

အွန်လိုင်းပေါ်တွင်တွင် ဘေးကင်းစွာနေခြင်း

ဆိုင်ဘာလုံခြုံရေးသည် ကျွန်ုပ်အတွက် အဘယ်ကြောင့် အရေးကြီးပါသနည်း?

အင်တာနက်နှင့် ဆိုရှယ်မီဒီယာများသည် ကျွန်ုပ်တို့အား သတင်းအချက်အလက်များမျှဝေရန်နှင့် သူငယ်ချင်းများ၊ မိသားစုများနှင့် အဆက်အသွယ်မပြတ်စေရန် ကူညီပေးသည့် အံ့ဩဖွယ်ပလက်ဖောင်းများဖြစ်သည်။

သို့ပေမယ့်လဲ ရာဇဝတ်ကောင်များနှင့် အခြားတရားမဝင်အဖွဲ့အစည်းများသည်လည်း သင့်ငွေ၊ သင့်အချက်အလက်များကို ရယူရန်ကြိုးစားခြင်း သို့မဟုတ် သင့်အား ခြိမ်းခြောက်ရန်ကြိုးစားခြင်း တို့အတွက် ၎င်းတို့ကို အသုံးပြုပါသည်။

၎င်းတို့သည် ကမ္ဘာပေါ်ရှိ မည်သည့်နေရာမှမဆို လည်ပတ်နိုင်ပြီး ဘာသာစကားအများစုကို ကျွမ်းကျင်စွာပြောနိုင်ပြီး ယုံကြည်စိတ်ချရသော ဝတ်ဆိုင်အတုများကို ဖန်တီးနိုင်သည်။ ၎င်းတို့သည် သင့်အား အီးမေးလ်၊ ဆိုရှယ်မီဒီယာနှင့် စာသားမက်ဆေ့ချ်မှတစ်ဆင့် ဆက်သွယ်မည်ဖြစ်ပြီး ၎င်းတို့သည် သင့်အား ကြောက်ရွံ့မှု သို့မဟုတ် စိုးရိမ်ပူပန်မှုဖြစ်စေရန် ကြိုးစားမည်ဖြစ်သောကြောင့် သင်ရှင်းရှင်းလင်းလင်း မတွေးတောနိုင်ပါ။

ထိုအရာအားလုံးကို သင်ပြင်ဆင်ထားရန်လိုအပ်ပြီး သူတို့အသုံးပြုသော လှည့်ကွက်များကို အမြဲသတိထားပါ။

အွန်လိုင်းမှာ ကြုံတွေ့ရတတ်တဲ့ ပြဿနာတချို့က ဘာတွေလဲ။

ဖော်ပြပါတို့သည် ကျွန်ုပ်တို့မြင်နေရသည့် အဖြစ်အများဆုံး အခြေအနေများဖြစ်သည်။

- လင့်ခ်တစ်ခုကို နှိပ်ရန် သင့်အား သံသယဖြစ်ဖွယ် အီးမေးလ် သို့မဟုတ် စာသားမက်ဆေ့ချ်တစ်ခု ရရှိသည်။
 - အဆိုပါလင့်ခ်များသည် သင်၏ login လော့ကင်အချက်အလက်များ သို့မဟုတ် ငွေကြေးအသေးစိတ်အချက်အလက်များကို ခိုးယူရန် ဒီဇိုင်းထုတ်ထားသည့် ဝတ်ဆိုင်အတုများဆီသို့ ဦးတည်သွားလေ့ရှိသည်။
- သင့်ထံသို့ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို တောင်းသော သံသယဖြစ်ဖွယ် ဖုန်းခေါ်ဆိုမှုတစ်ခု ဝင်လာသည်။
 - အထက်ဖော်ပြပါအတိုင်း ဖုန်းခေါ်ဆိုသူသည် သင့်ဘဏ်ဟု ဟန်ဆောင်ကာ အချက်အလက်တောင်းပါမည်။
- အခွင့်အာဏာပိုင် တစ်ဦးကဲ့သို့ ဟန်ဆောင်ပြီး တစ်ခုခုလုပ်ခိုင်းရန် ကြိုးစားနေသူတစ်ယောက်ဆီက ဆက်သွယ်မှုကို ရရှိပါသည်။
 - မကြာခဏဆိုသလို ထိုလူက သင့်ကိုတစ်နည်းနည်းဖြင့် ခြိမ်းခြောက်တတ်သည်။
- တစ်စုံတစ်ယောက်သည် သင့်အွန်လိုင်းအကောင့်တစ်ခု သို့မဟုတ် တစ်ခုထက်ပိုသောအကောင့်ထံသို့ ဝင်ရောက်သွားသည် (ဥပမာ- အီးမေးလ် သို့မဟုတ် ဆိုရှယ်မီဒီယာ)။

- တစ်စုံတစ်ယောက်သည် သင့်အွန်လိုင်းအကောင့်ထဲသို့ ဝင်ရောက်လာပါက ၎င်းတို့သည် အချက်အလက်များကို ခိုးယူခြင်း၊ ငွေပေးချေမှုများ ပြန်လည်ညွှန်းပေးခြင်း၊ သင့်အဖြစ်ယောင်ဆောင်ပြီး သင့်သူငယ်ချင်းများ သို့မဟုတ် မိသားစုဝင်များကို ပစ်မှတ်ထားခြင်း ပြုလုပ်လာနိုင်သည်။
- သင့်ခရက်ဒစ်ကတ်အသေးစိတ်အချက်အလက်များကို ခိုးယူခံရခြင်း သို့မဟုတ် အတုပြုလုပ်ရောင်းချခြင်း သို့မဟုတ် ရင်းနှီးမြှုပ်နှံမှုတစ်ခုတွင် သင့်အား ငွေအလွဲသုံးစားလုပ်ခြင်းခံရသည်။
 - လိမ်လည်လှည့်ဖြားသူများသည် သင့်အနေဖြင့် အလွန်ကောင်းသောရင်းနှီးမြှုပ်နှံမှုဟုထင်စေပြီး မတွေးဘဲချက်ချင်းဆုံးဖြတ်ချက်ချပြုလုပ်ရန်ရည်ရွယ်သည်။ သို့မဟုတ် စစ်မှန်သော ဝတ်ဆိုင်တစ်ခုမှ ဒေတာဖောက်ထွင်းခိုးယူခံရသောကြောင့် သင်၏အသေးစိတ်အချက်အလက်များသည် အွန်လိုင်းပေါ်တွင် ပေါက်ကြားသွားနိုင်သည်။

ဤနေရာတွင် နောက်ထပ် ဥပမာများ ရှိပါသည်-
[အခုဘဲ အကူအညီယူပါ - သင့်အွန်လိုင်းလုံခြုံမှုကို ထိန်းချုပ်ပါ](#)

အွန်လိုင်းမှာ ဘယ်လိုလုံခြုံအောင်နေရမလဲ။

- ရှည်လျားပြီး ထူးခြားသော စကားဝှက်များ passwords သုံးပါ။**
 - စကားဝှက်ရှည်လေး password၊ ပိုအားကောင်းလေဖြစ်သည်။
 - ကျပန်းစကားလုံးလေးလုံး ပေါင်းပြီး (ဥပမာ- TriangleRhinoOperationShoes) နှင့် လိုအပ်ပါက နံပါတ်များ၊ စာလုံးကြီးများနှင့် သင်္ကေတများ ပေါင်းထည့်ခြင်းဖြင့် စာလုံး 16 လုံးထက်မမေ့နိုင်သော စကားဝှက်တစ်ခု passwordကို ဖန်တီးပါ (ဥပမာ- Triangle&"Rhino"Operation2Shoes)။
 - အရေးကြီးတာက တူညီတဲ့စကားဝှက် password တွေကို နေရာတိုင်းတွင် ထပ်ခါတလဲလဲ မသုံးပါနဲ့။ ဒုစရိုက်သမားတစ်ဦးသည် သင့်စကားဝှက် password များထဲမှ တစ်ခုကို ရရှိပါက ၎င်းကို အခြားအကောင့်များတွင် စမ်းကြည့်မည်ဖြစ်သည်။
 - သင့်အတွက် စကားဝှက်များ password ကို သိမ်းထားရန်နှင့် စကားဝှက် password အသစ်များ ဖန်တီးရန် password manager ကို အသုံးပြုပါ။
 - [စကားဝှက်ကောင်း password များ ဖန်တီးပါ - သင့်အွန်လိုင်းလုံခြုံမှုကို ထိန်းချုပ်ပါ](#)
- နှစ်ဆင့်ခံ ဝင်ရောက်နည်း (two-factor authentication) ကိုသုံးပါ။**
 - ဤသည်မှာ ဝတ်ဆိုင်တစ်ခုသို့ သင်ဝင်ရောက်ရန်လိုအပ်သည့် နောက်ထပ် အချက်အလက်များဖြစ်သည် - များသောအားဖြင့် သင့်ဖုန်းကို ကုဒ်တစ်ခုပို့တတ်ပါသည်။
 - ဤနည်းပညာသည် အလွန်အားကောင်းပြီး သင့်အကောင့်ထဲသို့ သင်မသိပဲဝင်ရောက်ရန် ကြိုးစားမှုများကို ရပ်တန့်နိုင်သည်။
 - စစ်ဆေးအတည်ပြုသည့် အပ် 'authenticator app' ကို သုံးရန် တိုက်တွန်းပါသည်။
 - [နှစ်ဆင့်ခံ ဝင်ရောက်နည်း \(2FA\) ကိုသုံးပါ - သင့်အွန်လိုင်းလုံခြုံမှုကို ထိန်းချုပ်ပါ](#)

- **အွန်လိုင်းတွင် ကိုယ်ရေးအချက်အလက် မကျိုးပေါက်အောင်နေပါ။**

- ဆိုရှယ်မီဒီယာတွင် လုံခြုံစွာနေရန် အကောင်းဆုံးရွေးချယ်မှုမှာ သင်၏ ကိုယ်ရေးကိုယ်တာဆက်တင်များ (privacy settings) ကို ဖွင့်ထားခြင်းဖြစ်သည်။
- ၎င်းသည် ဆိုက်ဘာဒုစရိုက်သမားများ အပါအဝင် ကြိုရာလူများက သင့်ပို့စ်များကို မြင်နိုင်ခြင်း သို့မဟုတ် သင့်ထံ စာတိုပေးပို့ခြင်းကို ရပ်တန့်စေမည်ဖြစ်သည်။
- သင်ကိုယ်တိုင်၊ သင့်မိသားစု သို့မဟုတ် သင့်သူငယ်ချင်းများအကြောင်း ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို ဂရုတစိုက်တင်ပါ။
- သင်ဆက်သွယ်သောသူများသည် တခြားသူတစ်ယောက်မဟုတ်ဘဲ အစစ်အမှန်ဖြစ်ကြောင်း သေချာပါစေ။
- friend requests အတုများကို သတိထားပါ။ မိမိကိုယ်ကို စာနယ်ဇင်းသမားများဟု ပြောဆိုသူများ သို့မဟုတ် သင်ကောင်းစွာမသိသော သူများကို သတိထားပါ။
- [အွန်လိုင်းတွင် ကိုယ်ရေးအချက်အလက် မကျိုးပေါက်အောင်နေပါ - သင့်အွန်လိုင်းလုံခြုံမှုကို ထိန်းချုပ်ပါ](#)

- **အရာတိုင်း အပ်ဒိတ် update ဖြစ်နေပါစေ။**

- သင့်ဖုန်း၊ ကွန်ပျူတာ သို့မဟုတ် ဆော့ဖ်ဝဲလ်ကို အပ်ဒိတ် update လုပ်သောအခါတွင် ၎င်းသည် လုံခြုံရေးဟာကွက်များကို ပိတ်ပေးပါသည်။
- ဒုစရိုက်သမားများသည် ဝင်ရောက်ရန် နည်းလမ်းများကို အမြဲရှာဖွေနေပြီး ထို update အပ်ဒိတ်များက အားနည်းချက်များကို ပြုပြင်မွမ်းမံကာကွယ်မှုများ ပြုလုပ်ပေးသည်။
- သင့်စက်များကို ပုံမှန် ရီစတင် (restart) ပြုလုပ်ပါ။
- [အရာတိုင်း အပ်ဒိတ် updates ဖြစ်နေပါစေ - သင့်အွန်လိုင်းလုံခြုံမှုကို ထိန်းချုပ်ပါ](#)

- **လိမ်လည်မှုများကို သတိထားပါ။**

- အကောင်းဆုံးအကြံပြုချက်မှာ ဤလိမ်လည်လှည့်ဖြားမှုများကို သတိထားရန်နှင့် ၎င်းတို့ကိုနားစွင့်သိရှိနေရန်ဖြစ်သည်။
- တစ်ခုခုမှားယွင်းနေပုံ သံသယရှိပုံပေါက်ပါက သင့်ကို ဆက်သွယ်လာသူနှင့် ဆက်သွယ်မှု ရပ်လိုက်ပါ။ အထူးသဖြင့် ထိုသူများမှ ငွေတောင်းလာပါက ခင်မင်ရပုံပေါက်သည့်တိုင် သတိထားပါ။
- ထူးဆန်းသောလင့်ခ်များနှင့် အီးမေးလ်လိပ်စာများကို သတိထားပါ (ဥပမာ- သင့်ဘဏ်မှ သင့်အား Gmail အကောင့်တစ်ခုမှ အီးမေးလ်တစ်စောင် ပေးပို့မည်မဟုတ်ပါ)။
- မည်သည့်အခါမျှ မက်ဆေ့ချ်ထဲမှလင့်ခ်ကို မနှိပ်ပါနှင့်။
- သင့်စက်ထဲသို့ တရားဝင်အက်ပ်စတိုးများမှ အက်ပ်များကိုသာ ဒေါင်းလုဒ်လုပ်ပါ။
- သံသယရှိပါက၊ သင့်ထံဆက်သွယ်ထားသော အဖွဲ့အစည်းကို တိုက်ရိုက်ဆက်သွယ်ပါ။ သင့်ထံပို့ထားသော လင့်ခ်များ မနှိပ်ပါနှင့် သို့မဟုတ် ဖုန်းနံပါတ်များကို မခေါ်ပါနှင့်။

- သင်ကိုယ်တိုင်၊ သင့်အသိုင်းအဝိုင်းနှင့် သင်ဝင်ရောက်ထားသည့် မည်သည့်အဖွဲ့အတွက် အွန်လိုင်းလုံခြုံရေးအန္တရာယ်များကို သတိထားနေရန် ကြိုးစားပါ။
- **သင်၏အချက်အလက်များကိုကာကွယ်ပါ။**
 - Signal ကဲ့သို့သော encrypted messaging apps ကို အသုံးပြုပါ။ ထိုသို့ဖြင့် သင့်မက်ဆေ့ချ်များကို မည်သူမျှ ကြားဖြတ်မဖတ်နိုင်တော့ပါ။
 - HTTPS ဖြင့် စတင်သည့် ဝဘ်ဆိုက်နှင့်သာ သင်၏အချက်အလက်များကိုမျှဝေပါ။ S သည် “secure (လုံခြုံမှု)” ကို ကိုယ်စားပြုပြီး သင်နှင့် ဝဘ်ဆိုက်အကြား ပေးပို့သည့် အချက်အလက်မှန်သမျှကို ကုဒ်ဝှက် encrypted ထားသည်။
 - သင့်ဒေတာ data ကို ကာကွယ်ပြီး သင့်တည်နေရာကို ဝှက်ထားနိုင်သည့် virtual private network (VPN) ကို အသုံးပြုရန် စဉ်းစားပါ။
 - သင့်အက်ပ်စ် apps များတွင် သင်၏ ဒေတာ data ကို သင်၏ခွင့်ပြုချက်အရ မည်သို့မျှဝေအသုံးပြုခွင့်ရှိသည်ကို စစ်ဆေးပါ။ ဥပမာအားဖြင့်၊ ကြံ့ခိုင်ရေး (Fitness) အက်ပ်စ်သည် သင့်အဆက်အသွယ်များ contacts ကို အသုံးပြုခွင့် မလိုအပ်ပါ။

အလိမ်ခံရလျှင် သို့မဟုတ် ပိုဆိုးလျှင် မည်သို့ပြုလုပ်မည်နည်း။

အကူအညီတောင်းလိုရသော နေရာအများအပြားရှိပါသည်။ သင်ခွင့်ပြုချက်မပေးပါက ဤအဖွဲ့အစည်းများသည် သင့်အသေးစိတ်အချက်အလက်များကို အခြားမည်သူ့ကိုမျှ မျှဝေမည်မဟုတ်ပါ။

- သင်သည် CERT NZ portal ပေါ်တယ်မှတစ်ဆင့် NCSC သို့ ဆိုက်ဘာဖြစ်ရပ်များကို သတင်းပို့နိုင်သည်။ ကျွန်ုပ်တို့သည် သင့်အား အခြားအေဂျင်စီနှင့် ဆက်သွယ်နိုင်ပေးသည်- [Report an incident | CERT NZ](#)
- ငွေကြေးဆုံးရှုံးမှု ဖြစ်ပါက သင့်ဘဏ်ကို ချက်ချင်းဆက်သွယ်သင့်သည်။
- ပြည်ထဲရေးဌာန (Department of Internal Affairs) မှ ဆောင်ရွက်သည့် ဝန်ဆောင်မှုတစ်ခုဖြစ်သည့် 7726 သို့ သင့်ထံပေးပို့သောလိမ်လည်စာတိုများ အခမဲ့ပေးပို့နိုင်သည်။