Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

cyber.gov.au

သင်၏ အင်တာနက်သုံး ပစ္စည်းများဆိုင်ရာ လုံခြုံရေး အတွက် အကြံပြုချက်များ

ဩစတြေးလျဆိုင်ဘာ လုံခြုံရေးစင်တာအနေဖြင့် လူမှုအသိုင်းအဝိုင်းအတွင်းမှ လူများ အင်တာနက်သုံး ပစ္စည်းများ (IoT) ကို ဝယ်ယူခြင်းနှင့် လုံခြုံဘေးကင်းစွာ အသုံးပြုနိုင်စေရန်အတွက် ရည်ရွယ်ကာ ဤအချက်အလက်ကို ထုတ်ဝေခြင်း ဖြစ်ပါသည်။ IoT ပစ္စည်းဆိုသည်မှာ အင်တာနက်ဖြင့် ချိတ်ဆက်ထားသည့် နေ့စဉ်သုံး စက်ပစ္စည်းများ ဖြစ်ပါသည်။ IoT စက်ပစ္စည်း၏ ဥပမာ များမှာ ကလေးများကို စောင့်ကြည့်နိုင်သည့် baby monitor များ၊ ဒရုန်းများ၊ လုံခြုံရေး ကင်မရာ၊ စမတ်တီဗီနှင့် ဆိုလာ အင်ဗာတာ တို့ ဖြစ်ကြပါတယ်။ နေအိမ်အတွင်း သို့မဟုတ် စီးပွားရေးလုပ်ငန်းအတွင်းမှ IoT စက်ပစ္စည်းများသည် Wi-Fi သို့မဟုတ် ဖုန်းကွန်ရက်၏ 4G သို့မဟုတ် 5G များကို အသုံးပြုကာ အင်တာနက်ဖြင့် ချိတ်ဆက်ထားလေ့ ရှိပါသည်။

ဩစတြေးလျနိုင်ငံမှ နေအိမ်များနှင့် စီးပွားရေးလုပ်ငန်းများတွင် တွေ့ရလေ့ရှိသော IoT စက်ပစ္စည်းများသည် လုံခြုံရေးကို ရှေးရှုပြီး ဖန်တီးထားခြင်း မရှိကြောင်းကို တွေ့ရှိရပါသည်။ ထို့ကြောင့် အင်တာနက်မှ တဆင့် ထိုစက်ပစ္စည်းများ၏ ပျော့ကွက် ဟာကွက် အားနည်းချက်များကြောင့် တိုက်ခိုက်ခံရမှုများ ဖြစ်စေနိုင်ပါသည်။ ထိုကဲ့သို့ တိုက်ခိုက်မှုများမှတဆင့် ဆိုင်ဘာ ရာဇဝတ်သားများကို သင်၏ စက်ပစ္စည်းအတွင်းသို့ ခွင့်ပြုချက်မပါပဲ ဝင်ရောက်စေကာ သင်၏ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို မသမာသည့် အရာများအတွက် အသုံးပြုရန် ရယူမှုများ ပြုလုပ်နိုင်ပါသည်။

IoT စက်ပစ္စည်း တစ်ခုအား မဝယ်ခင်

စက်ပစ္စည်းများကို မဝယ်ခင် စက်ပစ္စည်းအကြောင်း လေ့လာသင့်ပါသည်၊ အကြောင်းရင်းမှာ ကုန်ထုတ်လုပ်သူများသည် လုံခြုံရေးနှင့် ပတ်သက်ပြီး လုံခြုံရေးအဆင့် တူညီစွာ ထည့်သွင်းထားခြင်း မရှိသည့်အတွက် ဖြစ်ပါသည်။ စက်ပစ္စည်းတစ်ခုကို မဝယ်ခင် အခြားကုန်ထုတ်လုပ်သူများ ရောင်းချသည့် အလားတူ စက်ပစ္စည်းများဖြင့် နှိုင်းယှဉ်ကြည့်ပါ။ ထည့်သွင်းစဉ်းစားရမည့် အချက်များမှာ-

1. **ဤစက်ပစ္စည်းကို နာမည်ကောင်းရနေသည့် ကုမ္ပဏီမှ ထုတ်လုပ်ခြင်းရှိမရှိ၊ ဤပစ္စည်းကို ရောင်းချသည့် ဆိုင်မှာ နာမည်ကောင်းရသည့် ဆိုင် ဟုတ်မဟုတ် ထည့်သွင်းစဉ်းစား သင့်ပါသည်။** နာမည်ကောင်းရထားသည့် ကုမ္ပဏီများသည် စက်ပစ္စည်းများကို ထုတ်လုပ်ရာတွင် လုံခြုံရေးကို ထည့်သွင်းစဉ်းစားပြီးမှ ထုတ်လုပ်နိုင်ခြေ များပါသည်။ နာမည်ကောင်းရသည့် ဆိုင်များသည် နာမည်ကောင်းရထားသည့် ကုမ္ပဏီများထုတ်လုပ်ထားသည့် စက်ပစ္စည်းများကို ရောင်းချလေ့ရှိပြီး ကုန်ထုတ်လုပ်သူများ ရည်ရွယ်သည့်အတိုင်း သင့်ဆီ စက်ပစ္စည်းရောင်းချနိုင်ရန်အတွက် ၎င်းတို့၏ ဈေးကွက် ချိတ်ဆက်မှုကို ကန့်သတ်ထားလေ့ရှိပါသည်။

2. **လျှို့ဝှက်အချက်အလက်ကုဒ်ကို ပြောင်းလဲရန် ဖြစ်နိုင်ပါသလား။** လျှို့ဝှက်အချက်အလက်ကုဒ်ကို ပြောင်းလဲမှုလုပ်ခြင်းသည် အမြဲတမ်းကောင်းမွန်သင့်တော်ပါသည်။ အကယ်၍ ထိုစက်ပစ္စည်းသည် အားနည်းသည့် လျှို့ဝှက်ကုဒ်များဖြင့် ရောက်ရှိလာပါက လျှို့ဝှက်ကုဒ်ကို ပြောင်းရန် ပို၍ အရေးကြီးပါသည်။ လုံခြုံရေး ကောင်းမွန်သည့် စက်ပစ္စည်းတွင် တမူထူခြားကာ ခန့်မှန်းရခက်ပြီး ရှုပ်ထွေးကာ ခန့်မှန်းရန် မဖြစ်နိုင်သည့် လျှို့ဝှက်ကုဒ်များ ရှိသင့်ပါသည်၊ အကြောင်းရင်းမှာ အားနည်းသည့် လျှို့ဝှက်ကုဒ်ဖြင့် တည်ဆောက်ထားသည့် စက်ပစ္စည်းများသည် တိုက်ခိုက်ရန် လွယ်ကူစေသည့်အတွက် ဖြစ်ပါသည်။

3. **ကုန်ထုတ်လုပ်သူဖက်မှ update များ ပေးပါသလား။** ကုမ္ပဏီများအနေဖြင့် ၎င်းတို့ ထုတ်လုပ်သည့် စက်ပစ္စည်းများတွင် အားနည်းချက်များ ရှိကြောင်း တွေ့ရှိသည့်အခါ ပြုပြင်မွမ်းမံမှုများ ပြုလုပ်ရန် အရေးကြီးပါသည်။ ဥပမာ၊ စက်ပစ္စည်း၏ ဆော့ဖ်ဝဲတွင် အားနည်းချက်ရှိကြောင်း သိရသည့်အခါ သို့မဟုတ် ဟက်ကာများအနေဖြင့် သင်၏ စက်ပစ္စည်းကို တိုက်ခိုက်နိုင်သည့် နည်းလမ်းများကို သိရှိသွားသည့်အခါတွင် ပြုပြင်မွမ်းမံမှု ပြုလုပ်ရန်အတွက် update များ လိုအပ်ပါသည်။

4. **မည်သည့် ဒေတာ အချက်အလက်များကို စက်ပစ္စည်းမှ စုဆောင်းကာ မည်သူများနှင့် ထိုအချက်အလက်များကို မျှဝေမှု လုပ်မည်နည်း။** မည်သည့် ဒေတာ အချက်အလက်များကို စုဆောင်းပြီး ထိုအချက်အလက်များကို မည်ကဲ့သို့ အသုံးပြုမည် ဆိုသည့် အကြောင်းအရာများကို ကုန်ထုတ်လုပ်သူများအနေဖြင့်၎င်းတို့၏ ဝဘ်ဆိုက် သို့မဟုတ် ကိုယ်ရေးကိုယ်တာဆိုင်ရာ မူဝါဒ privacy policy တွင် ဖော်ပြမှု လုပ်သင့်ပါသည်။ အွန်လိုင်း သို့မဟုတ် မိုဘိုင်း အက်ပလီကေးရှင်းများ စုဆောင်းထားသည့် အချက်အလက်များနှင့် ပတ်သက်ပြီး အမြဲတမ်း ထည့်သွင်းစဉ်းစားမှုများ လုပ်ရန် အရေးကြီးပါသည်။

5. **မိမိလိုချင်သည့် ပုံစံအတိုင်း ထိုစက်ပစ္စည်းများက လုပ်ဆောင်ပါသလား။** သင်လိုအပ်သည့်အရာထက် သာ၍ လုပ်ဆောင်ပေးသော စက်ပစ္စည်းကို ဝယ်ယူခြင်း ဥပမာ အင်တာနက်နှင့် ချိတ်ဆက်ခြင်းမျိုးက သင်၏ လုံခြုံရေးကို လျော့ကျမှု ဖြစ်စေနိုင်ပါသည်။ သင့်အနေဖြင့် အသုံးမပြုသည့် ထိုစက်ပစ္စည်း၏ စွမ်းဆောင်နိုင်မှုများက သင့်ကို အကျိုးမပြုပဲ သင့်စက်ပစ္စည်းကို တိုက်ခိုက်မှုလုပ်နိုင်ရန် အားနည်းမှုများ ဖြစ်စေနိုင်ပါသည်။

IoT အင်တာနက်သုံး ပစ္စည်း

သင်၏ ကွန်ယက်နှင့် ဒေတာအချက်အလက်များကို ပိုမိုလုံခြုံမှုရှိရန် အတွက် သင့်အနေဖြင့် စက်ပစ္စည်းကို စတင်အသုံးပြုသည့်အခါတွင် ရိုးရှင်းသော မေးခွန်းများကို ထည့်သွင်းစဉ်းစားသင့်ပါသည်။

1. **ဤပစ္စည်းသည် အင်တာနက်ဖြင့် ချိတ်ဆက်ရန် လိုအပ်ပါသလား။** အင်တာနက်ဖြင့် ချိတ်ဆက်နိုင်စွမ်း ရှိသည့်အတွက် အင်တာနက်နှင့် ချိတ်ဆက်တာမျိုး မဖြစ်သင့်ပါ။ အင်တာနက်ဖြင့် ချိတ်ဆက်ထားခြင်း မရှိသော စက်ပစ္စည်းများသည် တိုက်ခိုက်ခံရနိုင်ခြေ ပိုနည်းပါးပါသည်။ အင်တာနက်ဖြင့် ချိတ်ဆက်ရန် မလိုအပ်သည့် အရာအတွက် အသုံးပြုပါက အင်တာနက်ဖြင့် ချိတ်ထားမှု လုပ်သင့်မသင့် ထည့်သွင်း စဉ်းစားပါ။

2. **ဤစက်ပစ္စည်းသည် လုံခြုံသည့် နေရာတွင် တည်ရှိပါသလား။** အကယ်၍ ထိုစက်ပစ္စည်းကို လုံခြုံမှု မရှိသည့် နေရာတွင်လည်း ထားရှိနိုင်သည်ဆိုပါက လုံခြုံသည့် နေရာတွင် ထားရှိခြင်းအားဖြင့် ကိုယ်ထိလက်ရောက် တိုက်ခိုက်မှု လုပ်ခြင်း အန္တရာယ်ကို လျော့ချနိုင်ပါသည်။

3. **တခါတည်း ပါလာပြီးသား username နှင့် လျှို့ဝှက်ကုဒ် password များကို ပြောင်းသင့်ပါသလား။** သင့်အနေဖြင့် ခိုင်မာပြီး ခန့်မှန်းရခက်သည့် လျှို့ဝှက်ကုဒ် password နှင့် လျှို့ဝှက် စကားစု passphrase များ ထားရှိရန် အရေးကြီးပါသည်။ အကယ်၍ သင်ဝယ်ယူသည့် စက်ပစ္စည်းတွင် တမူထူခြားပြီး ခန့်မှန်းရခက်ကာ၊ ရှုပ်ထွေးပြီး ခန့်မှန်းရန် မဖြစ်နိုင်သည့် လျှို့ဝှက်ကုဒ် password မပေးထားပါက ပြောင်းလဲမှု လုပ်ရန် လိုအပ်ပါသည်။ နဂိုပါလာပြီးသား username နှင့် လျှို့ဝှက်ကုဒ်များကို စုဆောင်းကာ အွန်လိုင်းပေါ်တွင် တင်ထားလေ့ရှိသည့်အတွက် သင့် စက်ပစ္စည်းအတွက် အန္တရာယ်ရှိနိုင်ပါသည်။

4. **ကျွန်ုပ်၏ Wi-Fi ကွန်ရက်ကို လုံခြုံအောင် လုပ်ဆောင်ထားပြီလား၊ ၎င်းအတွက် လုံခြုံသည့် လျှို့ဝှက်ကုဒ် password ရှိပြီလား။** သင်၏ ကွန်ရက်နှင့် သင့်စက်ပစ္စည်းကို အလွယ်တကူ တိုက်ခိုက်မှု မလုပ်နိုင်ရန်အတွက် သင်၏ Wi-Fi ကွန်ရက် နှင့် router ကို လုံခြုံမှု ရှိအောင် လုပ်ဆောင်ပါ။

ပိုပိုသာသာ လုပ်ဆောင်ပါ

သင်၏ router တွင် IoT အင်တာနက်သုံး ပစ္စည်းများအတွက်သာ ထားရှိသည့် Wi-Fi ကွန်ရက်အပိုတစ်ခုကို ထားရှိပါ။ ထို ကွန်ရက်ကို သင်၏ Wi-Fi router တွင် 'guest' ကွန်ရက်အဖြစ် သတ်မှတ်နိုင်ပါသည်။ အကယ်၍ သင်၏ IoT အင်တာနက်သုံး ပစ္စည်းများ တစ်ခုနှင့် တစ်ခု ချိတ်ဆက်ထားရန် မလိုအပ်ပါက 'client isolation' ကို ဖွင့်ထားပါ။ သင်၏ IoT အင်တာနက်သုံး ပစ္စည်းများကို ထိလွယ်ရှလွယ်မှုရှိသည့် ဒေတာများဖြင့် ခွဲခြားထားခြင်းအားဖြင့် အင်တာနက်သုံး ပစ္စည်း တခုခု တိုက်ခိုက်ခံရပါက သင်၏ အခြားသော စက်ပစ္စည်းနှင့် ဒေတာများကို ဝင်ရောက်မှု မဖြစ်စေနိုင်သည့်အတွက် ဖြစ်ပါသည်။

5. **စက်အတွင်း မလိုအပ်သည့် အရာများကို ဖွင့်ထားမိပါသလား။** သင့် စက်ပစ္စည်းတွင် မလိုချင် သို့မဟုတ် အလိုအပ်သည့် အရာများပါဝင်ပါက (ဥပမာ ကင်မရာ သို့မဟုတ် မိုက်ခရိုဖုန်းများ) ဖြစ်နိုင်လျှင် ထိုအရာများကို ပိတ်ချထားသင့်ပါသည်။

ပိုပိုသာသာ လုပ်ဆောင်ပါ

ဆော့ဖ်ဝဲ၏ setting တွင် local LAN သို့မဟုတ် WAN/internet မှတဆင့် ထိုပစ္စည်း၏ ဝဘ် အက်မင် မျက်နှာပြင်ဆီ အဝေးမှ ဝင်ရောက်ခွင့်ပေးရန်အတွက် enabling remote access to the device's web administration interface from the local LAN or WAN/internet ဆိုသည့် ရေးသားချက်များ ရှိမရှိ ကြည့်ရှုပါ။ သင့်အနေဖြင့် အဝေးမှ ဝင်ရောက်ခွင့် မလိုအပ်ပါက local LAN ကိုသာ ရွေးချယ်ပါ။

IoT အင်တာနက်သုံး ပစ္စည်းကို ပြုပြင်ထိန်းသိမ်းခြင်း

သင်၏ IoT အင်တာနက်သုံး ပစ္စည်းကို စတင်အသုံးပြုသည့်အခါတွင် အရေးကြီးသည့် အချက်အချို့ကို မှတ်သားသင့်ပါသည်။ ထိုအချက်များမှာ-

1. **သင်၏ စက်ပစ္စည်းများကို ပုံမှန် reboot လုပ်ပါ။** သင်၏ စက်ပစ္စည်း အလုပ်လုပ်မှု နှေးကွေးလာလျှင် သို့မဟုတ် ကောင်းမွန်စွာ အလုပ်မလုပ်လျှင် ဗိုင်းရပ်စ်များ ရှိနိုင်ပါသည်။ မသမာသည့် malware များသည် အများအားဖြင့် memory တွင် ရှိတတ်သည့်အတွက် စက်ပစ္စည်းကို ပိတ်ချပြီး ပြန်ဖွင့်ခြင်းနည်းနှင့် reboot လုပ်ရုံမျှဖြင့် အလွယ်တကူ ဖယ်ရှားနိုင်ပါသည်။ သင်၏ စက်ပစ္စည်းကို reboot လုပ်သည့်တိုင် ဆက်လက်ပြီး နှေးကွေးနေပါက သို့မဟုတ် အလုပ်ကို ကောင်းမွန်စွာ မလုပ်ပါက factory reset ကို စမ်းကြည့်ပါ၊ သို့သော် ထိုကဲ့သို့ လုပ်ဆောင်ခြင်းသည် သင်နဂိုက ရှိထားသည့် ဒေတာ အချက်အလက်များနှင့် တခြားသင် ရွေးချယ်ထားသည့် setting များအားလုံး ပျောက်သွားမည် ဆိုသည်ကို တော့ သတိထားပါ။

2. **ပုံမှန် update များ လုပ်ပါ။** အချို့သော စက်ပစ္စည်းများသည် အလိုအလျောက် update များ လုပ်နိုင်ပါသည်။ အလိုအလျောက် မလုပ်သည့် စက်ပစ္စည်းများအတွက် ကုန်ထုတ်လုပ်သူနှင့် ပုံမှန်စစ်ဆေးကာ update များ ရှိသည့်အခါ update လုပ်ပါ။ သင်၏ စက်ပစ္စည်းအတွက် update များ မရှိတော့ပါက update လုပ်နိုင်မည့် စက်ပစ္စည်းအသစ်ကို ပြောင်းလဲ အသုံးပြုရန် စဉ်းစားပါ။ လုံခြုံရေးဆိုင်ရာ update များ မရှိသည့် စက်ပစ္စည်းများသည် အားနည်းချက်များ တွေ့ရှိသည့်အခါ အကာအကွယ်ရှိမှာမဟုတ်သည့်အတွက် သင်၏ ကွန်ရက်၊ ကိုယ်ရေးကိုယ်တာနှင့် ဒေတာ အချက်အလက်များအတွက် အန္တရာယ် ရှိနိုင်ပါသည်။

3. **စက်ပစ္စည်းကို အသုံးမပြုသည့်အခါတွင် ပိတ်ချထားပါ။** အသုံးမပြုခြင်း သို့မဟုတ် စောင့်ကြည့်မှု မရှိသည့် စက်ပစ္စည်းကို ဖွင့်ထားပြီး သင်၏ Wi-Fi ကွန်ရက်နှင့် အချိန်ကြာ ချိတ်ထားခြင်းအားဖြင့် သင်၏ စက်ပစ္စည်း တိုက်ခိုက်ခံရနိုင်ခြေကို ပိုဖြစ်စေနိုင်ပါသည်။ ထို အနေအထား တိုးတက်ရန် အလိုအလျောက် လုပ်နိုင်သည့် နည်းလမ်း တစ်ခုမှာ စက်ပစ္စည်းအတွက် လျှပ်စစ်မီးကို မိမိလိုချင်သည့် အချိန် အပိုင်းအတွက်သာ ဖွင့်ထားရန် timer သတ်မှတ်ပေးနိုင်ပါသည်။

4. **သင်၏ လစဉ် အင်တာနက် အသုံးပြုမှုနှင့် ဘေလ်နှုန်းထားများ သိသိသာသာ များလာခြင်းများ ရှိမရှိ စောင့်ကြည့်ပါ။** အင်တာနက် အသုံးပြုမှု များလာခြင်း သို့မဟုတ် ဘေလ် နှုန်းထားများ များပြားလာခြင်းသည် သင်၏ စက်ပစ္စည်း တိုက်ခိုက်ခံရကြောင်း ပြသနိုင်ပါသည်။ ထိုကဲ့သို့ ဖြစ်ပေါ်ခြင်းကို သင်၏ လုပ်ငန်းမှ IT ဌာနက စုံစမ်းခြင်းမျိုး မဟုတ်ပါက သင့်အနေဖြင့် factory reset ပြုလုပ်သင့်ပါသည်၊ (သို့သော် ထိုကဲ့သို့ လုပ်ဆောင်ခြင်းသည် သင်နဂိုက ရှိထားသည့် ဒေတာ အချက်အလက်များနှင့် တခြား သင်ရွေးချယ်ထားသည့် setting များအားလုံး ပျောက်သွားမည် ဆိုသည်ကိုတော့ သတိထားပါ) ထို့အပြင် သင်သုံးနေသည့် လျှို့ဝှက်ကုဒ် password ကိုလည်း ပြောင်းလိုက်ပါ။

IoT အင်တာနက်သုံး ပစ္စည်းကို စွန့်ပစ်ခြင်း

စက်ပစ္စည်းတစ်ခုကို စွန့်ပစ်ခြင်းအားဖြင့် (စွန့်ပစ်ခြင်း သို့မဟုတ် တဆင့် ရောင်းချခြင်း) အခြားလူများကို သင်၏ ကိုယ်ရေးကိုယ်တာ အကြောင်းအရာနှင့် အချက်အလက်များ ရယူရန် လွယ်ကူစေနိုင်ပါသည်။ ထိုကဲ့သို့ မဖြစ်ရန် ကာကွယ်နိုင်သည့် နည်းလမ်းများမှာ-

1. **ဒေတာအချက်အလက်နှင့် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များ အားလုံးကို ဖျက်ထားပါ။** စက်ပစ္စည်းအတွင်းနှင့် ၎င်းနှင့် ဆက်စပ်သည့် အက်ပလီကေးရှင်းများတွင် ရှိသည့် သင်၏ ဒေတာအချက်အလက်နှင့် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို မည်ကဲ့သို့ ဖျက်လိုက်နိုင်သည့် နည်းလမ်းကို ကုန်ထုတ်လုပ်သူဖက်မှ လုပ်ဆောင်ပေးသင့်ပါသည်။ သင်၏ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို ဖျက်လိုက်ခြင်းအားဖြင့် ထိုစက်ပစ္စည်းကို စွန့်ပစ်လိုက်သည့်တိုင် အခြားလူများ အချက်အလက် ရယူမှု မပြုလုပ်နိုင်ပါ။ ထို IoT အင်တာနက်သုံး ပစ္စည်း မရှိသည့်အခါ ထိုစက်ပစ္စည်းနှင့် ဆက်စပ်ပြီး ရှိသည့် အွန်လိုင်းအကောင့်ကိုလည်း ဖျက်လိုက်ပါ။

2. **စက်ပစ္စည်းကို factory reset လုပ်ဆောင်ခြင်း** Factory reset သည် သင့်စက်အတွင်း သိုလှောင်ထားသည့် ဒေတာများကို ဖျက်ဆီးမှာဖြစ်ပြီး သင်၏ လျှို့ဝှက်ကုဒ် password နှင့် username များ အားလုံးကို ဖျက်ပြီး နဂိုအသစ်ဝယ်ယူသည့်အတိုင်း ဘာဒေတာမှ မရှိအောင် လုပ်ဆောင်နိုင်ပါသည်။ စက်ပစ္စည်း၏ အသုံးပြုမှု လက်စွဲစာစောင် သို့မဟုတ် ကုန်ထုတ်လုပ်သူ၏ ဝဘ်ဆိုက်တွင် ထိုစက်ပစ္စည်းအား မည်ကဲ့သို့ factory reset လုပ်နိုင်သည့် နည်းလမ်းကို လေ့လာနိုင်ပါသည်။

3. **ထိုစက်ပစ္စည်းကို သင့်မိုဘိုင်းဖုန်း အပြင် တခြားချိတ်ဆက်ထားသော စက်များနှင့် ချိတ်ဆက်မှု မရှိတော့အောင် လုပ်ဆောင်ပါ။** သင်၏ အခြားသော စက်ပစ္စည်းများ၊ ကွန်ရက်အပြင် အွန်လိုင်းအကောင့်တို့နှင့် ချိတ်ဆက်မှု ရှိသေးသည့် စက်ပစ္စည်းတစ်ခုကို စွန့်ပစ်ခြင်းအားဖြင့် အခြားလူများကို သင့်၏ အချက်အလက်များရှိရာ ဝင်ရောက်မှု ဖြစ်စေနိုင်ပါသည်။ သင်၏ အခြားသော စက်ပစ္စည်းများကို ဆန်းစစ်ပြီး သင် စွန့်ပစ်မည့် စက်ပစ္စည်းနှင့် ချိတ်ဆက်မှုရှိသေးပါက ချိတ်ဆက်မှုကို ဖယ်ရှားလိုက်ပါ။ မလိုအပ်တော့သည့် မိုဘိုင်း အက်ပလီကေးရှင်းများထဲ ဝင်ရောက်ခွင့်များကိုလည်း ဖယ်ရှားလိုက်ပါ။

4. **စွန့်ပစ်မည့် စက်ပစ္စည်းပေါ်မှ ဖယ်ရှားနိုင်သည့် မီဒီယာ (ဥပမာ USB flash drives, memory cards စသည်တို့) မှန်သမျှကို ဖယ်ရှားပါ။** Factory reset လုပ်သည့်အခါ မီဒီယာများထဲတွင်ရှိသည့် ကိုယ်ရေးအချက်အလက်များကို မဖျက်သိမ်းနိုင်သည့်အတွက် ထိုမီဒီယာများကို လက်ဖြင့် ဖယ်ရှားပြီး ဖျက်ဆီးကာ၊ ထိုအမှိုက်ကိုလည်း စွန့်ပစ်မည့် စက်ပစ္စည်းနှင့် အတူမဟုတ်ပဲ တခြားနေရာတွင် သီးသန့်စွန့်ပစ်ပါ။

အကူအညီ ရယူရန်

ဩစတြေးလျနိုင်ငံ ဆက်သွယ် ညွှန်ကြားရေးမှူးရုံး၏ ဩစတြေးလျ ဆိုင်ဘာလုံခြုံရေးစင်တာအား အီးမေးလ်ဖြင့် asd.assist@defence.gov.au ဆက်သွယ်နိုင်သကဲ့သို့ အရေးပေါ် အကူအညီအတွက် ၂၄ နာရီ၊ ၇ ရက် ပတ်လုံး ခေါ်ဆိုနိုင်သည့် **1300 CYBER1 (1300 292 371) ကို ဖုန်းဆက်နိုင်ပါသည်။**

ဆိုင်ဘာ ရာဇဝတ်မှုများကို ReportCyber ၏ ဝဘ်ဆိုက်ဖြစ်သည့် www.cyber.gov.au/report တွင် တိုင်တန်းနိုင်ပါသည်။

အကယ်၍ သင်၏ မှတ်ပုံတင် အချက်အလက်များ အခိုးခံရပါက IDCARE စင်တာကို ၎င်းတို့၏ ဝဘ်ဆိုက်ဖြစ်သည့် www.idcare.org မှတဆင့် ဆက်သွယ်နိုင်ပါသည်။

သင်နှင့် သင့်မိသားစုအတွက် အကြံပြုချက်များကို www cyber.gov.au တွင် လေ့လာပါ။ အွန်လိုင်းတိုက်ခိုက်မှုများနှင့် ဆက်စပ်ပြီး တပ်လှန့်မှုများ သိရှိရန်အတွက် ACSC Alert Service တွင် sign up အခမဲ့ လုပ်ဆောင်နိုင်ပါသည်။

အွန်လိုင်းချိတ်ဆက်မှုတွင် ဩစတြေးလျသည် လုံခြုံမှုအရှိဆုံး နေရာဖြစ်အောင် လုပ်ဆောင်ကြပါစို့။

ဆိုင်ဘာလုံခြုံရေးအတွက် အကြံပြုချက်များအတွက် www.cyber.gov.au တွင် သွားရောက် လေ့လာနိုင်ပါသည်။

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤလမ်းညွှန်ချက်ပါ အကြောင်းအရာများသည် အထွေထွေအကြံပြုချက်သာဖြစ်ပြီး တရားရေးရာ အကြံပြုချက် အဖြစ် မမှတ်ယူသင့်သကဲ့သို့ တချို့အခြေအနေအတွက် အကူအညီ သို့မဟုတ် အရေးပေါ်အခြေအနေအတွက် အားထားရာ အကြံပြုချက်မဖြစ် မယူဆသင့်ပါ။ အရေးကြီးသည့်အခါ သင်ကြုံတွေ့ရသည့် အတွေ့အကြုံအတွက် သင့်တော်ပြီး သီးသန့် လွတ်လပ်မှုရှိသည့် ကျွမ်းကျင်ပညာရှင်များ၏ အကြံဉာဏ်များကို ရယူပါ။

ဤအကြံပြုချက်ပါ အချက်အလက်များအပေါ် မှီခိုရာက ပျက်စီးမှုဖြစ်ခြင်း၊ ဆုံးရှုံးရခြင်း သို့မဟုတ် ငွေကုန်ကြေးကျ ခံရပါက အစိုးရအနေဖြင့် တာဝန်ယူမည် မဟုတ်ပါ။

မူပိုင်ခွင့်

နိုင်ငံတော် အမှတ်တံဆိပ်ကို အသုံးပြုခြင်း

နိုင်ငံတော် အမှတ်တံဆိပ်အား မည်သည့်နေရာတွင် အသုံးပြုခြင်းဆိုင်ရာ အသေးစိတ်အချက်အလက်အား ဝန်ကြီးချုပ်နှင့် ဝန်ကြီးအဖွဲ့၏ ဝန်ကြီးဌာန၏ ဝဘ်ဆိုက်တွင် ဖော်ပြထားပါသည်၊ နိုင်ငံတော်၏ အမှတ်တံဆိပ် ဆိုင်ရာ အချက်အလက်နှင့် လမ်းညွှန်ချက်များ | pmc.gov.au.

အချက်အလက်ပိုများနှင့် ဆိုင်ဘာလုံခြုံရေး ချိုးဖောက်ခံရမှုအား မည်သို့ တိုင်တန်းနိုင်သနည်း အကြောင်း လေ့လာရန် နှင့် ဆက်သွယ်မှုလုပ်လိုပါက-

cyber.gov.au | 1300 CYBER1 (1300 292 371) ကို ဆက်သွယ်ပါ။

ဤနံပါတ်ကို သြစတြေးလျနိုင်ငံအတွင်းသာ အသုံးပြုနိုင်ပါသည်။

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre