**သင့်အဖွဲ့အစည်းကို အွန်လိုင်းတွင် လုံခြုံအောင်ထားပါ**

**လူမှုအသိုင်းအဝန်းများနှင့် အဖွဲ့အစည်းများအတွက် ဆိုက်ဘာလုံခြုံရေးသည် အဘယ်ကြောင့်အရေးကြီးသနည်း။**

ဤစာမျက်နှာတွင် သင့်အသိုင်းအဝိုင်းအဖွဲ့ သို့မဟုတ် အဖွဲ့အစည်းကို ဆိုက်ဘာလုံခြုံရေးခြိမ်းခြောက်မှုများမှ ကာကွယ်ရန် သင်လုပ်ဆောင်နိုင်သော အကြံဉာဏ်များနှင့် အဆင့်အချို့ ကိုဖော်ပြပေးထားသည်။ တစ်ဦးချင်းအတွက် သီးခြားလမ်းညွှန်တစ်ခုလည်း ရှိပါသည်။

ဤအကြံပြုချက်သည် အဖြစ်အများဆုံးနှင့် ပြင်းထန်သော ခြိမ်းခြောက်မှုများအပေါ် အခြေခံထားသည်။

* အပ်ဒိတ်များ Updates – လုံခြုံရေးဆိုင်ရာ အပေါက်များကို ဖာထေးရန် သင့်စက်ပစ္စည်းများတွင် ဆော့ဖ်ဝဲကို ခေတ်မီအောင် အပ်ဒိတ် update လုပ်ထားပါ။
  + သင့်အသိုင်းအဝိုင်းအဖွဲ့ သို့မဟုတ် အဖွဲ့အစည်း၏စက်ပစ္စည်းများကို အပ်ဒိတ် Update လုပ်ထားပါ။ ၎င်းတွင် ဖုန်းများ၊ ကွန်ပျူတာများ၊ WiFi router များနှင့် စမတ်ကိရိယာများအပါအဝင် အင်တာနက်သို့ ချိတ်ဆက်နိုင်သည့် အခြားအရာများ ပါဝင်သည်။
  + ဖြစ်နိုင်လျှင် စက်ပစ္စည်းများကို အလိုအလျောက်အပ်ဒိတ် automatic update လုပ်ခွင့်ပေးထားပါ။
* နှစ်ဆင့်ခံ ဝင်ရောက်ခြင်း (Two-factor authentication (2FA) – အကောင့်ထဲဝင်ရန် password အပြင် နောက်ထပ်အဆင့်တစ်ဆင့် လိုအပ်ခြင်းဖြင့် သင့်အကောင့်များတွင် လုံခြုံရေးကို အပိုထပ်ဆောင်းပေးပါသည်။ ထိုအဆင့်မှာ သင့်ဖုန်းရှိ အက်ပ် app တစ်ခုမှ ပေးသောကုပ် code ကို ထပ်ထည့်ရခြင်းဖြစ်နိုင်သည်။
  + မှတ်ချက်- ၎င်းကို multi-factor authentication (MFA)၊ နှစ်ဆင့်အတည်ပြုခြင်း (2SV) နှင့် အခြားအမည်များစွာ ဟုခေါ်သည်။
  + သင့်အသိုင်းအဝိုင်းအဖွဲ့ သို့မဟုတ် အဖွဲ့အစည်း၏အကောင့်များအားလုံးတွင် 2FA ကိုဖွင့်ပါ။
  + ဖြစ်နိုင်ပါက၊ လှည့်ဖျားမခံရနိုင်သော 2FA ပုံစံကို အသုံးပြုကြည့်ပါ၊ ဆိုလိုသည်မှာ ၎င်းကုဒ်များကို လှည့်စား၍ သင့်အားလွှဲပေးရန် မရပါ။ ၎င်းသည် လုံခြုံရေးကီး စက်ကရိယာ security key သို့မဟုတ် လက်ဗွေ သို့မဟုတ် မျက်နှာ ID ကဲ့သို့သော အရာတစ်ခု ဖြစ်နိုင်သည်။
* သင့်အွန်လိုင်းအကောင့်များကို သေချာစိစစ်မှတ်တမ်းတင်ထားပါ – အသိုင်းအဝိုင်းအဖွဲ့ သို့မဟုတ် အဖွဲ့အစည်းမှ ထွက်ခွာပြီးနောက် အဖွဲ့ဝင်ဟောင်းများသည် ၎င်းတို့၏ အကောင့်များသို့ ဝင်ရောက်နိုင်ခွင့်မရှိအောင် သေချာပြုလုပ်ပါ။
  + သင့်တွင် အကောင့်တစ်ခုတည်းကို ဝင်ရောက်အသုံးပြုသူ တစ်ဦးထက်ပိုပါက၊ ၎င်းတို့အားလုံးတွင် မတူညီသော လော့ဂ်အင် logins များ သေချာရှိစေပြီး အားလုံးတွင် 2FA ကို ဖွင့်ထားသည်။
  + အသုံးပြုသူအကောင့်အားလုံး၏စာရင်းကို သိမ်းဆည်းထားပြီး ဝန်ထမ်းများထွက်ခွာသွားသည့်အခါကဲ့သို့သော မလိုအပ်သည့်အရာများကို ပိတ်လိုက်ပါ။
  + သင့်အဖွဲ့ဝင်များထံ သင်ပေးခဲ့သည့် စက်ပစ္စည်းမှတ်တမ်းကို သိမ်းဆည်းထားပါ၊ ဝန်ထမ်းများထွက်ခွာသွားသည့်အခါ စက်ပစ္စည်းများကို ပြန်လည်ရယူရန်နှင့် ထိုစက်ပစ္စည်းများ ကို factory reset ပြုလုပ်ရန်သတိရပါ။ အဆောက်အဦးကို ဝင်ခွင့်အတွက်အသုံးပြုသောကုန် codes များကို ပြောင်းလဲရန် လိုအပ်သည်။
* သင့်အွန်လိုင်းအကောင့်များသို့ ဝင်ရောက်ခွင့်ရှိသူကို စစ်ဆေးပါ – သင့်အသိုင်းအဝိုင်းအဖွဲ့ သို့မဟုတ် အဖွဲ့အစည်းရှိလူများသည် ၎င်းတို့လိုအပ်သောအရာများကိုသာ ဝင်ရောက်ခွင့်ရှိသင့်သည်။
  + အကယ်၍ လူတစ်ဦး၏အကောင့်သည် ‘ဟက်ကာ’ ‘hacked’ ခံရပါက၊ ဤအဆင့်များသည် တိုက်ခိုက်သူလုပ်ဆောင်နိုင်သည့် အန္တရာယ်ကို ကန့်သတ်ထားသည်။
  + မလိုအပ်သော ခွင့်ပြုချက်များ (permissions) ကို ပုံမှန်စစ်ဆေးပြီး ဖယ်ရှားပါ။
  + သင့်တွင် “admin” အကောင့်တစ်ခုကို လူများစွာအသုံးပြုလျှင် ပုံမှန်မဟုတ်သော လုပ်ဆောင်ချက်မြင်တွေ့လျှင် ၎င်းကို စောင့်ကြည့်ပါ။ အထူးသဖြင့် နေ့စဉ်လုပ်ငန်းဆောင်တာများအတွက် ဤအကောင့်မျိုးရှိခြင်းကို ကန့်သတ်ရန်ကြိုးစားပါ။
  + ဤစည်းမျဉ်းများသည် router များကဲ့သို့သော စက်ပစ္စည်းများသို့ admin အကောင်သုံး၍ ဝင်ရောက်ခွင့်ကိုလည်း ကန့်သတ်မှုရှိရမည်။
* ဝန်ဆောင်မှုပေးသူများနှင့် သင့်စာချုပ်များကို ပြန်လည်သုံးသပ်ပါ – သင့်အတွက် IT ဝန်ဆောင်မှုများကို လုပ်ဆောင်ရန် တစ်ယောက်ယောက်၊ တစ်ဖွဲ့ဖွဲ့ ကို ငှားရမ်းထားလျှင်။
  + သင့်အသိုင်းအဝိုင်းအဖွဲ့ သို့မဟုတ် အဖွဲ့အစည်း၏ ဆိုက်ဘာလုံခြုံရေးလိုအပ်ချက်အရ ၎င်းတို့တွင် ဆိုက်ဘာလုံခြုံရေးအကာအကွယ်များ ရှိနေကြောင်း သေချာပါစေ။
* သင့်အကောင့်များနှင့် စနစ်များအားလုံး အတူတကွအလုပ်လုပ်ပုံကို သိပါ – ချိတ်ဆက်မှုများကို နားလည်ခြင်းက တိုက်ခိုက်သူသည် မည်သည့်နေရာမှ ဝင်ရောက်နိုင်ခဲ့သည်ကို သိရန် ကူညီပေးသည်။
  + ဥပမာ၊ အီးမေးလ်၊ cloud storage နှင့် အကောင့်ပလက်ဖောင်းများကြားရှိ ချိတ်ဆက်မှုများကို ပြန်လည်သုံးသပ်ပါ။
  + အွန်လိုင်းဘေးကင်းမှုပိုကောင်းမွန်ရန်အတွက် Virtual Private Network (VPN) ကို အသုံးပြုရန် စဉ်းစားပါ။ VPN ကိုအသုံးပြုခြင်းသည် သင့်အွန်လိုင်းလုပ်ဆောင်ချက်ကို ခြေရာခံရန်ကြိုးစားသူမည်သူမဆိုထံမှ ဖုံးကွယ်ကာကွယ်ထားသည်။ သင့်အသိုင်းအဝိုင်းအဖွဲ့ သို့မဟုတ် အဖွဲ့အစည်း၏အဖွဲ့ဝင်များ အဝေးမှချိတ်ဆက်အလုပ်လုပ်ပါက အထူးသဖြင့် ကောင်းမွန်ပါသည်။
* သင့်လူများကို ‘ဆိုက်ဘာကို စနစ်တကျ သုံးတတ်ရန်’ စီစ်ပါ။ — သင့်အသိုင်းအဝိုင်းအဖွဲ့ သို့မဟုတ် အဖွဲ့အစည်းရှိလူများသည် သင့်ရုံးရှိ systems များထက် ပစ်မှတ်ထားခံရနိုင်ခြေပိုများပါသည်။
  + ဝန်ထမ်းအားလုံးကို အခြေခံဆိုက်ဘာလုံခြုံရေးအတွက် လေ့ကျင့်ပေးပါ။ Own Your Online ဝဘ်ဆိုက် [Own Your Online | NCSC](https://www.ownyouronline.govt.nz/) တွင် သင့်ကိုယ်သင် လုံခြုံအောင်ထားပြီး အွန်လိုင်းတွင် လုံခြုံမှုရှိစေရန်နှင့် လိမ်လည်လှည့်စားမှုများကို မည်သို့ထောက်လှမ်းနိုင်စေရန် ကျယ်ပြန့်သော အကြံဉာဏ်နှင့် အကြံပြုချက်များ ရှိပါသည်။
  + ၎င်းတို့၏ ကိုယ်ရေးကိုယ်တာအကောင့်များနှင့် သင့်အဖွဲ့အစည်းအတွက် ၎င်းတို့အသုံးပြုသည့် အကောင့်များအတွက် အရေးကြီးကြောင်း သူတို့ကို သတိပေးပါ။
  + ကျွန်ုပ်တို့သည် တစ်ဦးချင်းစီအတွက် လမ်းညွှန်ချက်တစ်ခုလည်း ရှိသည်။ [LINK placeholder]
* အဖြစ်အပျက်တစ်ခုအတွက် အစီအစဥ်- အဖြစ်အပျက်ပြဿနာတစ်ခုဖြစ်ပွားသည့်အခါ လူအများကို ထိတ်လန့်မှုမဖြစ်စေရန် တုံ့ပြန်မှုအစီအစဥ်တစ်ခုထားရှိခြင်းသည် အရေးကြီးသည်။
  + အဖြစ်အပျက်တုံ့ပြန်မှု အစီအစဉ်တစ်ခုသည် အဖြစ်အပျက်တစ်ခုဖြစ်ခဲ့လျှင် မည်သူကမည်သို့အရာလုပ်ဆောင်ရမည်ကို ရှင်းရှင်းလင်းလင်းဖော်ပြသည်။ နမူနာပုံစံများကို ဤနေရာတွင် ရနိုင်ပါသည်။ [Incident Management |NCSC](https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Incident-Management-Be-Resilient-Be-Prepared.pdf)
  + ဖုန်းများ၊ ကွန်ပျူတာများ၊ သို့မဟုတ် အခြားစနစ်များ ချွတ်ယွင်းပါက လုပ်ဆောင်ရမည့် အစီအစဉ်ကို ထည့်သွင်းပါ။ ဤအစီအစဉ်ကို အမြဲတမ်းအပ်ဒိတ်လုပ်ပါ။
  + လိုအပ်သော လူတိုင်း၏ အဆက်အသွယ်အသေးစိတ်အချက်အလက်များကို သိမ်းဆည်းထားပါ။ ၎င်းတို့ကို ဆက်သွယ်ရန် အဓိကနည်းလမ်း များ ပျက်သွားပါက (အီးမေးလ်ကဲ့သို့သော) ဆက်သွယ်နိုင်သောအရန်အသေးစိတ်အချက်အလက်များကို သိမ်းဆည်းထားပါ။
  + အကယ်၍ system ထဲသင်ဝင်မရသောအခါ system အပြင်ဘက်တစ်နေရာရာတွင် ထိုအစီအစဉ် plan ကို သိမ်းထားပါ။