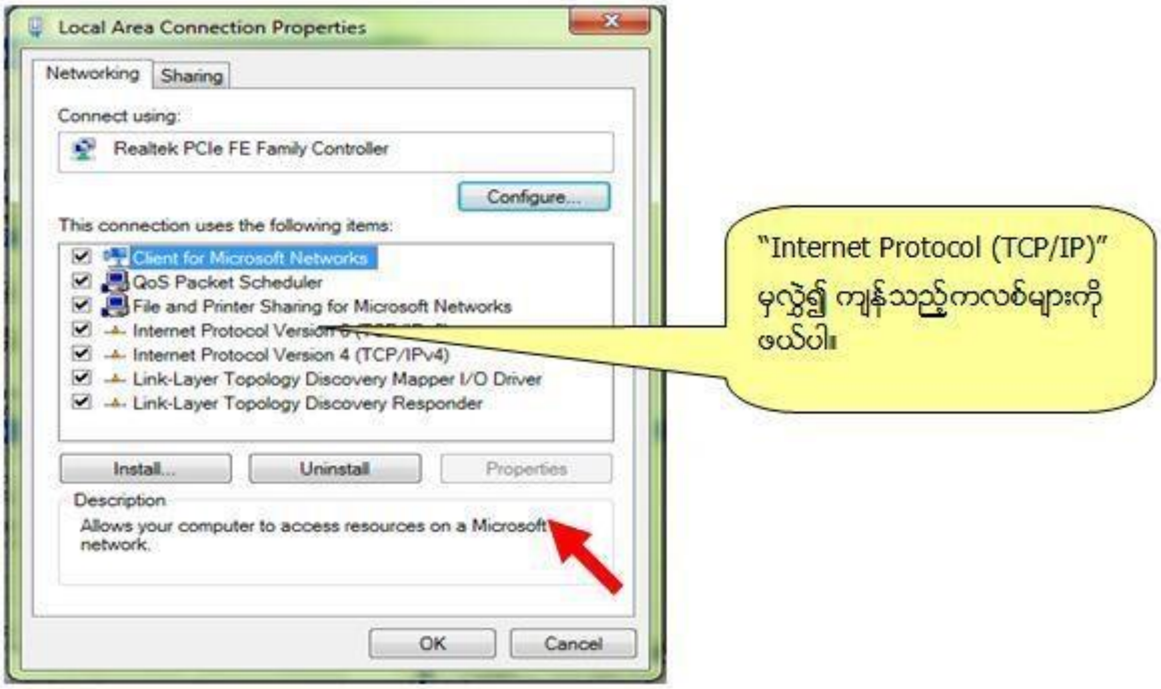


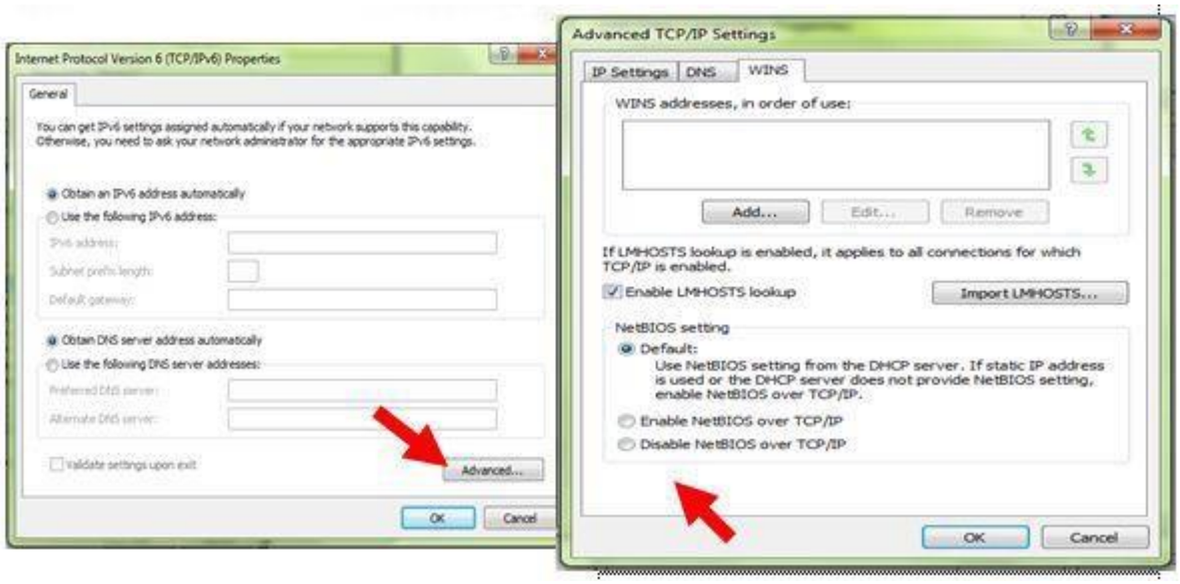

■ Local Area ၏ဆက်သွယ်မှုစနစ်ကိုပြောင်းပါ။

Local Area ၏ဆက်သွယ်မှုစနစ်ကိုပြောင်းပြီးလျှင်သင့်ကွန်ပျူတာကို Microsoft Windows Network မှမမြင်နိုင်စေရန်ပြုလုပ်ခြင်းကို အကြံပြုပါသည်။

လုပ်ဆောင်ချက်များ : [Start] ကိုကလစ်နှိပ်၍ ’n [Settings] ’n [Control Panel] ’n [Network Connection] ’n [Local Area Connection] ကိုညာကလစ်နှိပ်၍ ’n [Properties] ကိုကလစ်နှိပ်ပါ။ The Local Area Connection Properties Window ပေါ်လာ ပါမည်။

[Local Area Connection Properties] Window မှ “Internet Protocol (TCP/IP),” ကိုကလစ်နှိပ်၍ ’n [Properties] ’n [Details] ’n [WINS] ’n [Disable NetBios over TCP/IP]ကိုကလစ်နှိပ်ပါ။



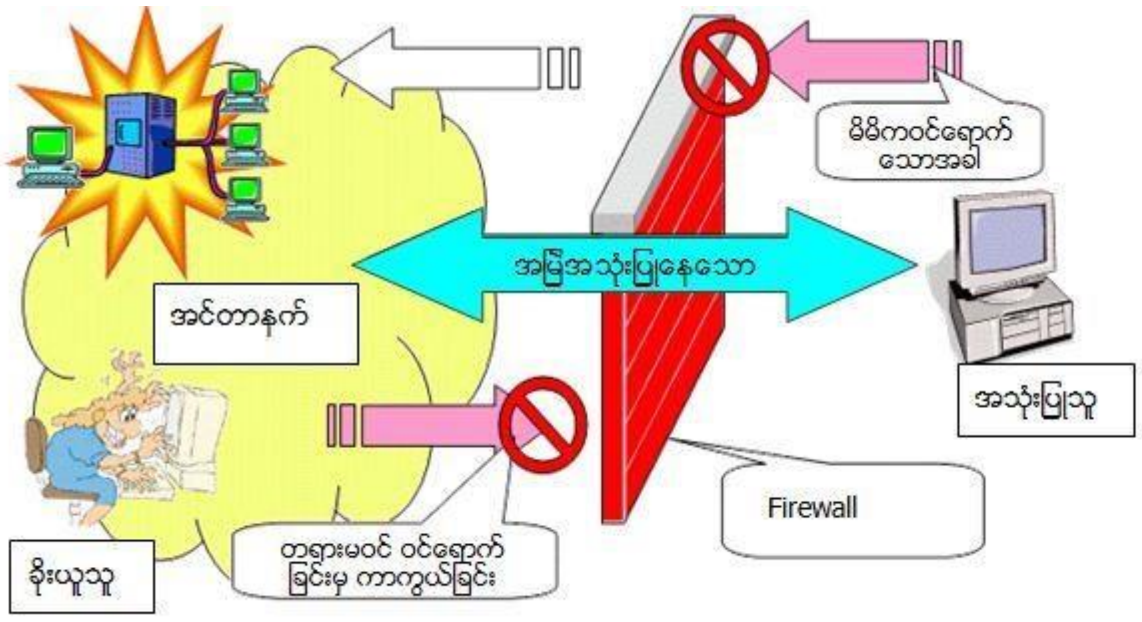




(သတိပေးချက်)

အကယ်၍သင်သည် Networkနှင့်ပြန်လည်ဆက်သွယ်သောအခါ သင့်ကွန်ပျူတာ၏စနစ်ကို မူလနေရာသို့ ပြန်လည်ထားရှိရန်လိုအပ်ပါသည်။ ထိုသို့မပြုလုပ်ပါကNetworkမှတဆင့်Printerများနှင့်ဆက်သွယ်၍ မရနိုင်ခြင်း ၊ဖိုင်များဖလှယ်၍ မရနိုင်ခြင်းများဖြစ်နိုင်ပါသည်။
အကယ်၍သင်သည် Network မှ Printerများနှင့်ဆက်သွယ်မထားလျှင် (သို့) ဖိုင်များဖလှယ်ခြင်းကို အသုံးမပြုလျှင်သင့်ကွန်ပျူတာ၏စနစ်ကို ပြန်လည်ပြုပြင်ရန်မလိုအပ်ပါ။

၅။ Firewall ဆော့ဖ်ဝဲလ် (ဘက်ပေါင်းစုံလုံခြုံမှုစနစ်ကာကွယ်ခြင်းဆော့ဖ်ဝဲလ်) များကို
အသုံးပြုပါ။

Firewall ဆော့ဖ်ဝဲလ်သည် တရားမဝင် ဝင်ရောက်ခံရခြင်းမှကာကွယ်ပေးနိုင်သော အဓိကလက်နက်ဖြစ်သည်။ ဗိုင်းရပ်စ်ကာကွယ်ခြင်း၊ Spywareကာကွယ်ခြင်းများတွင် သာမက Firewall စနစ် (သို့) ကိုယ်ပိုင် Firewall ဆော့ဖ်ဝဲလ်ကို ဘက်ပေါင်းစုံလုံခြုံမှုစနစ်ကာကွယ်ခြင်းဆော့ဖ်ဝဲလ်နှင့် တွဲဖ က်အသုံးပြုရန် အကြံပြုပါသည်။ Firewallသည်ကွန်ပျူတာနှင့် အင်တာနက်ကြား သတင်းအချက်အလက် ဖလှယ်ခြင်းကို ထိန်းချုပ်ပေးသောကြောင့် မမှန်မကန်ဝင်ရောက်မှုများတွေ့ရှိပါက သတိပေးချက်များပေါ်လာခြင်း၊ ကာကွယ်ပေးခြင်းများကို ပြုလုပ်ပေးပါသည်။ ထို့အပြင် Spyware ဗိုင်းရပ်စ်များမှတဆင့် မိမိကွန်ပျူတာအတွင်းမှ သတင်းအချက်အလက်များကို ပြင်ပသို့ပေးပို့ခြင်းများဖြစ်ပေါ်သောအခါ Firewallသည်သတိပေးချက်များပြုလုပ်ပေးခြင်းဖြင့် သင့်ကွန်ပျူတာကို အချိန်မီကာကွယ်ပေးနိုင်ပါမည်။



မိုဘိုင်းစနစ်များတွင် Routerနှင့်Firewallစနစ်များရှိသည့်အတွက်၎င်းတို့ကိုအသုံးပြုပါကမိမိကွန်ပျူတာတွင် ကိုယ်ပိုင် Firewall ဆော့ဖ်ဝဲလ် (သို့)ဘက်ပေါင်းစုံလုံခြုံမှုစနစ်ကာကွယ်ခြင်း ဆော့ဖ်ဝဲလ်ကိုအသုံးပြုရန်အကြံပြုပါသည်။

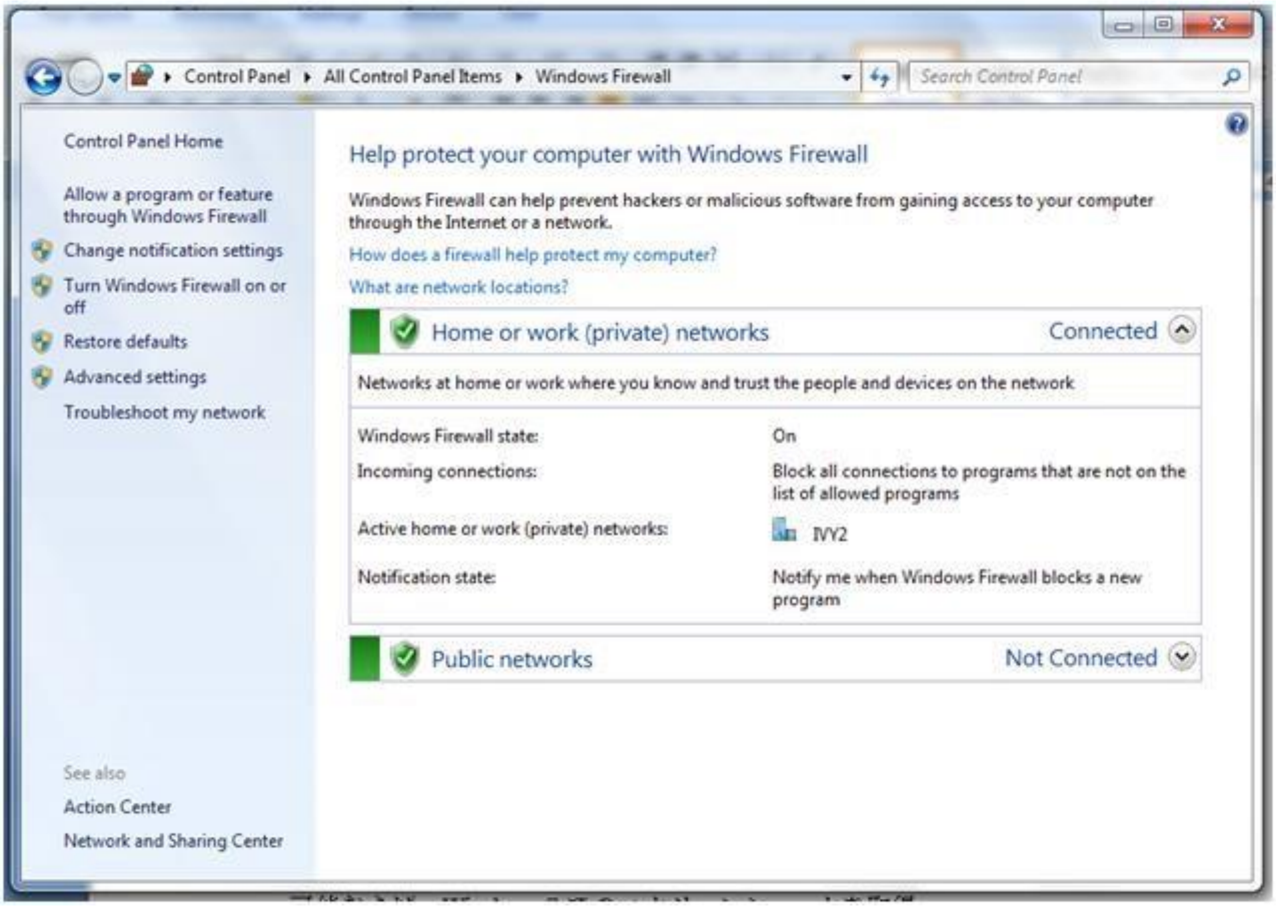
အကယ်၍သင်သည် Windows XP ကို အသုံးပြုပါက OS တွင်ပါဝင်သော Window Firewallကိုအသုံးပြုရန်အကြံပြုပါသည်။

Window Firewall သည် ပြင်ပမှ မလိုလားဖွယ်အချက်အလက်များဝင်ရောက်မှုများကို ကာကွယ်ပေးသော်လည်း အတွင်းမှအချက်အလက်များပြင်ပသို့ပျံ့နှံ့ခြင်းများကို ကာကွယ်မပေးနိုင်ပါ။ (Windows XP တွင်ဖြစ်သည်။ Windows Vista တွင် နှစ်ဘက်စလုံးမှဝင်ရောက်ခြင်းကို ကာကွယ်ပေးနိုင်ပါသည်။)သို့သော် ၎င်းသည် OS နှင့် Applicationဆော့ဖ်ဝဲလ်များ၏ စနစ်အားနည်းမှုကြောင့်ဝင်ရောက်လာနိုင်သောပြင်ပမှတိုက်ခိုက်မှုများ ကိုကောင်းစွာ ကာကွယ်ပေး နိုင်ပါသည်။ ထို့ကြောင့် သင်သည် ကိုယ်ပိုင် Firewall ဆော့ဖ်ဝဲလ် (သို့) ဘက်ပေါင်းစုံလုံခြုံမှုစနစ်ကာကွယ်ခြင်း ဆော့ဖ်ဝဲလ်ကို အသုံးမပြုနိုင်ပါက Window Firewall ကိုအသုံးပြုပါ။

လုပ်ဆောင်ချက် :

Start'n Setting 'n Control panel 'n

Windows Security Center 'n Windows Firewall

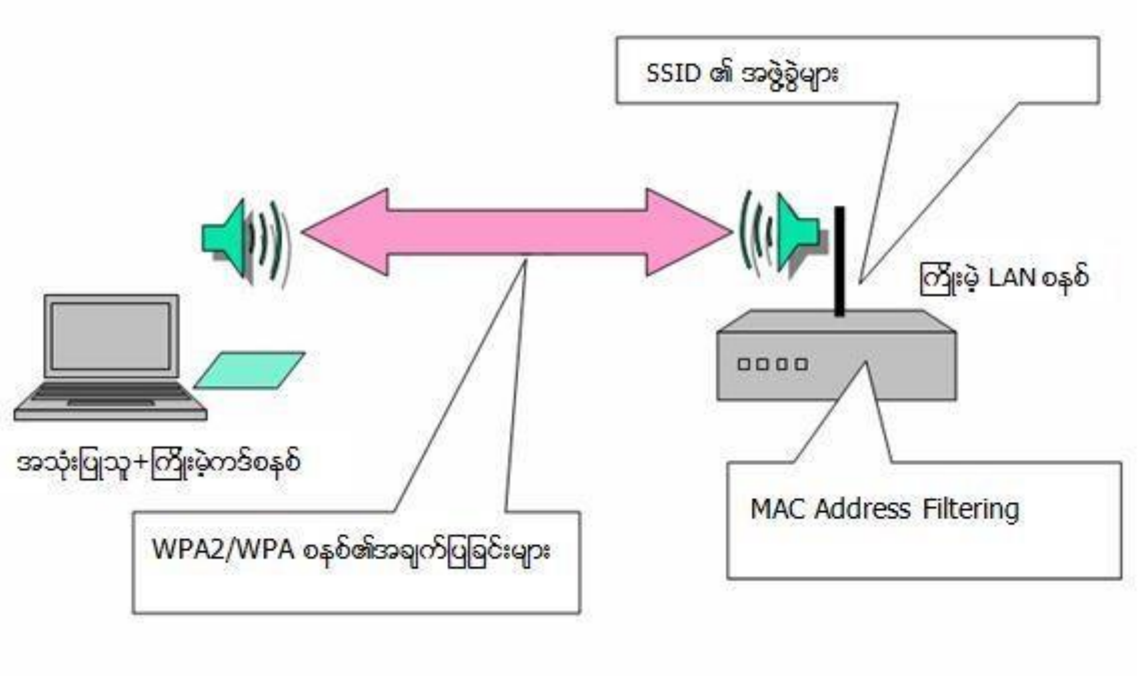


၆။ ကြိုးမဲ့ LAN စနစ်၏အခြေခံ။

 ကြိုးမဲ့ LAN စနစ်သည် Network ကြိုးများဆက်သွယ်စရာမလိုဘဲ နေအိမ် (သို့) ရုံးခန်းများအတွင်း လျှပ်စစ်လှိုင်း ရောက်နိုင်သည့်အတိုင်းအတာအထိ အသုံးပြုနိုင်သောစနစ်ဖြစ်ပါသည်။သို့သော် လုံခြုံမှုစနစ်တွင် တပ်ဆင်မှုလွဲချော်ပါက မိမိကွန်ပျူတာအတွင်းမှ အချက်အလက်များ ခိုးယူခံရနိုင်ခြင်း (သို့) မိမိ၏ကြိုးမဲ့ LAN စနစ်ကိုအခြားသူတစ်ဦးမှခိုးယူသုံးစွဲခြင်းများဖြစ်နိုင်ပါသည်။

;နောက်ဆုံးပေါ်ကြိုးမဲ့ LAN စနစ်များသည်အသုံးပြုသူများအတက်ွ လိုအပ်မှုများကိုအနည်းဆုံးဖြစ်အောင် ပြုလုပ် ထားပါသည်။

;အောက်ပါနည်းလမ်းများကို လိုက်နာပါ။ (အသေးစိတ်အနေဖြင့် ကြိုးမဲ့ LAN စနစ်၏ ညွှန်ကြားချက်များကိုလေ့လာပါ။)




■ Wireless Access Point Device

;□ WPA/WPA2 (*5) တွင်ထားပါ။

※ WEP (*6) ၏စနစ်အားနည်းခြင်းရှိသည့်အတွက် အသုံးမပြုသင့်ပါ။

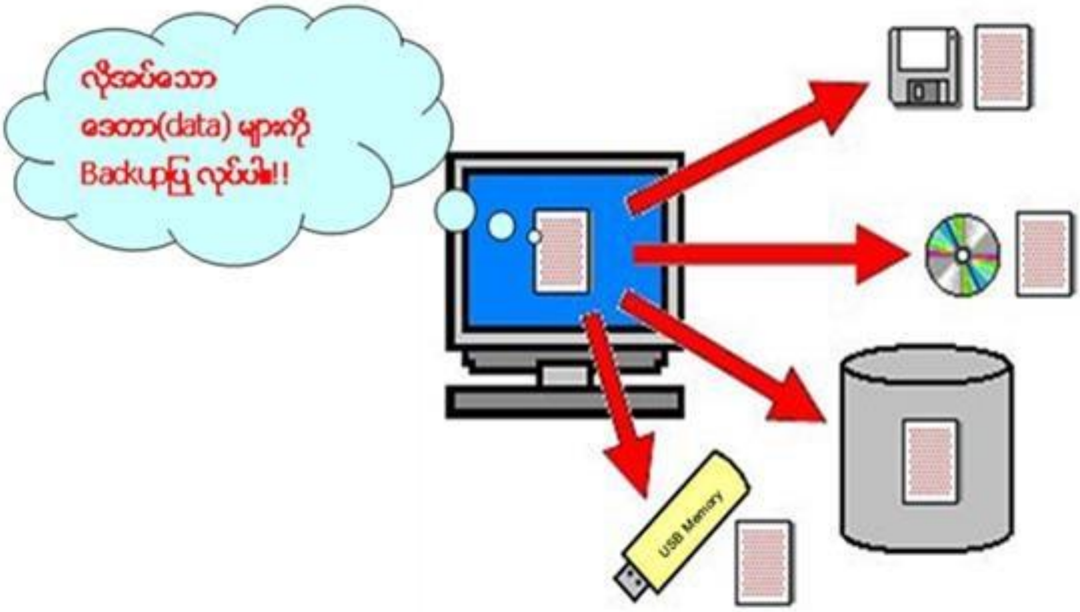
;□ SSID (*7) တွင်ထားပါ။

□ MAC address (*8) ၏ filtering ကိုတပ်ဆင်ပါ။

□ မိမိနှင့်မသိသူများထံမှဆက်သွယ်မှုများကို လက်မခံပါနှင့်။

■ Access point ၏တပ်ဆင်မှုစနစ်နှင့်အညီ
ကွန်ပျူတာ၏စနစ်ကိုပြုပြင်ပါ။

၇။ လိုအပ်သော ဖိုင်များကို အရန်အဖြစ် ကူးယူထားပါ။
မိမိကန္ဒ ပျူတာသည် တရားမဝင်ဝင်ရောက်ခြင်းခံရသောအခါတင္ဒ ၄င်း၊
မယုံကြည်ရသောပရိုဂရမ်များ ဝင်ရောက်၍ သော်၎င်း၊
ကန္ဒ ပျူတာ၏စနစ်ကိုပြောင်းလဲလို၍သော်၎င်း၊ မိမိကန္ဒ ပျူတာကို နဂိုအတိုင်း
ပြန်လည်ပြင်ဆင်မွန်းမံရန် ကွန်ပျူတာစနစ်က အသစ်ပြန်စရပါမည်။
ထိုသို့မပြုလုပ်မှီအရေးကြီးသော ဖိုင်များကို အရန်အဖြစ် ကူးယူထားရန် လိုအပ်ပါသည်။
ထို့အပြင်အသုံးပြုထားသော မူရင်း CD-ROM များကို သေသေချာချာ သိမ်းဆည်းထားရပါမည်။
အကယ်၍ မိမိကွန်ပျူတာ၏စနစ်ကို မွန်းမံလိုက်သည့်အခါ မူရင်း CD-ROM မှတဆင့်ကူးယူခြင်းဖြင့်
နဂိုအတိုင်း ပြန်လည်ဖြစ်ပါမည်။




[System Recovery Function]

Windows XP တွင် Recovery စနစ်ပါရှိပါသည်။ ထိုစနစ်ကိုအသုံးပြု၍ မိမိကွန်ပျူတာကို နဂိုအတိုင်းပြန်လည်ပြင်ဆင်မွန်းမံနိုင်ပါသည်။
ဥပမာ မိမိကွန်ပျူတာသည် တရားမဝင် ဝင်ရောက်ခြင်းခံရသောအခါတွင်ထိုစနစ်ကိုအသုံးပြု၍ မိမိကွန်ပျူတာကို နဂိုအတိုင်း ပြန်လည်ပြင်ဆင်မွန်းမံနိုင်ပါသည်။ ထို့ပြင်မယုံကြည်ရသောဖိုင်များကို ဖွင့်မိရာမှတဆင့် သံသယဖြစ်ဖွယ် တွေ့ရှိပါက ထိုစနစ်ကိုအသုံးပြု၍ မိမိကွန်ပျူတာကို ပြန်လည်ပြင်ဆင်မွန်းမံနိုင်ပါသည်။ အသေးစိတ်ကိုအောက်ဖော်ပြပါဆိုဒ်တွင် ဝင်ရောက်လေ့လာပါ။

Recovering Windows XP using the System Recovery Function (Microsoft ကုမ္ပဏီ)

http://support.microsoft.com/default.aspx?scid=kb;ja;306084

၈။ အကယ်၍ ကူးဆက်ခြင်းခံရပါက……

သင့်ကွန်ပျူတာသည် တရားမဝင် ဝင်ရောက်ခြင်းခံရသော သံသယဖြစ်ဖွယ်တွေ့ရှိပါကဦးစွာဗိုင်းရပ်စ်နှိမ်နင်းရေး ဆော့ဖ်ဝဲလ်များ (Spyware / Virusစစ်ဆေးနှိမ်နင်းရေးဆော့ဖ်ဝဲလ်များ) ကိုအသုံးပြု၍ကွန်ပျူတာကိုစစ်ဆေးပါ။ တရားမဝင် ဝင်ရောက်နေသော ပရိုဂရမ်အမည်ကိုတွေ့ရှိပြီး ၎င်းကိုဖယ်ရှား၍မရနိုင်ပါက မိမိအသုံးပြုသော လုံခြုံမှုစနစ်ကာကွယ်ခြင်းဆော့ဖ်ဝဲလ်၏ Websiteတွင်၎င်းပရိုဂရမ်အမည်နှင့်ဖယ်ရှားနိုင်မည့်နည်းလမ်းများကို ရှာဖွေစုံစမ်းပါ။ လုံခြုံမှုစနစ်ကာကွယ်ခြင်းဆော့ဖ်ဝဲလ်ကို အသုံးမပြုဘဲအင်တာနက်နှင့် ချိတ်ဆက်လိုပါက အခမဲ့ပေးသောOnlineScanကို သုံး၍တရားမဝင်ဝင်ရောက်နေသော ပရိုဂရမ်အမည်နှင့်ဖယ်ရှားနိုင်မည့် နည်းလမ်းများကိုရှာဖွေပါ။ တရားမဝင် ဝင်ရောက်နေသော ပရိုဂရမ်အမည်ကိုသိရှိပါက Online Scan လုပ်သည့် Websiteမှဖော်ပြထားသော ဖယ်ရှားနိုင်မည့် သင့်တော်သည့်နည်းလမ်းဖြင့် စမ်းသပ်အသုံးပြုပါ။

၉။ ကိုးကားချက်

အောက်ဖော်ပြပါဆိုဒ်များသို့ ဝင်ရောက်လေ့လာပါ။

■ တရားမဝင် ဝင်ရောက်ခြင်းခံရခြင်းမှကာကွယ်ခြင်း

http://www.ipa.go.jp/security/fusei/ciadr.html

■ ကွန်ပျူတာကိုတရားမဝင် ဝင်ရောက်ခြင်းခံရခြင်းနှင့်ပတ်သက်သောအမေးအဖြေများ

http://www.ipa.go.jp/security/ciadr/faq01.html

■ security at home : ကွန်ပျူတာကိုကာကွယ်ခြင်း (Microsoft ကုမ္ပဏီ)

http://www.microsoft.com/japan/protect/"

၁၀။ ဝေါဟာရ ရှင်းလင်းချက်

(*2) စနစ်အားနည်းခြင်း

လုံခြုံမှုစနစ်အားနည်းခြင်းသည် အခြားစနစ်များ network၂း၊ Applicationများ၊

protocolsများ၏လုံခြုံရေးစနစ်ကိုပါအဆင့်နိမ့်ကျစေပါသည်။ ထိုမှတဆင့် မလိုလားအပ်သောအဖြစ်အပျက်များဖြစ်ပေါ်လာစေပြီး ပြုပ်ဆောင်ချက်များ၊ အမှားများကို ဖြစ်ပေါ်စေပါသည်။ Operating စနစ်အားနည်းခြင်း၊ Application စနစ်အားနည်းခြင်း စသည်ဖြင့်ရှိပါသည်။ ထို့ပြင် ဆော့ဖ်ဝဲလ်အားနည်းခြင်းအပြင်လုံခြုံမှုစနစ်မလုံလောက်လျှင်လည်းစနစ် အားနည်းခြင်းဖြစ်နိုင်ပါသည်။ ၎င်းကို အများအားဖြင့် Security whole ဟုခေါ်ဆိုပါသည်။

(*3) Access Control

ကွန်ပျူတာလုံခြုံမှုစနစ်အရ ကွန်ပျူတာအသုံးပြုသူမှ မိမိ၏ကွန်ပျူတာစနစ်အတွင်း ဝင်ရောက်နိုင်ခြင်း (သို့)ထိန်းချုပ်နိုင်ခြင်း ကိစ္စများကိုခေါ်ဆိုပါသည်။

(*4) အသုံးပြုသူ ID နှင့် Password

အသုံးပြုသူ ID နှင့် Password ဆိုသည်မှာ မိမိကိုယ်ပိုင်ဖြစ်ကြောင်း သက်သေများဖြစ်သည်။ ၎င်းတို့သည်အကြမ်းအားဖြင့်လက်ဗွေ၊ လက်မှတ်၊ အသံ၊ ဓာတ်ပုံစသည်ဖြင့်ဖြစ်နိုင်သော်လည်း ဤစာအုပ်တွင် မိမိကိုယ်ပိုင်ဖြစ် ကြောင်းသက်သေများကို အသုံးပြုသူ ID နှင့် Password ဟုခေါ်ဆိုပါသည်။

(*5) WPA2/WPA (Wi-Fi Protected Access)

WEP နှင့်အစားထိုးရန်အတွက် ကြိုးမဲ့ LAN စနစ်ကိုအားပေးသော Wi-Fi Alliance စနစ်ကိုခေါ်ပါသည်။ WEP ၏စနစ်အားနည်းချက် ကိုဖြည့်ဆည်းထားပြီး လုံခြုံမှုစနစ်ကိုပါ အားဖြည့်ပေးထားပါသည်။ WPA2 စနစ်သည် ပို၍ခိုင်မာသောလုပ်ထုံးများ (Advanced Encryption Standard) ကိုအသုံးပြုထားပါသည်။

(*6) WEP (Wired Equivalent Privacy)

IEEE ၏အဓိပ္ပာယ်ဖွင့်ဆိုချက်အရ ခိုင်မာသော RC4လုပ်ထုံးများကိုအခြေခံသည့်စနစ်ဖြစ်သည်။ သို့သော် WEPစနစ်တွင်အားနည်းချက်များစွာ တွေ့ရှိရပါသည်။

(*7) SSID (Service Set IDentifier)

Access point (AP) ကို မှတ်မိစေရန်အသုံးပြုသော IDကို ခေါ်ပါသည်။ ESSID ဟုလည်းခေါ်ဆိုပါသည်။

(*8) Mac Address

Mac Address တွင်ကြိုးမဲ့ LAN Adaptor စနစ်၏ ID ကို ခေါ်ပါသည်။

※ဤစာအုပ်သည် ကွန်ပျူတာသတင်းအချက်အလက်များကာကွယ်ဆောင်ရွက်မှုအဖွဲ့အစည်း (IPA) ၏
ကွန်ပျူတာကွန်ရက် လုံခြုံရေးစင်တာမှပြဌာန်း ထုတ်ဝေပါသည်။
ဂျပန်အစိုးရ၏ဘာသာပြန်မှုဖြင့်အရှေ့တောင်အာရှနိုင်ငံများသို့ အခမဲ့ဖြန့်ဝေပေးမည်ဖြစ်ပါသည်။ထို့ပြင် ဤစာအုပ်သည်
ဂျပန်အစိုးရ၏ ခွင့်ပြုချက်မရဘဲစီးပွားဖြစ်ကူးယူအသုံးပြုခြင်း၊ လွှဲပြောင်းပေးခြင်း၊ ထုတ်လွှင့်ပြသခြင်းများ မပြုလုပ်ရ။
(ဆက်သွယ်ရန်: အစိုးရ၏ကွန်ပျူတာသတင်းအချက်အလက်များ၏ကွန်ရက်လုံခြုံရေးစင်တာ（NISC）〒 100-0014တိုကျိုမြို့ချိုရောဒရပ်ကွက် နဂတမြို့နယ်2-4-12 poc@nisc.go.jp)

"Be Secure, Aware and Vigilant"

Copyright © 2016, Myanmar Computer Emergency Response Team.

Pdf Prepared By: Heavenly Moe