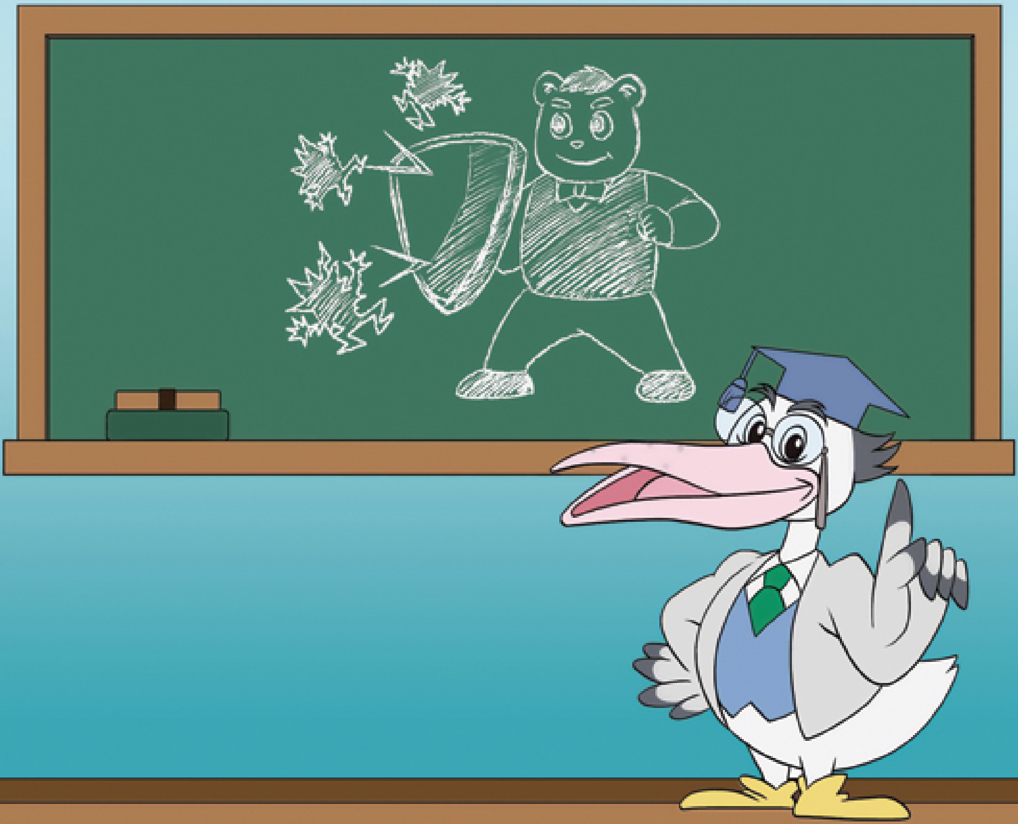
ကာတွန်းစာအုပ်

ဆိုက်ဘာလုံခြုံရေးကို သင်ယူကြပါစို့

သိရှိသတိပြုစေရန်၊ လုံခြုံမှုရှိစေရန် နှင့် နိုးနိုးကြားကြားရှိစေရန်



စမတ်ဖုန်းများအတွက် လုံခြုံရေး

အပိုင်း၁

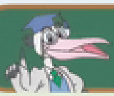
ဘာဖြစ်တာပါလိမ့်
သတိပေးချက်။
သင့်စမတ်ဖုန်းထဲတွင် တရားမဝင်
Application တစ်ခု တွေ့ရှိရသောကြောင့်
သင့်စမတ်ဖုန်းအား Lock ပြန်ဖြည်ရန်
ကျေးဇူးပြု၍ ၃ ရက်အတွင်း
မြန်မာငွေ ▲▲▲ သိန်း ပေးချေပါ။
ငွေကြေးမပေးချေရသေးမီအထိ
သင့်စမတ်ဖုန်းအား
Lock ချထားမည်ဖြစ်သည်။
အိုး... အမလေး ငါ့ရဲ့စမတ်ဖုန်း အလုပ်မလုပ်တော့ပါလား။
ငါ ဘယ်လိုလုပ်ရပါ့မလဲ။
ဥပဒေချိုးဖောက်မှု
ငါ ဘယ်သူ့ကို ပြောရမလဲ မသိတော့ဘူး။
ကောင်းပြီ။ ငါ့ဖုန်း Lock ကျနေတာကို ပြန်ဖြည်ဖို့ ငွေပေးလိုက်ရင် ပြန်ကောင်းလာမယ် ထင်တာပဲ။

XX ဘဏ်
အားလုံးအဆင်ပြေသွားမှာပါ။ ဒါပေမယ့် ဈေးတော့ တော်တော်ကြီးတယ်။
ကောင်းပြီ။ ခုတော့ ဖုန်းလေး ပြန်ကောင်းတော့မယ်။
ဘာ
ဘာလဲ။
သင့်ရဲ့မိုဘိုင်းဖုန်း Lock ပြန်မဖြည်နိုင်ပါ။
ဆရာ ကူညီပါဦး။
ဘာဖြစ်လို့လဲ။
ကျွန်တော့် မိုဘိုင်းဖုန်း Lock ပြန်ဖြည်ဖို့ ငွေလည်းပေးပြီးသွားပြီ။ ဒါပေမယ့် အခုထိ Lock ကျနေတုန်းပဲ။
ဒါ လိမ်တာပဲ ဖြစ်ရမယ်။
အခမဲ့ရတဲ့ မိုဘိုင်း Application တွေမှာ ပိုင်းရပ်စ်တွေ တွေ့ရတတ်တယ်။
ဒါကြောင့် Anti-virus Software ကို Install တာမျိုးနဲ့ စိတ်ချရတဲ့ site တွေကနေပဲ Application တွေကို Download တာမျိုး စတာတွေ လုပ်သင့်ပါတယ်။
ဟုတ်ကဲ့ ကျွန်တော် နားလည်ပါပြီ။

NO.1 (အနှစ်ချုပ်) စမတ်ဖုန်းများအတွက် လုံခြုံရေး

ရှောင်ကြဉ်ရန်

- အန္တရာယ်ရှိသော ဗိုင်းရပ်စ်များကို ကွန်ပျူတာများတွင် သာမက စမတ်ဖုန်းများတွင်လည်း တွေ့ရှိရပါသည်။
- သင့်ကွန်ပျူတာ (သို့မဟုတ်) စမတ်ဖုန်းများတွင် အခမဲ့ရရှိသော Application များမှ အန္တရာယ် ကျရောက်တတ်ပါသည်။
- သင့်ကွန်ပျူတာ (သို့မဟုတ်) စမတ်ဖုန်းများ၏ Operating System (သို့) Application များကို Update မပြုလုပ်ခဲ့လျှင်လည်း အန္တရာယ် ရှိနိုင်ပါသည်။



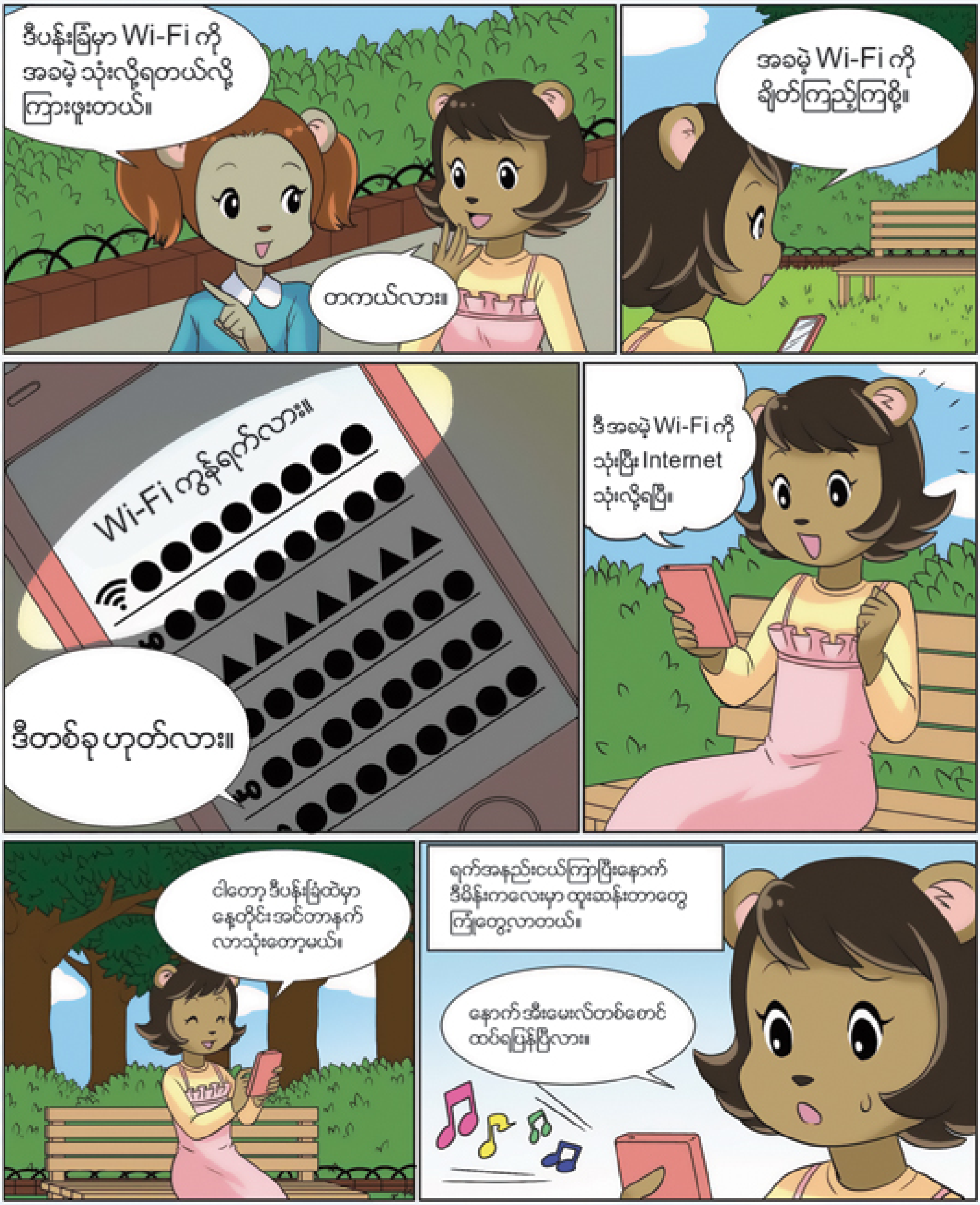
ဆောင်ရွက်ရန်

- သင်၏ကွန်ပျူတာနှင့် စမတ်ဖုန်းများတွင် Anti-virus Software ကို Install ပြုလုပ်ပါ။
- Application များကို Download ရယူရာတွင် ၎င်းတို့၏ဖော်ပြချက်၊ ထုတ်လုပ်သူ၊ ကုမ္ပဏီအချက်အလက်များနှင့် ဝေဖန်ရေးသားချက်များကို သေချာစစ်ဆေးပြီး ယုံကြည်စိတ်ချရသော ဝက်ဘ်ဆိုက်များမှသာ Download ရယူပါ။
- သင့်ကွန်ပျူတာနှင့် စမတ်ဖုန်းများ၏ Operating System နှင့် Application များကို အမြဲတမ်း နောက်ဆုံးဗားရှင်းသို့ Update ပြုလုပ်ပါ။

သိမှတ်စရာ အတိုအထွာ

- Ransomware ဆိုသည်မှာ သင်၏ကွန်ပျူတာ (သို့မဟုတ်) စမတ်ဖုန်းကို Lock ကျသွားစေသော အန္တရာယ်ရှိသည့် Software အမျိုးအစားဖြစ်ပြီး Lock ပြန်ဖြည်ရန် ငွေကြေးပေးချေရပါသည်။ ကွန်ပျူတာများ သာမက စမတ်ဖုန်းများတွင် တွေ့ရှိရသော Ransomware ကို အထူးသတိပြုပါ။
- Spam Mail များတွင် တွဲလျက်ပါရှိလာသော ဖိုင်များကို မဖွင့်ပါနှင့်။ ၎င်းဖိုင်များကို ဖွင့်ခဲ့လျှင် သင်၏ကွန်ပျူတာနှင့် စမတ်ဖုန်းများသည် ဗိုင်းရပ်စ်များကြောင့် အန္တရာယ်ရှိနိုင်ပါသည်။

အပိုင်း ၂ ကြိုးမဲ့ LAN ၏ လုံခြုံရေး



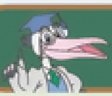
သိပ်မကြာခင်ကပဲ Spam အီးမေးလ် တွေ အများကြီး ရခဲ့တယ်။
သင့်ဆီမှာအီးမေးလ် အသစ်အစောင် ၇၂၀ ရှိနေပါသည်။
နောက်ထပ် ထူးဆန်းတာတွေလဲ ဖြစ်လာတယ်။
ဖုန်းတွေလဲ ခေါ်ခံရတယ်။
ဖုန်းဝင်တာ အခါ ၃၀ တောင် ရှိနေပြီ။
ထို့ပြင်
ငါမနေ့က အင်တာနက်သုံးရင်း နှင့်ခါတ်ပုံကို အင်တာနက်မှာ တွေ့လိုက်တော့ အရမ်းအံ့ဩသွားတယ်။
သေချာရဲ့လား
ဒါကရော ဘာလဲ
ငါ ဒီပုံကို ဘယ်လူမှုကွန်ရက်စာမျက်နှာ မှာမှ မတင်ထားဖူးပါဘူး။
Mr. Anonymity

ဟားဟား
အမလေး။ ငါ့ဆီ ဒီပြဿနာမျိုး ဘယ်လိုလာဖြစ်ရတာလဲ။
ဆရာရေ ကျွန်မရဲ့ဓါတ်ပုံတွေ အင်တာနက်မှာ ပျံ့နေတယ်။
အို... ဟုတ်လားသမီး။ သမီးတော့ ပြဿနာအကြီးကြီး တက်ပြီပေါ့။
ပန်းခြံထဲမှာ အခမဲ့လွှင့်ပေးတဲ့ Wifi ကို သုံးကတည်းက ကျွန်မမှာ ထူးခြားတာတွေ တစ်ချို့တစ်ခု ဖြစ်နေတော့တာပဲ။
အဲ့အကြောင်းရင်းကြောင့်ဆိုတာ ဖြစ်နိုင်တာပေါ့။ မသိတဲ့ Wi-Fi ကို ချိတ်ပြီး အင်တာနက် သုံးတာက အရမ်းအန္တရာယ် များပါတယ်။
ဒါကြောင့် Encrypt လုပ်ထားပြီး စိတ်ချယုံကြည်ရတဲ့ Wi-Fi ကိုပဲ အသုံးပြုသင့်ပါတယ်။
အန္တရာယ်များမှန်းမသိခဲ့ဘူး။ အလကားရလို့ သုံးမိတာပါ။
အခုကစပြီး အဲ့လိုအခမဲ့ရတဲ့ Wi-Fi မျိုးကို မသုံးမိဖို့ သတိထားပါတော့မယ်။

NO.2 (အနှစ်ချုပ်) ကြိုးမဲ့ LAN ၏ လုံခြုံရေး

ရှောင်ကြဉ်ရန်

- မည်သူမဆို အသုံးပြုနိုင်ရန် လွှင့်ထားသော အခမဲ့ Wi-Fi Access Point အချို့သည် အန္တရာယ်ရှိစေရန် ရည်ရွယ်ချက်များဖြင့် ပြုလုပ်ထားခြင်းဖြစ်ပါသည်။
- အန္တရာယ်ရှိသည့် Access Point ကို ချိတ်ဆက်မိသောအခါတွင် တစ်စုံတစ်ယောက်မှ သင်၏ ဆက်သွယ်မှုများကို ကြားဖြတ်လုပ်ဆောင်နိုင်သည်ကို သတိပြုရပါမည်။
- သင်သည် ယုံကြည်စိတ်ချရသော အများပြည်သူများ အသုံးပြုနေသည့် ISP မှ Wireless LAN ကို အသုံးပြုသည့်တိုင်အောင် Encrypt မပြုလုပ်ထားပါက သင်၏ ဆက်သွယ်မှုများကို ကြားဖြတ်ရယူနိုင်မည် ဖြစ်သည်။



ဆောင်ရွက်ရန်

- မယုံကြည်ရသော၊ မသိသော နေရာမှ အများပြည်သူသုံး Wi-Fi များကို ချိတ်ဆက်အသုံးမပြုပါနှင့်။
- အကယ်၍ အများပြည်သူသုံး Wi-Fi ကို ချိတ်ဆက်ရန် လိုအပ်လာပါက Encrypt လုပ်ထားကာ စိတ်ချရသည့် Wi-Fi ကိုသာ အသုံးပြုပါ။

သိမှတ်ဖွယ်ရာ အတိုအထွာ

- သင်သည် အများပြည်သူသုံး Wi-Fi ကို အသုံးပြုမည်ဆိုလျှင် Wi-Fi ၏ဖွဲ့စည်းပုံစနစ်ကို သတိပြုပါ။ သင်၏ကွန်ပျူတာ (သို့မဟုတ်) စမတ်ဖုန်းတွင် "ဖိုင်မျှဝေခြင်းစနစ်"ကို ဖွင့်ပေးထားခဲ့မည်ဆိုပါက တူညီသော Wi-Fi ကို အသုံးပြုနေသော မည်သူမဆို သင်၏ ဖိုင်များကို တွေ့မြင်နိုင်မည် ဖြစ်ပါသည်။
- သင်၏ Wi-Fi ကို Password ထားခြင်းဖြင့် လုံခြုံစိတ်ချပါစေ။ အခြား မသိသောသူများ၏ ချိတ်ဆက်မှုကို ခွင့်မပြုပါနှင့်။

အင်တာနက်ပေါ်မှ လိမ်လည်မှု

အပိုင်း၃

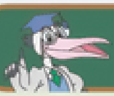
XX ဘဏ်ကို
ကဲ ပြီးသွားပြီ! ကျူသင့်ငွေလဲ ချေပြီးပြီဆိုတော့ အိတ်ကလေးရဖို့ စောင့်နေရုံပဲ လိုတော့တယ်။
ငါတကယ်လိုချင်နေတဲ့ အိတ်ကလေးကို ၉၀ % လျှော့ဈေးနဲ့ ဝယ်လိုက်နိုင်ပြီ။
ဟယ် တကယ်လား
တစ်လကြာပြီးနောက်
ဟင်း ... အိတ်က ခုထိကို မရောက်လာသေးပါလား။
Pi
Pi
စတိုးဆိုင်ရဲ့ Website ကို ဝင်ကြည့်ဦးမှပါပဲ။
အိုး! ဘာဖြစ်တာပါလိမ့်။
Website စာမျက်နှာက ပိတ်ထားပါလား။ ဆိုင်ကို ဖုန်းခေါ်ရမယ်။
404 Not Found.
ဒီစာမျက်နှာကို ယခု အသုံးပြု၍ မရသေးပါ။

ကျွန်မ လွန်ခဲ့တဲ့တစ်လလောက်က
ရှင်တို့အွန်လိုင်းဆိုင်ကနေ
အိတ်တစ်လုံး ဝယ်ခဲ့တာ
ခုထိ ရောက်မလာသေးလို့ပါ။
အားနာပါတယ်။
ကျွန်တော်တို့မှာ
အွန်လိုင်းဆိုင် မရှိပါဘူး။
တစ်ခုခု မှားနေတာ
ထင်ပါတယ်ဗျ။
ဟမ် !!!
ဆရာ!
ဟုတ်ပြီ။
ဒါက အင်တာနက်ပေါ်က
လိမ်လည်မှုတစ်မျိုးပါပဲ။
အင်တာနက်ပေါ်က လိမ်တယ်ဆိုတာ
အွန်လိုင်းဈေးရောင်းတာမျိုးကို
အယောင်ဆောင်ပြီး မင်းရဲ့
ပိုက်ဆံကို ခိုးဖို့လုပ်တာမျိုးပါပဲ။
ဒါကြောင့် Website ရဲ့ URL က မှန်ရဲ့လား နဲ့
အီးမေးလ်တွေ ပို့သူကလဲ
အမှန်အကန်လား အတုအယောင်လား ဆိုတာ
မင်းအနေနဲ့ စစ်ဆေးကို စစ်ဆေးရမယ်။
ကျွန်မ အဲ့လိုမျိုး မသိခဲ့တော့
လဲလိုက်ရတာ မတန်လိုက်တာ။
အခုကစပြီး
သေချာစစ်ဆေးပါ့မယ်။

NO.3 (အနှစ်ချုပ်) အင်တာနက်ပေါ်မှ လိမ်လည်မှု

ရှောင်ကြဉ်ရန်

- အကယ်၍ သင်သည် အွန်လိုင်းဈေးဝယ်ယူမှု (သို့) အွန်လိုင်းဘဏ်စနစ်ကို အသုံးပြုသောအခါတွင် အွန်လိုင်းလိမ်လည်မှုများနှင့် မမျှော်လင့်ဘဲ ကြုံတွေ့နိုင်ပါသည်။
- လိမ်လည်မှုများက အသုံးပြုသူများကို Phishing Site ကဲ့သို့သော ဖန်တီးထားသည့် အလိမ်အညာ Site များထံ သွားရန် ညွှန်ပြတတ်ပါသည်။
- သင်သည် Spam Mails တွင် ပါဝင်သော Attached Files (သို့) အတုအယောင် Site များကို ဖွင့်ကြည့်မိသောအခါတွင် ဗိုင်းရပ်စ်များ ကူးစက်ခြင်း (သို့) အတုအယောင် Site များထံ မှားယွင်းလွှဲပြောင်းမိခြင်းများ ဖြစ်နိုင်ပါသည်။



ဆောင်ရွက်ရန်

- Website URL များ၏ မှန်ကန်မှု (သို့) အီးမေးလ်ကို ပေးပို့သူ မှန်ကန်မှု ရှိ - မရှိကို သေချာစွာ စစ်ဆေးပါ။
- နားလည်ရန် ခက်ခဲသော စကားလုံးများဖြင့် ရေးသားထားသည့် သံသယဖြစ်ဖွယ် Website များနှင့် ဆက်သွယ်ရန် အချက်အလက်များ မပါရှိသော Website များကို မကြည့်သင့်ပေ။

သိမှတ်စရာ အတိုအထွာ

- တရားဝင်ဘဏ် Website များကို တုပထားသော Phishing Site များအား သတိထားရမည်ဖြစ်သည်။ ၎င်း Website များသည် ယခုအချိန်တွင် များပြားလာကာ သင့် Online Banking Account ၏ ID နှင့် Password များကို ခိုးယူ၍ သင့်ပိုက်ဆံကို ရယူခြင်းမျိုး ပြုလုပ်နိုင်ပါသည်။

SNS အသုံးပြုရန် လမ်းညွှန်

SNS - လူမှုကွန်ရက်ဝန်ဆောင်မှု

အပိုင်း၄

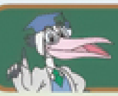
ဒီနေရာမှာ တွေ့ဖို့ ဘာလို့များ သူ ချိန်းတာပါလိမ့်။
ဒီနားမှာ လူလဲ ရှိပုံမပေါ်ဘူး။
TAP
ဟုတ်
ဟဲလို
အိုး
မင်းပိုက်ဆံတွေ ငါတို့ကို ပေးစမ်း!
အိုး ... မဟုတ်ဘူး!

သူတို့ ငှိုက်ဆဲတွေ အကုန်ပျသွားပြီ။
ဒီနေ့ အဲ့ပလတ်စတစ်ရုပ်ကိုလဲ
ကြည့်ချင်စိတ် မရှိတော့ပါဘူး။
စိတ်ပျက်ဖို့ကောင်းလိုက်တာ
ဒီနေ့အတွက် ချိန်းထားတာကို ဖျက်ရတော့မှာပေါ့။
ဘာလဲ ... ဘာလို့ သူက ထွက်သွားရတာလဲ?
ဒါဆို မနက်ဖြန်တွေ့ကြတာပေါ့။
အိုကေ တွေ့ကြတာပေါ့
Rabbit Taro ထွက်သွားပြီ
အိုး ... မင်းချောက်ချခံရတာကို မင်း မသိဘူးလား?
ချောက်ချခံရတယ်?
SNS ပေါ်မှာ ကိုယ်ရေးအချက်အလက်တွေ ခိုးယူဖို့က အရမ်းလွယ်တယ်။
မင်းရဲ့ကိုယ်ရေးအချက်အလက်တွေ ခိုးယူခံရတာနဲ့ ရာဇဝတ်မှုထဲမှာ မင်းကိုယ်တိုင် ပါသွားပြီပဲ။
ဒါကြောင့် မသိတဲ့သူတွေနဲ့ အဆက်အသွယ်မလုပ်သင့်ဘူး။ တကယ့်လက်တွေ့ဘဝမှာလဲ အဲ့လိုမသိတဲ့သူနဲ့ ဆုံဖို့ကို မလိုဘူး။
ကျွန်တော် တော်တော် တုံးတာပဲ။ အခုကစပြီး SNS ကို သတိထားပြီး သုံးပါ့မယ်။

NO.4 (အနှစ်ချုပ်) အင်တာနက်ပေါ်မှ လိမ်လည်မှု

ရှောင်ကြဉ်ရန်

- ရည်ရွယ်ချက်ရှိရှိ အန္တရာယ်ပေးနိုင်သောသူများသည် ဆွဲဆောင်မှုရှိသော သူများ၏ ဓါတ်ပုံများကိုအသုံးပြုပြီး အယောင်ဆောင်ကာ သင့်ထံ ဆက်သွယ်မှုပြုလုပ်နိုင်ပါသည်။
- ထို့နောက် ထိုသူများသည် သင့်အား တိုက်ရိုက်တွေ့ဆုံရန် တောင်းဆိုကာ သင့်အား ရာဇဝတ်မှု ဖြစ်ပေါ်စေပါသည်။
- အဆိုးရွားဆုံးအခြေအနေမှာ ပြန်ပေးဆွဲမှု၊ လူကုန်ကူးမှု စသည့် ရာဇဝတ်မှုများတွင် သင့်အား ပါဝင်ပတ်သက်စေခြင်းပင် ဖြစ်ပါသည်။



ဆောင်ရွက်ရန်

- မသိသောသူများနှင့် ဆက်သွယ်ခြင်း မပြုပါနှင့်။
- အကယ်၍ မသိသောသူများက တောင်းဆိုလာခဲ့ပင်လျှင် တိုက်ရိုက်တွေ့ဆုံခြင်း မပြုပါနှင့်။

သိမှတ်ဖွယ်ရာ အတိုအထွာ

- တစ်ခါတစ်ရံတွင် သူစိမ်းများက သင့်ကို ရာဇဝတ်မှုများတွင် ပါဝင်ရန် ဆက်သွယ်တတ်ပါသည်။
- သင်၏နာမည်၊ ဓါတ်ပုံ၊ ဖုန်းနံပါတ်၊ လိပ်စာ အစရှိသည့် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို မသိသည့် သူစိမ်းများထံ မပေးပါနှင့်။
- တစ်ခါတစ်ရံတွင် အန္တရာယ်ပေးနိုင်သူများသည် သင့်သူငယ်ချင်း အယောင်ဆောင်ကာ သင့်ထံ ဆက်သွယ်လာတတ်ပါသည်။ ထို့ကြောင့် သင့်သူငယ်ချင်းဟုတ် - မဟုတ်ကို သေချာအောင် ပြုလုပ်သင့်ပါသည်။

အင်တာနက်ပေါ်မှာ အခက်အခဲ အန္တရာယ်တွေ အများကြီးရှိပါတယ်။
ဒါပေမယ့် အင်တာနက်ကို ကောင်းကောင်းအသုံးချနိုင်မယ်ဆိုရင် တစ်ကမ္ဘာလုံးမှာ ရှိတဲ့သူတွေနဲ့ အချိန် နေရာမရွေး ကျွန်ုပ်တို့ ဆက်သွယ်လို့ရနိုင်ပါတယ်။
ဆိုက်ဘာလုံခြုံရေး လမ်းညွှန်ချက်များအတိုင်း အင်တာနက်ကို ကောင်းမွန်စွာ အသုံးပြုကြပါစို့။

သိရှိသတိပြုစေရန်၊ လုံခြုံမှုရှိစေရန် နှင့် နိုးနိုးကြားကြားရှိစေရန်

知る　守る　続ける

ASEAN · JAPAN
Information Security Awareness