Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

အသေးစားစီးပွားရေးလုပ်ငန်းဆိုင်ရာ ဆိုက်ဘာလုံခြုံရေးလမ်းညွှန်

အကြောင်းအရာ ရှုပ်ထွေးမှု
ရိုးရှင်းသည် ● ○ ○

cyber.gov.au

နိဒါန်း

သေးငယ်သည့် စီးပွားရေးလုပ်ငန်းတစ်ခုအတွက် အသေးစား ဆိုက်ဘာလုံခြုံရေး အဖြစ်အပျက်တစ်ခုကပင်လျှင် ဆိုးရွားသော အကျိုးဆက်များ ဖြစ်စေနိုင်သည်။ ဤလမ်းညွှန်တွင် သင်၏ စီးပွားရေးလုပ်ငန်းကို အဖြစ်များသော ဆိုက်ဘာလုံခြုံရေး ခြိမ်းခြောက်မှုများမှ ကာကွယ်ရန် အခြေခံလုံခြုံရေး အစီအမံများ ပါဝင်သည်။ ပထမ ဆုံးအနေဖြင့် အောက်ပါအစီအမံ သုံးခုကို ကျွန်ုပ်တို့ အကြံပြုလိုပါသည်

- အချက်အလက်မျိုးစုံဖြင့် အတည်ပြုခြင်းကို ဖွင့်ပါ
- သင်၏ ဆော့ဖ်ဝဲလ်ကို အပ်ဒိတ်လုပ်ပါ
- သင်၏ အချက်အလက်များကို အရန်သိမ်းထားပါ

ဤလမ်းညွှန်တွင် သင့်စီးပွားရေးလုပ်ငန်းနှင့် မသက်ဆိုင်သော အစီအမံများ ပါဝင်နိုင်သည် သို့မဟုတ် သင့်စီးပွားရေးလုပ်ငန်းတွင် ပိုမိုရှုပ်ထွေးသော လိုအပ်ချက်များရှိနိုင်သည်။ ဤလမ်းညွှန်ကို ဖတ်ပြီးနောက်တွင် အသေးစားစီးပွားရေး လုပ်ငန်းများအနေဖြင့် မဖြစ်မနေလိုအပ်သော အရာရှစ်ခုအနက် အခြေခံအဆင့်တစ်ကို အကောင်အထည်ဖော်ရန် အကြံပြုပါသည်။ ဤအကြံဉာဏ် သို့မဟုတ် ဆိုက်ဘာလုံခြုံရေးနှင့် ပတ်သက်၍ ပို၍ကျယ်ကျယ်ပြန့်ပြန့် မေးမြန်းလိုပါက အိုင်တီပညာရှင် သို့မဟုတ် ယုံကြည်စိတ်ချရသော အကြံပေးတစ်ဦးနှင့် စကားပြောဆိုရန် အကြံပြုပါသည်။

အစီအမံတစ်ခုစီအတွက် မည်သို့လုပ်ဆောင်ရမည် အကြံဉာဏ်များအပါအဝင် ကျွန်ုပ်တို့၏ လမ်းညွှန်ချက်အပြည့်အစုံကို ဖတ်ရှုရန် cyber.gov.au သို့ သွားရောက်ပါ။

မာတိကာ

အသေးစားစီးပွားရေးလုပ်ငန်းများကို ခြိမ်းခြောက်မှုများ

အလိမ်အညာမက်ဆေ့ချ်များ

အလိမ်အညာမက်ဆေ့ချ်များသည် ဆိုက်ဘာရာဇဝတ်သားများက အသေးစားစီးပွားရေး လုပ်ငန်းများကို ပစ်မှတ်ထားသည့် တွေ့ရများသော နည်းလမ်းတစ်ခုဖြစ်သည်။ ၎င်းတို့၏ ရည်ရွယ်ချက်မှာ သင် သို့မဟုတ် သင်၏ ဝန်ထမ်းများကို အောက်ပါအရာများလုပ်ခိုင်းပြီး လိမ်လည်ရန်ဖြစ်သည် -

- ငွေ သို့မဟုတ် လက်ဆောင်ကတ်များ ပေးပို့ခြင်း
- အန္တရာယ်ရှိသော လင့်ခ်များ သို့မဟုတ် ပူးတွဲပေးပို့မှုများပေါ်တွင် ကလစ်နှိပ်စေခြင်း
- စကားဝှက်ကဲ့သို့ အရေးကြီးအချက်အလက်များကို ရယူခြင်း။

ဆိုက်ဘာရာဇဝတ်သားများသည် အီးမေးလ်၊ စာသားမက်ဆေ့ချ်များ၊ ဖုန်းခေါ်ဆိုမှုများနှင့် လူမှုမီဒီယာမှတစ်ဆင့် သင်၏ စီးပွားရေးလုပ်ငန်းကို လှည့်ဖြားရန် ကြိုးစားနိုင်သည်။ ၎င်းတို့သည် မကြာခဏအားဖြင့် သင်ယုံကြည်ရသည့် လူတစ်ယောက် သို့မဟုတ် အဖွဲ့အစည်းတစ်ခုကဲ့သို့ ဟန်ဆောင်တတ်သည်။

လျှို့ဝှက်အချက်အလက်ခိုးယူ တိုက်ခိုက်မှုများ

အသေးစားစီးပွားရေးလုပ်ငန်းများအတွက် အထူးစိုးရိမ်ပူပန်စရာမှာ **လျှို့ဝှက်အချက်အလက်ခိုးယူ တိုက်ခိုက်မှုများ** ဖြစ်သည်။ ဤအလိမ်အညာမက်ဆေ့ချ်များတွင် မကြာခဏ အားဖြင့် အကောင့်တစ်ခုသို့ ဝင်ရောက်ရန် သို့မဟုတ် လျှို့ဝှက်အချက်အလက်များကို ထည့်သွင်းရန် သင့်အားတိုက်တွန်းထားသည့် ဝက်ဘ်ဆိုက်အတုု၏ လင့်ခ်တစ်ခု ပါဝင်သည်။

လျှို့ဝှက်အချက်အလက်ခိုးယူ တိုက်ခိုက်မှုများသည် ပုံမှန်အားဖြင့် သင့်အကောင့် စကားဝှက်များကို ကျိုးပေါက်စေပါသည်။ ဆိုက်ဘာရာဇဝတ်သားများသည် အသေးစားစီးပွားရေးလုပ်ငန်းများ၏ လူမှုမီဒီယာအကောင့်များကို “သိမ်းယူ” ပြီး ငွေညှစ်ရန် ဤနည်းလမ်းကို မကြာခဏ အသုံးပြုတတ်သည်။

လျှော့ချရန် နည်းလမ်းများ

မက်ဆေ့ချ်တစ်ခုသည် လူသိများသော အဖွဲ့အစည်းတစ်ခုမှ ဖြစ်ပြီး သံသယဖြစ်စရာဖြစ်နေပါက သတိထားပါ။မက်ဆေ့ချ်သည် တရားဝင်ခြင်းရှိမရှိ စစ်ဆေးရန် လူပုဂ္ဂိုလ် သို့မဟုတ် စီးပွားရေးလုပ်ငန်းကို သီးခြားဆက်သွယ်ပါ။ ဥပမာ တရားဝင်အရင်းအမြစ်မှတစ်ဆင့် သင်တွေ့ရှိသော အဆက်အသွယ် အသေးစိတ်အချက်အလက်များကို စီးပွားရေးလုပ်ငန်း၏ တရားဝင် ဝက်ဘ်ဆိုက်သို့ ဝင်ရောက်ကြည့်ရှုခြင်းဖြင့် အသုံးပြုပါ။ သံသယရှိသော မက်ဆေ့ချ်တွင် ပါဝင်သည့် ဝဘ်ဆိုက်ကို အသုံးမပြုပါနှင့်။

- အလိမ်အညာမက်ဆေ့ချ်များကို သိရှိခြင်းနှင့် သတင်းပို့ခြင်း
- လျှို့ဝှက်အချက်အလက်များခိုးယူသည့် အလိမ်အညာ မက်ဆေ့ချ်များကို မည်သို့ရှာဖွေရမည်ကို လေ့လာခြင်း
- လူမှုရေး အင်ဂျင်နီယာမက်ဆေ့ချ်များကို ရှာဖွေခြင်း။

သာဓကဖြစ်ရပ်လေ့လာခြင်း-

ပစ္စည်းသယ်ယူပို့ဆောင်ရေးကုမ္ပဏီမှ ဝန်ထမ်းတစ်ဦးသည် ၎င်းတို့၏ အမှုဆောင်အရာရှိဝန်ထမ်းတစ်ဦးထံမှ $500 တန် MasterCard ကြိုတင်ငွေပေးချေရသည့် ခရက်ဒစ်ကတ် 6 ကတ်ကို ဝယ်ခိုင်းသည့် အီးမေးလ်တစ်စောင်ကို ရရှိခဲ့သည်။ ကတ်များသည် ဝန်ထမ်းများအတွက် လက်ဆောင် ပေးရန်ဖြစ်သောကြောင့် ၎င်းကိုလျှို့ဝှက်ထားရန် အမှုဆောင်အရာရှိချုပ်က ပြောကြားခဲ့သည်။ ဝယ်ယူပြီးနောက် ဝန်ထမ်းအား ကတ်များ၏ နှစ်ဖက်စလုံးကို ဓာတ်ပုံရိုက်ပြီး ဝယ်ယူမှုသက်သေအဖြစ် အမှုဆောင်အရာရှိချုပ်ထံ ပေးပို့ရန် တောင်းဆိုခဲ့သည်။

ညွှန်ကြားထားသည့်အတိုင်း ဝန်ထမ်းသည် စာတိုက်သို့သွားပြီး လက်ဆောင်ကတ်များကို ဝယ်ယူရန် ၎င်း၏ ကိုယ်ပိုင်ခရက်ဒစ်ကတ်ကို အသုံးပြုခဲ့သည်။ သူမက အမှုဆောင်အရာရှိ၏အီးမေးလ်ကို အကြောင်းပြန်ပြီး သက်သေအဖြစ် လက်ဆောင်ကတ်များ၏ ဓာတ်ပုံများကို ပေးပို့ခဲ့သည်။

စာတိုက်မှ ပြန်လာပြီးနောက် ဝန်ထမ်းသည် အမှုဆောင်အရာရှိချုပ်ထံ ကတ်များကို သွားပေးခဲ့ရာ ၎င်းတို့အကြောင်းကို အမှုဆောင်အရာရှိချုပ်က မသိခဲ့ပါ။ **ပြန်လည်သုံးသပ်ရာတွင် လက်ဆောင်ကတ်များနှင့် ပတ်သက်သော အီးမေးလ်အားလုံးသည် ကျပန်းအီးမေးလ်လိပ်စာမှ ဖြစ်ပြီး အမှုဆောင်အရာရှိချုပ်၏ တရားဝင်အီးမေးလ်အကောင့်မှ မဟုတ်ပါ။ ၎င်းသည် အလိမ်အညာမက်ဆေ့ချ်တစ်ခု ဖြစ်ခဲ့သည်။**

အီးမေးလ်တိုက်ခိုက်မှုများ

လျှို့ဝှက်အချက်အလက်ခိုးယူခြင်း ကဲ့သို့သော အလိမ်အညာမက်ဆေ့ချ်များအပြင် အသေးစားစီးပွားရေး လုပ်ငန်းများအပေါ် တိုက်ခိုက်သည့် တွေ့ရများသော အီးမေးလ်တိုက်ခိုက်မှုမှာ **စီးပွားရေးလုပ်ငန်း အီးမေးလ် ကျိုးပေါက်မှု** (BEC) ဖြစ်သည်။ ပြစ်မှုကျူးလွန်သူများသည် ကျိုးပေါက်နေသော အီးမေးလ်အကောင့်များကို အသုံးပြုခြင်းဖြင့် သို့မဟုတ် စီးပွားရေးလုပ်ငန်းအစစ်နှင့် ဆင်တူသော ဒိုမိန်းအမည်ကို အသုံးပြုခြင်းကဲ့သို့ အခြားနည်းလမ်းများမှတစ်ဆင့် လုပ်ငန်းကိုယ်စားလှယ်များဟန်ဆောင်နိုင်သည်။ သတင်းအချက်အလက်ခိုးယူခြင်းအပြင် ဤတိုက်ခိုက်မှုများ၏ ရည်ရွယ်ချက်မှာ အများအားဖြင့် အလိမ်ခံရသူများအား လိမ်လည်သူ ကိုင်ဆောင်သည့် ဘဏ်စာရင်းသို့ ငွေပေးပို့အောင် လိမ်ညာခြင်းဖြစ်သည်။

လျှော့ချရန် နည်းလမ်းများ

အီးမေးလ်တိုက်ခိုက်မှုများမှ အကောင်းဆုံးကာကွယ်မှုမှာ သင်၏ ဝန်ထမ်းများအား သင်တန်းပေးခြင်းနှင့် အသိပညာပေးခြင်းဖြစ်သည်။ သင်၏ ဝန်ထမ်းများအနေဖြင့် အောက်ပါတို့နှင့်အတူ အီးမေးလ်များကို အမြဲတမ်းသတိထားကြောင်း သေချာပါစေ-

- ငွေပေးချေမှုများအတွက် တောင်းဆိုမှုများ၊ အထူးသဖြင့် အရေးပေါ် သို့မဟုတ် ရက်လွန်နေလျှင်
- ဘဏ်အချက်အလက်များ ပြောင်းလဲခြင်း
- မမှန်ကန်ဟုထင်ရသော အီးမေးလ်လိပ်စာ ဥပမာ ကုန်ပစ္စည်းပေးသွင်းသူ၏ ကုမ္ပဏီအမည်နှင့် အတိအကျ မကိုက်ညီသော ဒိုမိန်းအမည်။

ဤတိုက်ခိုက်မှုများသည် အလွန်ဖျက်ဆီးနိုင်သော်လည်း လျှော့ချရေး အစီအမံများသည် လွယ်ကူပြီး **ကုန်ကျစရိတ်မရှိသလောက်နီးပါးဖြစ်သည်။ ဝန်ထမ်းများသည် ဤကဲ့သို့ အီးမေးလ်များကို လက်ခံရရှိသောအခါ ၎င်းတို့သည် တရားဝင်ကြောင်း အတည်ပြုရန် ပေးပို့သူကို ဖုန်းခေါ်ဆိုခြင်းသည် အထိရောက်ဆုံး လျှော့ချမှုဖြစ်သည်။ သင့်ထံပေး** ပို့ထားသော အဆက်အသွယ် အသေးစိတ်အချက်အလက်များမှာ အတုများဖြစ်နိုင်သောကြောင့် ၎င်းတို့ကို မသုံးပါနှင့်။ ငွေပေးချေမှု တောင်းဆိုချက်များကို လက်ခံရရှိသည့်အခါ သို့မဟုတ် ဘဏ်အသေးစိတ်အချက်အလက်များကို ပြောင်းလဲသည့်အခါ ဝန်ထမ်းများ လိုက်နာရမည့် တရားဝင်လုပ်ငန်းစဉ်တစ်ခုကို မိတ်ဆက်ပေးပါ။

သင်၏ စီးပွားရေးလုပ်ငန်းကို BEC အလိမ်အညာမက်ဆေ့ချ်များနှင့် အီးမေးလ်ကျိုးပေါက်မှုများကို အောက်ပါအရင်းအမြစ်များဖြင့် ကာကွယ်ရန် လေ့လာပါ-

- စီးပွားရေးလုပ်ငန်း အီးမေးလ် ကျိုးပေါက်မှု
- သင့်စီးပွားရေး လုပ်ငန်းကို အီးမေးလ်လိမ်လည်မှုနှင့် ကျိုးပေါက်မှုမဖြစ်အောင် ကာကွယ်ပါ
- သင့်စီးပွားရေးလုပ်ငန်းသည် အီးမေးလ် လိမ်လည်မှု သို့မဟုတ် ကျိုးပေါက်မှုဖြင့် ပစ်မှတ်ထားခံရပါက ဘာလုပ်ရမလဲ။

သာဓကဖြစ်ရပ်လေ့လာခြင်း-

ဆောက်လုပ်ရေးလုပ်ငန်း အသေးစားတစ်ခုသည် ၎င်းတို့၏ ကုန်ပစ္စည်းပေးသွင်းသူထံမှ ဘဏ်များပြောင်းလဲခဲ့ကြောင်း အီးမေးလ်တစ်စောင်ကို လက်ခံရရှိခဲ့သည်။ ကုန်ပစ္စည်းပေးသွင်းသူသည် ငွေတောင်းခံလွှာ ပေးချေမှုများအတွက် အကောင့်အသေးစိတ်အချက်အလက်အသစ်များကို ပေးခဲ့သည်။

အီးမေးလ်သည် တရားဝင်ပုံရသောကြောင့် ဆောက်လုပ်ရေးလုပ်ငန်းသည် ဘဏ်အကောင့် အသေးစိတ်အချက်အလက်များ ပြောင်းလဲခြင်းကို အတည်ပြုရန် ကုန်ပစ္စည်းပေးသွင်းသူကို ဖုန်းမခေါ်ခဲ့ပါ။

ကုမ္ပဏီက ကုန်ပစ္စည်းပေးသွင်းသူထံမှ $70,000 ကျော် ငွေတောင်းခံလွှာကို ငွေပေးချေခဲ့သည်။ နောက်တစ်နေ့တွင် အခြားဝန်ထမ်းတစ်ဦးက မှားယွင်းပြီး အဆိုပါ ငွေတောင်းခံလွှာအတွက် နောက်ထပ်ဒေါ်လာ $70,000 ကျော်ကို ထပ်မံပေးချေခဲ့သည်။ စုစုပေါင်း $150,000 ကျော်ကို ဘဏ်အကောင့်သစ်သို့ ငွေပေးချေခဲ့သည်။

၎င်းတို့က နှစ်ခါထပ်လွှဲထားသော ငွေပေးချေမှုကို ပြန်ပေးနိုင်မလားဟုမေးရန် ကုမ္ပဏီက ၎ င်းတို့၏ ကုန်ပစ္စည်းပေးသွင်းသူကို ဖုန်းခေါ်ဆိုသောအခါ ပေးသွင်းသူက ဘဏ်အသေးစိတ်အချက်အလက်များ မှားယွင်းနေကြောင်း အသိပေးခဲ့သည်။ စုံစမ်းစစ်ဆေးမှုတစ်ခုကို ချက်ချင်း စတင်ခဲ့ပြီး ကုန်ပစ္စည်းပေးသွင်းသူက ၎င်းတို့၏ အီးမေးလ်အကောင့်တစ်ခုကို ခိုးဝင်ခံရပြီး လိမ်လည်သော ဘဏ်စာရင်း အသေးစိတ်အချက်အလက်များကို ပေးပို့ထား **ကြောင်း တွေ့ရှိခဲ့သည်။ ပို့ဆောင်ပြန်လည်မရရှိခဲ့ပါ။**

အန္တရာယ်ရှိ ဆော့ဖ်ဝဲ

မောလ်ဝဲ သည် ငွေညှစ်ရန်ဆော့ဖ်ဝဲ၊ ဗိုင်းရပ်စ်များ၊ သူလျှို ဆော့ဖ်ဝဲလ်နှင့် အဖျက်ဆော့ဖ်ဝဲလ်တို့ကဲ့သို့ အန္တရာယ်ဖြစ်စေရန် ဒီဇိုင်းပြုလုပ်ထားသော အန္တရာယ်ရှိဆော့ဖ်ဝဲများအားလုံး အကျုံးဝင်သော အသုံးအနှုန်းတစ်ခု ဖြစ်သည်။ မောလ်ဝဲသည်-

- သင်၏ ကိရိယာပေါ်ရှိဖိုင်များကို ခိုးယူနိုင်သည် သို့မဟုတ် ပိတ်နိုင်သည်
- သင်၏ ဘဏ် သို့မဟုတ် ခရက်ဒစ်က ဒ်နံပါတ်များကို ခိုးယူနိုင်သည်
- သင်၏ အသုံးပြုသူအမည်များနှင့် စကားဝှက်များကို ခိုးယူနိုင်သည်
- သင့်ကွန်ပျူတာကို ထိန်းချုပ်နိုင်သည် သို့မဟုတ် သူလျှိုလုပ်နိုင်သည်။

မောလ်ဝဲက သင့်စက်ကို ကောင်းမွန်စွာအလုပ်မလုပ်နိုင်စေခြင်း၊ ဖိုင်များကို ဖျက်ပစ်ခြင်း သို့မဟုတ် ပျက်စီးစေခြင်းတို့ ဖြစ်စေနိုင်သည် သို့မဟုတ် အခြားသူများအား သင်၏ ပုဂ္ဂိုလ်ရေး သို့မဟုတ် စီးပွားရေးဆိုင်ရာ အချက်အလက်များကို ရယူကြည့်ရှုခွင့် ရစေနိုင်သည်။ သင်၏ ကိရိယာတွင် မောလ်ဝဲ ကူးစက်ခံရပါက သင်သည် အခြားတိုက်ခိုက်မှုများအတွက် အန္တရာယ်ရှိနိုင်သည်။ သင်၏ ကွန်ရက်ပေါ်ရှိ အခြားကိရိယာများသို့လည်း မောလ်ဝဲပြန့်နှံ့နိုင်သည်။

သင်၏ ကိရိယာကို အောက်ပါတို့အပါအဝင် အမျိုးမျိုးသော နည်းလမ်းများဖြင့် မောလ်ဝဲကူးစက်နိုင်သည်-

- မောလ်ဝဲကူးစက်ခံထားရသော ဝက်ဘ် ဆိုက်များသို့ ဝင်ရောက်ကြည့်ရှုခြင်း
- ကူးစက်ခံရသောဖိုင်များ သို့မဟုတ် ဆော့ဖ်ဝဲများကို အင်တာနက်မှ ဒေါင်းလုဒ်ဆွဲခြင်း
- ကူးစက်ခံထားရသော အီးမေးလ် ပူးတွဲပေးပို့မှုများကို ဖွင့်ခြင်း။

ငွေညှစ်ရန်ဆော့ဖ်ဝဲ

ငွေညှစ်ရန်ဆော့ဖ်ဝဲသည် အသုံးများသည့် အန္တရာယ်ရှိသော မောလ်ဝဲအမျိုးအစားတစ်ခု ဖြစ်သည်။ ၎င်းသည် သင့်ဖိုင်များကို သင် ရယူကြည့်ရှု၍ မရနိုင်တော့စေရန် ဖိုင်များကိုပိတ်ထားခြင်း သို့မဟုတ် လျှို့ဝှက်ကုတ်လုပ်ခြင်း ဖြင့် အလုပ်လုပ်သည်။ ယေဘုယျအားဖြင့် ဒစ်ဂျစ်တယ် ငွေကြေး ပုံစံဖြင့် ဖိုင်များကို ပြန်လည်ရယူပေးရန် တောင်းဆိုနိုင်သည်။ ဆိုက်ဘာရာဇဝတ်သားများသည် တောင်းထားသည့်ငွေကို မရရှိပါက ဒေတာများကို အွန်လိုင်းတွင် တင်မည် သို့မဟုတ် ရောင်းချမည်ဟုလည်း ခြိမ်းခြောက်နိုင်သည်။

လျှော့ချရန် နည်းလမ်းများ

ဗိုင်းရပ်စ်ကာဆော့ဖ်ဝဲ သို့မဟုတ် လုံခြုံရေးဆော့ဖ်ဝဲသည် သင့်ကို မောလ်ဝဲမှ ကာကွယ်ရန်ကူညီပေးနိုင်သော်လည်း မည်သည့် ဆော့ဖ်ဝဲမှ 100% ထိရောက်သည်မဟုတ်ပါ။ ဝန်ထမ်းများသည် အီးမေးလ်များ၊ ဝက်ဘ်ဆိုက်များနှင့် ဖိုင်ဒေါင်းလုပ်ဆွဲခြင်းများနှင့် ပတ်သက်၍ သတိထားရမည်ဖြစ်ပြီး ဘေးကင်းလုံခြုံရန် ၎င်းတို့၏ ကိရိယာများကို ပုံမှန် အပ်ဒိတ်လုပ်ရမည်။

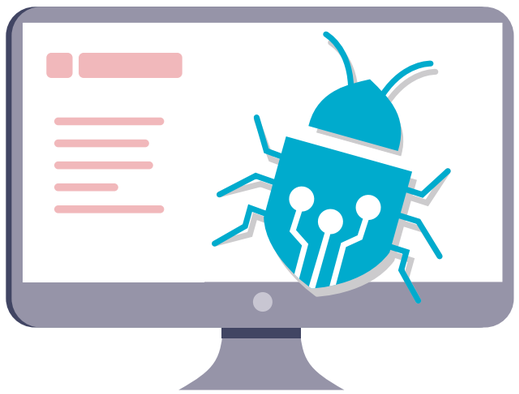
- ငွေညှစ်ရန်ဆော့ဖ်ဝဲ
- ငွေညှစ်ရန်ဆော့ဖ်ဝဲ တိုက်ခိုက်မှုများမှ သင့်ကိုယ်သင်ကာကွယ်ပါ
- သင် ငွေညှစ်ခံရပါက မည်သို့ပြုလုပ်မည်နည်း။

သာဓကဖြစ်ရပ်လေ့လာခြင်း-

နံနက်ခင်းတစ်ခုတွင် ကားအပိုပစ္စည်း စတိုးဆိုင်ဝန်ထမ်းတစ်ဦးက အလုပ်သို့ရောက်ရှိလာပြီး ၎င်းတို့ ဆာဗာကွန်ပျူတာကို ဖွင့်၍မရနိုင်ဖြစ်နေသည်။ ၎င်းတို့၏ အိုင်တီပံ့ပိုးသူသည် ဆာဗာသို့ ဝင်ရောက်ခွင့်ရသောအခါ ကွန်ပျူတာဒေတာအားလုံးကို လျှို့ဝှက်ကုတ်လုပ်ထားသည်ဟု ပြောသော ဝင်းဒိုးတစ်ခုပွင့်နေသည်ကို တွေ့ရှိရသည်။ ၎င်းမှတ်စုသည် ဖိုင်များကိုဖွင့်ရန် Bitcoin ဖြင့် အခကြေးငွေပေးရန် တောင်းဆိုထားသည်။

ကွန်ပျူတာထဲတွင် အရန်ဒရိုက်ဗ်တစ်ခုထည့်ထားသည့်တိုင် ၎င်းမှာလည်း လျှို့ဝှက်ကုတ်ရေးထားခြင်းခံရသည်။ ၎င်းတို့သည် နောက်ထပ်အရန်ဒရိုက်ဗ်များကို ချိတ်ဆက်ရန် ကြိုးစားခဲ့သော်လည်း ဖိုင်များကို စက္ကန့်အနည်းငယ်အတွင်း အလိုအလျောက် လျှို့ဝှက်ကုတ်ရေးခြင်းခံရသည်။ **၎င်းတို့၏ ဒေတာကို ပြန်လည်ရယူရန် ကြိုးပမ်းခြင်းမပြုမီ ငွေညှစ်သည့် ဆော့ဖ်ဝဲကို ဖယ်ရှားရန်မအောင်မြင်ခဲ့ခြင်းကြောင့် ၎င်းတို့တွင်ရှိသမျှ အရန်ဖိုင်များ ဆုံးရှုံးခဲ့ရသည်။**

ကျန်ရှိသော တစ်ခုတည်းသော ရွေးချယ်စရာမှာ ဆာဗာကို မူလဝယ်စဉ်ကအတိုင်း ပြန်လည်သတ်မှတ်ပြီး စနစ်အသစ်ဖြင့် အသစ်စတင်ရန် ဖြစ်သည်။ ၎င်းတို့၏ လုပ်ငန်းသည် နှစ်ပေါင်းများစွာ စုဆောင်းထားရှိခဲ့သည့် အချက်အလက်များ ဆုံးရှုံးခဲ့ရပြီး အသစ်ပြန်စတင်ခဲ့ရပါသည်။



သင်၏အကောင့်များကိုလုံခြုံအောင်ထားပါ

အချက်အလက်မျိုးစုံဖြင့်အတည်ပြုခြင်းကိုဖွင့်ပါ

အချက်အလက်မျိုးစုံဖြင့် အတည်ပြုခြင်းကိုဖွင့်ခြင်း (MFA) သည် သင်၏ အကောင့်များကို ရယူအသုံးပြုရန် ပိုမိုခက်ခဲစေသည်။

MFA သည် သင်၏ အကောင့်တွင် လုံခြုံရေးအလွှာတစ်ခု ထပ်ထည့်ပေးသည်။ ၎င်းသည် သင်၏ အကောင့်များကို မည်သူမဆို ရယူအသုံးပြုခြင်းမှ ကာကွယ်ရန် အထိရောက်ဆုံး နည်းလမ်းများထဲမှ တစ်ခုဖြစ်သည်၊ ထို့ကြောင့် ၎င်းကို သင်တတ်နိုင်သမျှ နေရာတိုင်းတွင် အသုံးပြုသင့်သည်။ သင်၏ အကောင့်ထဲသို့ ဝင်သော မည်သူမဆိုသင်၏ အသုံးပြုသူအမည်နှင့် စကားဝှက် အပြင် အခြားတစ်ခုခုပေးရန် လိုအပ်ပါမည်။ ၎င်းသည်စာသားမက်ဆေ့ချ်သို့မဟုတ် authenticator app မှထူးခြားသောကုဒ် တစ်ခုဖြစ်နိုင်သည်။ ပိုမိုသိရှိလိုပါက **cyber.gov.au/mfa** တွင် ရရှိနိုင်သော MFA အပေါ် ကျွန်ုပ်တို့၏ အကြံဉာဏ်ကို ဖတ်ပါ။

✓ သင် ၏ အရေးကြီးဆုံးအကောင့်များမှစ ၍ ဖြစ်နိုင်သမျှနေရာတိုင်းတွင် MFA ကိုဖွင့်ပါ။

ဝင်ရောက်ခွင့်ထိန်းချုပ်မှုများကို အကောင်အထည်ဖော်ပါ

အသုံးပြုသူဝင်ရောက်မှုကို ကန့်သတ်ခြင်းသည် ဆိုက်ဘာလုံခြုံရေးဖြစ်ရပ်တစ်ခုကြောင့် ဖြစ်ပွားသော ပျက်စီးမှုကို ကန့်သတ်နိုင်သည်။

ဝင်ရောက်ခွင့်ထိန်းချုပ်မှုများသည် အချို့သောဖိုင်များနှင့် စနစ်များသို့ဝင်ရောက်ခွင့်ကို ကန့်သတ်ရန် နည်းလမ်းတစ်ခု ဖြစ်သည်။ ပုံမှန်အားဖြင့် ဝန်ထမ်းများသည် စီးပွားရေးလုပ်ငန်းတစ်ခုတွင် အချက်အလက်များ၊ အကောင့်များနှင့် စနစ်များအားလုံးကို အပြည့်အဝ ရယူကြည့်ရှုရန် မလိုအပ်ပါ။ ၎င်းတို့ကို ၎င်းတို့၏ တာဝန်များ လုပ်ဆောင်ရန် လိုအပ်သည့် အရာများကိုသာ ဝင်ရောက်ကြည့်ရှုခွင့်ပြုသင့်သည်။

ဆိုက်ဘာလုံခြုံရေးကြောင့် ဖြစ်ပွားသော ထိခိုက်ပျက်စီးမှုများကို ဝင်ရောက်ကြည့်ရှုမှု ကန့်သတ်ခြင်းက ကူညီပေးပါမည်။ ဥပမာအားဖြင့် ဝန်ထမ်းတစ်ဦး၏ ကွန်ပျူတာတွင် ငွေညှစ်ရန်ဆော့ဖ်ဝဲ ကူးစက်ခံရပါက ဝင်ရောက်ကြည့်ရှုမှု ကန့်သတ်ထားလျှင် ၎င်းသည် လုပ်ငန်းတစ်ခုလုံးကို မဟုတ်ဘဲ ဖိုင်အနည်းငယ်အပေါ်သာ သက်ရောက်မှုရှိနိုင်သည်။

✓ အသုံးပြုသူတစ်ဦးချင်းစီသည် ၎င်းတို့၏ တာဝန်အတွက် လိုအပ်သည့်အရာများကိုသာ ရယူကြည့်ရှုနိုင်ကြောင်း သေချာပါစေ။

ခိုင်မာသော စကားဝှက်များ သို့မဟုတ် ဝှက်စာစကားစုများကို အသုံးပြုပါ

သင့်အကောင့်များကို ဘေးကင်းလုံခြုံသော စကားဝှက် သို့မဟုတ် ဝှက်စာစကားစုဖြင့် ဆိုက်ဘာရာဇဝတ်သားများရန်မှ ကာကွယ်ပါ။

အသေးစားလုပ်ငန်းများစွာသည် စကားဝှက်အသုံးပြုပုံအားနည်းခြင်းကြောင့် ဆိုက်ဘာတိုက်ခိုက်မှုများကို ရင်ဆိုင်ကြရသည်။ ဥပမာအားဖြင့် အလားတူစကားဝှက်ကို အကောင့်များစွာတွင် ပြန်လည်အသုံးပြုခြင်းမျိုး ဖြစ်သည်။ ခိုင်မာသည့်စကားဝှက်များ ဖန်တီးရန် **စကားဝှက်မန်နေဂျာ** နှင့် ဝှက်စာစကားစုနှစ်မျိုးစလုံးကို အသုံးပြုနိုင်သည်။

စကားဝှက်မန်နေဂျာ သည် သင်၏ စကားဝှက်များအတွက် အွန်လိုင်းမီးခံသေတ္တာကဲ့သို့ လုပ်ဆောင်သည်။ သင်သည် ၎င်းကို သင်၏ အကောင့်တစ်ခုချင်းစီအတွက် ခိုင်မာပြီး **ထူးခြားသော** စကားဝှက်များကို ဖန်တီးရန်နှင့် သိမ်းဆည်းရန် အသုံးပြုနိုင်သည်။ အကယ်၍ သင့်တွင် အကောင့်အများအပြားရှိပါက ၎င်းသည် ထူးခြားသော စကားဝှက်များကို မှတ်ထားရမည့် ဝန်ထုပ်ဝန်ဖိုးကို ဖယ်ရှားပေးသည်။ သင်၏ စကားဝှက် မန်နေဂျာတွင် အားလုံးကို မှတ်တမ်းတင်ထားသောကြောင့် စကားဝှက်များ သို့မဟုတ် ၎င်းတို့နှင့် သက်ဆိုင်သည့် အကောင့်များကို မှတ်ထားရန်မလိုအပ်ပါ။

သင်ပံ့မှန်ဝင်ရောက်သော သို့မဟုတ် စကားဝှက်မန်နေဂျာတွင် မသိမ်းဆည်းလိုသည့် အကောင့်များအတွက် သင်၏ စကားဝှက်အဖြစ် ဝှက်စာစကားစုကို အသုံးပြုရန် စဉ်းစားပါ။ ဝှက်စာစကားစုသည် ကျပန်းစကားလုံးများ ပေါင်းစပ်မှု ဖြစ်သည်၊ ဥပမာ 'သင်းကျောက် ကြက်သွန်နီ ရွှံ့မှန့်ကြိုးလိမ်'။ အလွယ်တကူ မှတ်မိနိုင်သည့် စိတ်ချရသည့် စကားဝှက်တစ်ခုကို သင်လိုချင်သည့်အခါ ၎င်းတို့သည် အသုံးဝင်ပါသည်။ လေးလုံး သို့မဟုတ် ထိုထက်ပိုသော စကားလုံးများကို ကျပန်းရောနှောမှုကို အသုံးပြုပြီး ထူးခြားအောင်ထားပါ- အကောင့်ပေါင်းများစွာတွင် **ဝှက်စာစကားစုတစ်လုံးတည်းကို ကို ထပ်မံအသုံးပါနှင့်။** ပိုမိုသိရှိလိုပါက **cyber.gov.au/passphrases** တွင် ရရှိနိုင်သော ဝှက်စာစကားလုံးများနှင့် စကားဝှက်မန်နေဂျာများနှင့် ပတ်သက်သည့် ကျွန်ုပ်တို့၏ အကြံဉာဏ်ကို ဖတ်ပါ။

✓ သင်၏ အရေးကြီးသော အကောင့်တစ်ခုချင်းစီအတွက် ထူးခြားသော စကားဝှက်များကို ဖန်တီးရန်နှင့် သိမ်းဆည်းရန် စကားဝှက်မန်နေဂျာကို အသုံးပြုပါ။

မျှဝေအသုံးပြုသည့် အကောင့်များကိုစီမံခန့်ခွဲခြင်း

အကောင့်များကို မျှဝေခြင်းသည် လုံခြုံရေးကို ထိခိုက်စေနိုင်ပြီး အန္တရာယ်ရှိသော လှုပ်ရှားမှုများကို ခြေရာခံရန် ခက်ခဲစေသည်။

အသေးစားစီးပွားရေးလုပ်ငန်းတစ်ခုတွင် ဝန်ထမ်းများအနေဖြင့် အကောင့်များကို မျှဝေရန် လိုအပ်သော တရားဝင်အကြောင်းရင်းများရှိနိုင်သော်လည်း ၎င်းကို တတ်နိုင်သမျှ ရှောင်ရှားသင့်သည်။ ဝန်ထမ်းများစွာက တူညီသောအကောင့်ကို အသုံးပြုသောအခါ သက်ဆိုင်ရာဝန်ထမ်းတစ်ဦးထံသို့ လှုပ်ရှားမှုကို ပြန်လည်ခြေရာခံရန် ခက်ခဲနိုင်ပြီး ဆိုက်ဘာရာဇဝတ်မှု ကျူးလွန်သူများကို ခြေရာခံရန် ပိုမိုခက်ခဲနိုင်သည်။ အကယ်၍ သင်သည် စကားဝှက်ကို မပြောင်းလဲပါက ဝန်ထမ်းများသည် လုပ်ငန်းမှ ထွက်ခွာပြီး နောက်ပင် အကောင့်များကို ဝင်ရောက်အသုံးပြုနိုင်သည်။

✓ မျှဝေအသုံးပြုသည့် အကောင့်များကိုကန့်သတ်ပြီး သင့်လုပ်ငန်းတွင်အသုံးပြုသော မည်သည့်အကောင့်ကိုမဆို လုံခြုံစွာထားပါ။

သင်၏ ကိရိယာများနှင့် သတင်းအချက်အလက်များကိုကာကွယ်ပါ

သင်၏ ဆော့ဖ်ဝဲလ်ကို အပ်ဒိတ်လုပ်ပါ

သင်၏ ဆော့ဖ်ဝဲလ်ကို အချိန်နှင့်အလိုက် ထိန်းသိမ်းခြင်းသည် သင်၏ လုပ်ငန်းကို ဆိုက်ဘာတိုက်ခိုက်မှုမှကာကွယ်ရန် အကောင်းဆုံးနည်းလမ်းများထဲမှ တစ်ခုဖြစ်သည်။

အပ်ဒိတ်များသည် သင်၏ လည်ပတ်သည့်စနစ်နှင့် အခြားဆော့ဖ်ဝဲလ်များ၌ လုံခြုံရေးချို့ယွင်းချက်များကို ဖြေရှင်းနိုင်သည်၊ သို့ဖြစ်၍ ဆိုက်ဘာရာဇဝတ်သားတစ်ဦး အတွက် ချိုးဖောက်ဝင်ရောက်ရန် ပို၍ခက်ခဲနိုင်ပါသည်။ ချို့ယွင်းချက်အသစ်များကို အမြဲတွေ့ရှိရပါသည်၊ ထို့ကြောင့် အပ်ဒိပ်လုပ်ရန် နှိုးဆော်ချက်များကို လျစ်လျူမရှုပါနှင့်။ သင်၏ ဆော့ဖ်ဝဲလ်ကို ပုံမှန်အပ်ဒိပ်လုပ်ခြင်းသည် ဆိုက်ဘာရာဇဝတ်သားတစ်ယောက်က သင်၏ စက်ပစ္စည်းကို မောလ်ဝဲထည့်ခြင်း သို့မဟုတ် သင့်စက်ပစ္စည်းထဲ ခိုးဝင်ခြင်းကဲ့သို့ လူသိများသော အားနည်းချက်ကို အသုံးပြုနိုင်မည့် အခွင့်အလမ်းကို လျော့ချပေးပါမည်။ အကယ်၍ သင်သည် အကူအညီလိုအပ်ပါက ACSC သည် အပ်ဒိတ်များနှင့် ပတ်သက်သည့် လမ်းညွှန်ချက်များကို ထုတ်ပြန်ထားပါသည်။

သင်၏ စက်ပစ္စည်း သို့မဟုတ် ဆော့ဖ်ဝဲသည် အလွန်ဟောင်းလွန်းပါက အပ်ဒိတ်များ မရရှိနိုင်ပါ။ ထုတ်လုပ်သူသည် ထုတ်ကုန်ကို အပ်ဒိတ်များဖြင့် ထောက်ပံ့ခြင်းကို ရပ်တန့်ထားပါက လုံခြုံမှုရှိစေရန် ထုတ်ကုန်အသစ်သို့ အဆင့်မြှင့်တင်ရန် စဉ်းစားသင့်သည်။ အဓိက အပ်ဒိတ်များ မရရှိတော့သော စနစ်များ ဥပမာများမှာ **iPhone 7** နှင့် **Microsoft Windows 7** ဖြစ်သည်။

ပိုမိုသိရှိလိုပါက **cyber.gov.au/updates** တွင် ရရှိနိုင်သော ကျွန်ုပ်တို့၏ အပ်ဒိတ်များနှင့်ပတ်သက်သည့် လမ်းညွှန်ချက်ကို ဖတ်ပါ။

✓ သင်၏ စက်ပစ္စည်းများနှင့် ဆော့ဖ်ဝဲများအတွက် အလိုအလျောက် အပ်ဒိတ်များကိုဖွင့်ပါ။

လုံခြုံရေး ဆော့ဖ်ဝဲကို အသုံးပြုပါ

ဗိုင်းရပ်စ်ကာဆော့ဖ်ဝဲနှင့် ငွေညှစ်ရန်ဆော့ဖ်ဝဲ ကာကွယ်မှုကဲ့သို့သော လုံခြုံရေးဆော့ဖ်ဝဲများသည်သင်၏ စက်ပစ္စည်းများကို ကာကွယ်ရန်ကူညီနိုင်သည်။

သင်၏ စက်ပစ္စည်းများမှ မောလ်ဝဲကို ရှာဖွေရန်နှင့် ဖယ်ရှားရန် လုံခြုံရေးဆော့ဖ်ဝဲကိုအသုံးပြုပါ။ ဗိုင်းရပ်စ်ကာဆော့ဖ်ဝဲများကို သံသယဖြစ်ဖွယ် ဖိုင်များနှင့် ပရိုဂရမ်များကို ပုံမှန် စကန်ဖတ်ရန် ပြင်ဆင်ထားနိုင်ပါသည်။ ခြိမ်းခြောက်မှုတစ်ခုတွေ့ရှိပါက သင်သည် သတိပေးချက်ကို လက်ခံရရှိမည်ဖြစ်ပြီး သံသယဖြစ်ဖွယ်ဖိုင်ကို သီးသန့်ခွဲထားပါမည် သို့မဟုတ် ဖယ်ရှားပါမည်။

အသေးစားစီးပွားရေးလုပ်ငန်းများစွာသည် ဗိုင်းရပ်စ်များနှင့် မောလ်ဝဲများမှ ကာကွယ်ရန် **ဝင်းဒိုးလုံခြုံရေးကို အသုံးပြုနိုင်သည်။** ဝင်းဒိုးလုံခြုံရေးကို ဝင်းဒိုး 10 နှင့် ဝင်းဒိုး 11 ကိရိယာများတွင် တစ်ပါတည်းထည့်သွင်း တည်ဆောက်ထားပြီး အခမဲ့ ဗိုင်းရပ်စ်နှင့် ခြိမ်းခြောက်မှု ကာကွယ်စောင့်ရှောက်ခြင်းလည်း ပါဝင်သည်။ သင်သည် ၎င်းကို သင်၏ စက်ပစ္စည်း ပေါ်တွင် ငွေညှစ်ဆော့ဖ်ဝဲ ကာကွယ်စောင့်ရှောက်ရေး အင်္ဂါရုပ်များကိုလည်း ဖွင့်ထားရန် အသုံးပြုနိုင်သည်။

အစားထိုးထုတ်ကုန်များနှင့် ရွေးချယ်စရာများအတွက် **cyber.gov.au** တွင် ဗိုင်းရပ်စ်ကာကွယ်ရန် ဟု ရှာဖွေခြင်းဖြင့် ကျွန်ုပ်တို့၏ ဗိုင်းရပ်စ်ကာ ဆော့ဖ်ဝဲနှင့်ပတ်သက်သည့် အကြံဉာဏ်ကို ဖတ်ပါ။

✓ သင်၏ စက်ပစ္စည်းများပေါ်တွင် ပုံမှန်စကန် ဖတ်ရန် လုံခြုံရေးဆော့ဖ်ဝဲကို သတ်မှတ်ပါ။

သင်၏ အချက်အလက်များကို အရန်သိမ်းထားပါ

ပုံမှန် အရန်သိမ်းဆည်းခြင်းသည် သင်၏ အချက်အလက်များ ပျောက်ဆုံးပါက သို့မဟုတ် ကျိုးပေါက်ပါက ပြန်လည်ရယူရန် ကူညီပေးနိုင်ပါသည်။

အရေးကြီးသောအချက်အလက်များကို အရန်သိမ်းဆည်းခြင်းသည် သင်၏ လုပ်ငန်းတွင် ပုံမှန် သို့မဟုတ် အလိုအလျောက် အလေ့အကျင့်ဖြစ်သင့်သည်။ ပုံမှန် အရန်သိမ်းဆည်းခြင်း မပြုလုပ်ထားလျှင် ဆိုက်ဘာတိုက်ခိုက်မှုတစ်ခုပြုလုပ်ခံခဲ့ရပါက သင့်အချက်အလက်များကို ပြန်လည်ရယူရန် မဖြစ်နိုင်ပါ။

သင်၏ သတင်းအချက်အလက်များကို အရန်သိမ်းဆည်းရန် သင်အသုံးပြုနိုင်သည့် နည်းလမ်းများနှင့် ထုတ်ကုန်များ စွာရှိသည်။ သင်၏ လုပ်ငန်းကို အရန်သိမ်းဆည်းထားခြင်းနှင့် ပတ်သက်သည့် အသေးစိတ်အကြံဉာဏ်များအတွက် **cyber.gov.au/backups** တွင် ရရှိနိုင်သော ကျွန်ုပ်တို့၏ အရန်သိမ်းဆည်းခြင်းများအတွက် အကြံဉာဏ်ကို ဖတ်ပါ။ အကောင်းဆုံးရွေးချယ်မှုသည် လုပ်ငန်းတစ်ခုချင်းစီအတွက် ကွဲပြားမည်ဖြစ်ရာ မသေချာပါက IT ပညာရှင်တစ်ဦးနှင့် စကားပြောပါ။

✓ သင်၏ သတင်းအချက်အလက်များကို ပုံမှန် သိမ်းဆည်းရန် အစီအစဉ်တစ်ခုကို ဖန်တီးပြီး အကောင်အထည်ဖော်ပါ။

သင်၏ ကွန်ရက်နှင့် ပြင်ပဝန်ဆောင်မှုများကို လုံခြုံအောင်လုပ်ပါ

သင်၏ ကွန်ရက်ရှိ အလားအလာရှိသော အားနည်းချက်များကို ဖြေရှင်းခြင်းဖြင့် သင်၏ စီးပွားရေးလုပ်ငန်းကို ဆိုက်ဘာတိုက်ခိုက်မှုမှ ကာကွယ်ပါ။

သင်၏ ကွန်ရက်တွင်ရှိသော စက်ပစ္စည်းများနှင့် ဝန်ဆောင်မှုများသည် ဆိုက်ဘာရာဇဝတ်သားများအတွက် အဓိက ပစ်မှတ်ဖြစ်နိုင်သည်။ ဤစနစ်များစွာသည် ဘေးကင်း လုံခြုံရန် ရှုပ်ထွေးနိုင်သည်၊ ထို့ကြောင့် အိုင်တီပညာရှင် တစ်ဦးနှင့် အောက်ပါ အကြံပြုချက်များကို ဆွေးနွေးပါ။

- **သင်၏ဆာဗာများကို လုံခြုံအောင်ထားပါ** - သင်သည် သင်၏ အိမ် သို့မဟုတ် လုပ်ငန်းတွင် NAS သို့မဟုတ် အခြားဆာဗာကို အသုံးပြုပါက ၎င်းတို့ကို လုံခြုံစေရန် ပို၍ဂရုစိုက်ပါ။ ဤကိရိယာများသည် အရေးကြီးသောဖိုင်များကို မကြာခဏ သိမ်းဆည်းထားသောကြောင့် သို့မဟုတ် အရေးကြီးသော လုပ်ဆောင်ချက်များကို လုပ်ဆောင်ရသောကြောင့် ဆိုက်ဘာရာဇဝတ်သားများအတွက် အများဆုံးပစ်မှတ်များ ဖြစ်လေ့ရှိသည်။ ဤကိရိယာများကို ကာကွယ်ရန် လျှော့ချနိုင်သည့် နည်းဗျူဟာများစွာ ရှိပါသည်။ ဥပမာအားဖြင့် မည်သည့်ဆာဗာ သို့မဟုတ် NAS ကိရိယာကိုမဆို ပုံမှန် အပ်ဒိတ်လုပ်ရန် အရေးကြီးသည်။ စီမံခန့်ခွဲမှုအကောင့်များကို ခိုင်မာသော ဝှက်စာစကားစု သို့မဟုတ် အချက်အလက်မျိုးစုံဖြင့်အတည်ပြုခြင်းဖြင့် လုံခြုံအောင် ထားသင့်သည်။
- **ပြင်ပထိတွေ့သည့်ခြေရာကို ကိုအနည်းဆုံးဖြစ်အောင်လုပ်ပါ** - သင်၏ ကွန်ရက်ပေါ်ရှိ မည်သည့် အင်တာနက်ချိတ်ဆက်ထားသော ဝန်ဆောင်မှုမဆို စစ်ဆေးပြီး လုံခြုံအောင်လုပ်ပါ။ ၎င်းတွင် Remote Desktop I File Shares I Webmail နှင့် အဝေးမှစီမံခန့်ခွဲရေး ဝန်ဆောင်မှုများပါ ဝင်နိုင်သည်။
- **ကလောက်ဒ်ဝန်ဆောင်မှုများသို့ ရွှေ့ပြောင်းပါ**- သင့်ကိုယ်ပိုင် စီမံခန့်ခွဲခြင်းအစား တစ်ပါတည်းထည့်သွင်းတည်ဆောက်ထားသည့် လုံခြုံရေးပါရှိသည့် အွန်လိုင်း သို့မဟုတ် ကလောက်ဒ်ဝန်ဆောင်မှုများကို အသုံးပြုရန် စဉ်းစားပါ။ ဥပမာ အီးမေးလ် သို့မဟုတ် ဝက်ဘ်ဆိုက် လက်ခံခြင်းကဲ့သို့သော အရာများအတွက် ကိုယ်တိုင်လည်ပတ်ပြီး လုံခြုံရေးဆောင်ရွက်မည့်အစား အွန်လိုင်းဝန်ဆောင်မှုများကို အသုံးပြုပါ။
- **သင်၏ ဝိုင်ဖိုင်စက် လုံခြုံရေးကို မြှင့်တင်ပါ** - ပုံသေ စကားဝှက်များကို အပ်ဒိတ်လုပ်ခြင်း၊ ဖောက်သည်များ သို့မဟုတ် လာရောက်သူများအတွက် "ည့်သည်" Wi - Fi ဖွင့်ခြင်းနှင့် အခိုင်မာဆုံး လျှို့ဝှက်ကုတ်လုပ်ထားသည့် ပရိုတိုကောလ်များကို အသုံးပြုခြင်းအပါအဝင် သင့် ဝိုင်ဖိုင်စက်ကို လုံခြုံစေမည့် နည်းလမ်းများနှင့် စပ်လျဉ်းသည့် ကျွန်ုပ်တို့၏ လမ်းညွှန်ချက်ကိုလိုက်နာပါ။ နောက်ထပ်အချက်အလက်များအတွက် **cyber.gov.au** တွင် ဝိုင်ဖိုင်စက်ကို ရှာပါ။
- **သင်၏ ဆိုက်ဘာထောက်ပံ့ရေး ကွင်းဆက်ကို နားလည်ပါ**- ခေတ်သစ်စီးပွားရေးလုပ်ငန်းများသည် ဝန်ဆောင်မှုများစွာကို မကြာခဏ ပြင်ပသို့အပ်နှံသည်။ ဥပမာအားဖြင့် စီမံခန့်ခွဲရေး ဝန်ဆောင်မှုပေးသူကို ၎င်းတို့၏ IT ကို ထိန်းသိမ်းစောင့်ရှောက်ရန် အသုံးပြုခြင်းဖြစ်သည်။ ဤဝန်ဆောင်မှုများ သို့မဟုတ် ဝန်ဆောင်မှုပေးသူများနှင့် လုံခြုံရေးဆိုင်ရာ ပြဿနာများသည် သင့်လုပ်ငန်းအပေါ် သိသိသာသာ သက်ရောက်မှုရှိနိုင်သည်။ ဆိုက်ဘာထောက်ပံ့ရေးကွင်းဆက် အန္တရာယ်စီမံခန့်ခွဲမှုဆိုင်ရာ အသေးစိတ်အကြံဉာဏ်များအတွက် **cyber.gov.au** တွင် ကျွန်ုပ်တို့၏ ဆိုက်ဘာထောက်ပံ့ရေး ကွင်းဆက် လမ်းညွှန်ချက်ကို ဖတ်ပါ။

✓ IT ပညာရှင်တစ်ဦးနှင့် သင့်ကွန်ရက်ကို လုံခြုံအောင်လုပ်နိုင်မည့် နည်းလမ်းများအကြောင်း ဆွေးနွေးပါ။

သင်၏ ဝက်ဘ်ဆိုက်ကို ခိုင်မာအောင်လုပ်ပါ

ဝက်ဘ်ဆိုက်များသည် ဆိုက်ဘာတိုက်ခိုက်မှုများအတွက် အဓိကပစ်မှတ် ဖြစ်သည်။

အလေ့ကပါ အခြေခံလုံခြုံရေး အစီအမံအချို့ကို လိုက်နာခြင်းဖြင့် သင်၏ ဝက်ဘ်ဆိုက်ကို လုယူခံရခြင်းမှ ကာကွယ်ပါ-

- အချက်အလက်မျိုးစုံဖြင့်အတည်ပြုခြင်း သို့မဟုတ် ခိုင်မာသောစကားဝှက်နှင့်အတူ သင်၏ဝက်ဘ် ဆိုက်ထဲသို့ ဝင်ခြင်းကို လုပ်ခြုံအောင်လုပ်ပါ
- သင့် ဝက်ဘ်ဆိုက်၏ အကြောင်းအရာ စီမံခန့်ခွဲမှုစနစ်များနှင့် ထပ်တိုးဆော့ဖ်ဝဲအစိတ်အပိုင်းများကို ပုံမှန်အပ်ဒိတ်လုပ်ပါ
- ဆိုက်ဘာတိုက်ခိုက်ခံရပြီးနောက် သင့်ဝတ်ဆိုက်ကို ပြန်လည်ရယူနိုင်စေရန် ၎င်းကိုပုံမှန် အရန်သိမ်းဆည်းပါ။

ဝက်ဘ်ဆိုက်ပိုင်ရှင်များအတွက် ACSC တွင် ထပ်ဆောင်း ရင်းမြစ်များရှိသည်။ ဤရင်းမြစ်များကို **cyber.gov.au** တွင် ရှာဖွေပါ -

- သင့်ဝက်ဘ်ဆိုက် အတွက် Quick Wins
- Implementing Certificates, TLS, HTTPS နှင့် Opportunistic TLS
- ဒိုမိန်းပိုင်ရှင်များအတွက် ဒိုမိန်းအမည်စနစ်လုံခြုံရေး
- ဝန်ဆောင်မှုငြင်းပယ်ခြင်း တိုက်ခိုက်မှုများအတွက် ကြိုတင်ပြင်ဆင်ခြင်းနှင့် တုံ့ပြန်ခြင်း

✓ ဝက်ဘ်ဆိုက်လုံခြုံရေးနှင့်စပ်လျဉ်း၍ ACSC ရင်းမြစ်များတွင် ဖတ်ပါ

သင့်စက်ပစ္စည်းများကို မရောင်းမီ သို့မဟုတ် မစွန့်ပစ်မီ ပြန်လည်သတ်မှတ်ပါ

သင်၏ စက်ပစ္စည်းဟောင်းများရှိ အချက်အလက်များကို လူစိမ်းများမှ ရယူကြည့်ရှုနိုင်ပါသည်။

အကယ်၍ သင်၏ စက်ပစ္စည်းများကို လုံခြုံစွာ မစွန့်ပစ်ထားပါက ဆိုက်ဘာရာဇဝတ်သားများသည် ၎င်း ၏ အချက်အလက်များကို ရယူနိုင်သည်။ ၎င်းတွင်အီးမေးလ်များ၊ ဖိုင်များနှင့် အခြားလုပ်ငန်းဆိုင်ရာ အချက်အလက်များ ပါဝင်နိုင်သည်။ ရောင်းချခြင်း၊ လဲလှယ်ခြင်း သို့မဟုတ် လွှင့်ပစ်ခြင်း မပြုမီ သင်၏ လုပ်ငန်းသုံးစက်ကိရိယာများမှ သတင်းအချက်အလက်အားလုံးကို ဖယ်ရှားပါ။ ဥပမာအားဖြင့် မူလဝယ်စဉ်ကအတိုင်း ပြန်လည်သတ်မှတ်ခြင်းတို့ဖြစ်သည်။ ၎င်းသည် မည်သည့် သတင်းအချက်အလက်ကိုမဆို ရှင်းပစ်ရန်နှင့် ၎င်း၏ မူလ ဆက်တင်များကို ပြန်လည်ထားရှိရန် ကူညီပေးနိုင်ပါသည်။

သင်၏ စက်ကိရိယာများကို ပြန်လည်သတ်မှတ်ရန်နှင့်စပ်လျဉ်းသည့် အကြံဉာဏ်အတွက် သင်၏ စက်ကိရိယာကို ဘေးကင်းလုံခြုံစွာ မည်သို့စွန့်ပစ်ရမည်နှင့်ပတ်သက်၍ ကျွန်ုပ်တို့၏ လမ်းညွှန်ချက်ကို ဖတ်ပါ။ **cyber.gov.au** တွင် စွန့်ပစ်မည်ကို ရှာဖွေပါ။

✓ လုပ်ငန်းသုံး စက်ပစ္စည်းများကို ရောင်းချခြင်း သို့မဟုတ် စွန့်ပစ်ခြင်းမပြုမီ မူလဝယ်စဉ်က အတိုင်း ပြန်လည်သတ်မှတ်ပါ။

သင်၏ စက်ကိရိယာများကို လော့ခ်ချပြီး ရုပ်ပိုင်းဆိုင်ရာ အရ လုံခြုံအောင်ထားပါ

သင်၏ လုပ်ငန်းသုံး စက်ပစ္စည်းများသို့ ဝင်ရောက်ခွင့်ကို ကန့်သတ်ခြင်းသည် အန္တရာယ်ရှိသော လှုပ်ရှားမှုများ အတွက် အခွင့်အလမ်းများကို လျော့ချပေးသည်။

သင်၏ လုပ်ငန်းသုံး စက်ပစ္စည်းများသို့ ရုပ်ပိုင်းဆိုင်ရာ ဝင်ရောက်မှုကို ကန့်သတ်ခြင်းသည် ဒေတာခိုးယူခံရခြင်း သို့မဟုတ် အခြားအန္တရာယ်ရှိသော လှုပ်ရှားမှုများကို ကာကွယ်ရန် ရိုးရှင်းသောနည်းလမ်းတစ်ခုဖြစ်သည်။ လုပ်ငန်းသုံး စက်ပစ္စည်းများကို ခွင့်ပြုချက်မရှိသော ဝန်ထမ်းများ သို့မဟုတ် အများပြည်သူများ ဝင်ရောက်ကြည့်ရှုနိုင်သည့်နေရာတွင် မထားသင့်ပါ။

သင်၏ လုပ်ငန်းသုံး စက်ပစ္စည်းများကို ပိုမိုကာကွယ်ရန် လုံခြုံရေးထိန်းချုပ်မှုများကို အသုံးပြုပါ။ အနည်းဆုံးအားဖြင့် ၎င်းတို့ကို ဖွက်စာစကားစု၊ PIN သို့မဟုတ် ဇီဝအချက်အလက်များဖြင့် လော့ခ်ချထားသင့်သည်။ ဤကိရိယာများကို အသုံးမပြုပါက အချိန်အနည်းငယ်ကြာပြီးနောက် အလိုအလျောက် လော့ခ်ချစေရန် သတ်မှတ်ထားကြောင်း သေချာပါစေ။

✓ **ကိရိယာများကို အသုံးမပြုပါက အချိန်အနည်းငယ်ကြာပြီးနောက် အလိုအလျောက် လော့ခ်ချစေရန် သတ်မှတ်ပါ။**

သင့် စီးပွားရေးဆိုင်ရာ အချက်အလက်များကို ကာကွယ်ပါ

သင့်လုပ်ငန်းမှ ထိန်းသိမ်းထားသော အချက်အလက်များသည် ဆိုက်ဘာရာဇဝတ်သားများအတွက် ဆွဲဆောင်နိုင်သည့် ပစ်မှတ်တစ်ခုဖြစ်သည်။

ဒေတာကျိုးပေါက်မှုများ မြင့်တက်လာနေပါသည်- သင့်လုပ်ငန်းကို သားကောင်အဖြစ်အကျမခံပါနှင့်။ သင့်လုပ်ငန်းက မည်သည့်အချက်အလက်များကို မည်သည့်နေရာတွင် ထားရှိသည်ကို နားလည်ရန် အရေးကြီးသည်။ သင်သိရှိလျှင် ဤလမ်းညွှန်တွင်ဖော်ပြထားသော အကြံပြုချက်များကို အသုံးပြု၍ သင်၏ အချက်အလက်များကို ဆိုက်ဘာရာဇဝတ်သားများ ဝင်ရောက်ရယူခြင်းမှ ကာကွယ်ရန် ကူညီပါ။ အချို့သော စီးပွားရေးလုပ်ငန်းများသည် ဥပဒေအရ နောက်ထပ် တာဝန်ဝတ္တရားများလည်း ရှိနိုင်သည်။

- **သင်၏စီးပွားရေးဆိုင်ရာ အချက်အလက်များကို စုစည်းပါ။** သင်သည် စက်ပစ္စည်း သို့မဟုတ် ဝန်ဆောင်မှုများစွာတွင် သိမ်းဆည်းထားသော အချက်အလက်များရှိနိုင်သည်။ အချက်အလက်များကို ဗဟိုချုပ်ကိုင်မှုမထားဘဲ ထိန်းသိမ်းသည့်အခါ သင် လုံခြုံအောင်ထားပြီး အရန်သိမ်းဆည်းရမည့် စနစ်အရေအတွက် တိုးလာသည်။ များစွာသော စနစ်များသည် ဆိုက်ဘာရာဇဝတ်သားများအတွက် တိုက်ခိုက်နိုင်ရန် အခွင့်အလမ်းများစွာကို လည်း ဖန်တီးပေးနိုင်သည်။ ဖြစ်နိုင်လျှင် သင့်လုပ်ငန်း အချက်အလက်များကို ဘေးကင်းလုံခြုံပြီး ပုံမှန် အရန်သိမ်းဆည်းထားသည့် ဗဟိုနေရာတွင် သိမ်းဆည်းပါ။ သင်၏ ဒေတာများကို ဗဟိုမှထိန်းချုပ်ခြင်းသည် သင်၏ စနစ်များ ကျိုးပေါက်ခဲ့ပါက ပိုမိုကြီးမားသော ကျိုးပေါက်မှုတစ်ခု ဖြစ်လာနိုင်ပါသည်။ ထို့ကြောင့် ဤဗဟိုတည်နေရာကို လုံခြုံသော အပြင်အဆင်များနှင့် ကန့်သတ်ထားသော ဝင်ရောက်မှုများဖြင့် လုံလောက်စွာ ကာကွယ်ထားကြောင်း သေချာပါစေ။ အကြံဉာဏ်ရယူရန် IT သို့မဟုတ် ဆိုက်ဘာလုံခြုံရေး ပညာရှင်တစ်ဦးနှင့် စကားပြောပါ။

- **အချက်အလက်များကို အကာအကွယ်ပေးရန် သင်၏ တာဝန်ဝတ္တရားများကို သိရှိပါ။** အချို့သော အသေးစား စီးပွားရေး လုပ်ငန်းများသည် ၎င်းတို့ စုဆောင်းထားသော ပုဂ္ဂိုလ်ရေးအချက်အလက်များကို ကိုင်တွယ်ရန် ဥပဒေရေးရာတာဝန်ရှိနိုင်သည်။ ပိုမိုလေ့လာရန် **oaic.gov.au** တွင် ရရှိနိုင်သော ဩစတြေးလျ သတင်းအချက်အလက် ကော်မရှင်ရုံး၏ အသေးစားစီးပွားရေးလုပ်ငန်းများအတွက် လမ်းညွှန်ကို ဖတ်ပါ။ အကယ်၍ မသေချာပါက ဥပဒေပညာရှင်တစ်ဦးနှင့် တိုင်ပင်ပါ။

✓ **သင်၏ လုပ်ငန်းက ထိန်းသိမ်းထားသော အချက်အလက်များကို နားလည်ထားပြီး ၎င်းကို ကာကွယ်ရန်မှာ သင့်တာဝန်ဖြစ်သည်။**

သင်၏ဝန်ထမ်းများကို ပြင်ဆင်ပေးပါ

ဝန်ထမ်းများအား ပညာပေးခြင်း

ဆိုက်ဘာလုံခြုံရေး အလေ့အကျင့်ကောင်းရှိသော ဝန်ထမ်းများသည် ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများမှ သင့်အား ပထမဆုံး ကာကွယ်စောင့်ရှောက်ပေးမည်ဖြစ်သည်။

သင်၏ ဝန်ထမ်းများသည် အောက်ပါအကြောင်းအရာများ အပါအဝင် ဆိုက်ဘာလုံခြုံရေးနှင့် ပတ်သက်၍ သိရှိထားရမည်-

- လုပ်ငန်းအီးမေးလ် ကျိုးပေါက်မှုနှင့် ငွေညှစ်ရန်ဆော့ဖ်ဝဲကဲ့သို့ တွေ့ရများသည့် ဆိုက်ဘာလုံခြုံရေး ခြိမ်းခြောက်မှုများ
- ခိုင်မာသော စကားဝှက်များ သို့မဟုတ် ဝှက်စာ စကားလုံးများ၊ MFA နှင့်ဆော့ဖ်ဝဲအပ်ဒိတ်များ အပါအဝင် အကာအကွယ်ပေးသည့်အစီအမံများ
- အလိမ်အညာမက်ဆေ့ချ်များနှင့် လျှို့ဝှက် အချက်အလက်ခိုးယူ တိုက်ခိုက်မှုများကို ရှာဖွေပုံ
- စီးပွားရေးဆိုင်ရာ တိကျသော မူဝါဒများ (ဥပမာ - သံသယဖြစ်ဖွယ် အီးမေးလ်များကို အစီရင်ခံခြင်း၊ သို့မဟုတ် ငွေတောင်းခံလွှာများကို မပေးချေမီ မှန်ကန်ကြောင်းအတည်ပြုခြင်းအတွက် လုပ်ငန်းစဉ်များ)
- အရေးပေါ်အခြေအနေတစ်ခုတွင် ဘာလုပ်ရမည်နည်း။

ACSC ဝက်ဘ်ဆိုက် cyber.gov.au/learn တွင် ဤအကြောင်းအရာအများစုအတွက် ရင်းမြစ်များရှိသည်။ သင်သည် သင်၏ ဝန်ထမ်းများအား အသိပညာပေးရန် အခြားနည်းလမ်းများကို စဉ်းစားနိုင်သည်၊ ဥပမာအားဖြင့် တရားဝင် သင်တန်း သို့မဟုတ် လုပ်ငန်းတွင်းသင်တန်းမျိုး ဖြစ်သည်။ သို့သော် သင်ဆုံးဖြတ်ပြီးပါက ဆိုက်ဘာလုံခြုံရေးသင်တန်းသည် တစ်ကြိမ်သာ လိုအပ်သည့် လိုအပ်ချက်မဟုတ်ကြောင်းနှင့် အခါအားလျော်စွာ မွမ်းမံသင့်သည်ကို အမှတ်ရပါ။

✓ **ဆိုက်ဘာလုံခြုံရေး သတိရှိမှုကို သင့် လုပ်ငန်းတွင် မည်သို့သင်ကြားပေးမည်ကို ဆုံးဖြတ်ပါ။**

အရေးပေါ်အစီအစဉ်တစ်ခု ပြုလုပ်ပါ

အရေးပေါ်အစီအစဉ်သည် သင့်လုပ်ငန်း ဆိုက်ဘာတိုက်ခိုက်ခံရမှု၏ အကျိုးသက်ရောက်မှုကို လျှော့ချနိုင်သည်။

Cyber လုံခြုံရေးပြဿနာတစ်ခုကို တုံ့ပြန်သည့်အခါ မိနစ်တိုင်းသည် အရေးကြီးပါသည်။ အရေးပေါ်အစီအစဉ် တစ်ခုရှိခြင်းသည် သင်၏ ဝန်ထမ်းများအနေဖြင့် မည်သို့ပြုလုပ်ရမည်ကို စဉ်းစားရမည့် အချိန်ပိုနည်းသွား နိုင်ပြီး လုပ်ဆောင်ရန် အချိန်ပိုရလာနိုင်သည်။

သင်၏ အရေးပေါ်အစီအစဉ်ကို ဖန်တီးသောအခါ အောက်ပါမေးခွန်းများကို စဉ်းစားပါ-

- အလားအလာရှိသော ဆိုက်ဘာလုံခြုံရေး ဖြစ်ရပ်များကို သတင်းပို့ရန် သင့်ဝန်ထမ်းများ အတွက် လုပ်ငန်းစဉ်က အဘယ်နည်း။
- အကူအညီအတွက် မည်သူ့ကို ဆက်သွယ်ပါသလဲ။ ဥပမာ - IT ပညာရှင်များနှင့် သင့်ဘဏ်။
- အဖြစ်အပျက်ကို သင်၏ ဝန်ထမ်းများ၊ ပါဝင်ပတ်သက်သူများ သို့မဟုတ် ဖောက်သည်များအား မည်သို့ဆက်သွယ်ပြောပြမည်နည်း။
- အရေးကြီးသောစနစ်များ အော့ဖ်လိုင်းဖြစ်နေပါက ပုံမှန် အတိုင်း လုပ်ငန်းကို သင်မည်သို့ စီမံခန့်ခွဲမည်နည်း။

သင် ဝန်ထမ်းများသည် ၎င်းတို့တွင်ရှိသည့် အခန်းကဏ္ဍများ သို့မဟုတ် တာဝန်ဝတ္တရားများ အပါအဝင် အရေးပေါ် အစီအစဉ်နှင့် အကျွမ်းတဝင်ရှိကြောင်း သေချာပါစေ။ သင်၏ စနစ်များ အော့ဖ်လိုင်းဖြစ်နေချိန်တွင် သင်လိုအပ်ခဲ့ပါကရရှိနိုင်ရန် အစီအစဉ်ကို စာရွက်မိတ္တူတစ်စောင်ထားပါ။

✓ **ဆိုက်ဘာလုံခြုံရေး ဖြစ်ရပ်များအတွက် အရေးပေါ်အစီအစဉ်တစ်ခုကို ဖန်တီးပါ**

အမြဲသိရှိနေပါ

ACSC မှ နောက်ဆုံးရအချက်အလက်များကို လက်ခံရန် ACSC ၏ မိတ်ဖက်တစ်ဦးဖြစ်လာပါ။

ACSC မိတ်ဖက်ဖြစ်လာခြင်းအားဖြင့် နောက်ဆုံးပေါ် ဆိုက်ဘာခြိမ်းခြောက်မှုများနှင့် အားနည်းချက်များအကြောင်း အမြဲသိရှိနေပါ။ ဤဝန်ဆောင်မှုသည် ဆိုက်ဘာခြိမ်းခြောက်မှုအသစ်တစ်ခုကို ဖော်ထုတ်သိရှိသည့်အခါ လစဉ် သတင်းလွှာများနှင့် သတိပေးချက်များပေးလိမ့်မည်။

ဆိုက်ဘာလုံခြုံရေးသည် အလျင်အမြန် ပြောင်းလဲနေသော နယ်ပယ်တစ်ခုဖြစ်သည်။ ဆိုက်ဘာရာဇဝတ်သားများသည် ၎င်းတို့၏ ရှာဖွေတွေ့ရှိပြီး မိနစ်အနည်းငယ်အတွင်း အားနည်းချက်များကို တက်ကြွစွာ အမြတ်ထုတ်လေ့ရှိကြသည်။

ဆိုက်ဘာလုံခြုံရေးအခြေအနေကို သိရှိနေခြင်းသည် သင်၏ လုပ်ငန်း ရင်ဆိုင်ရနိုင်သည့် အန္တရာယ်များနှင့် ၎င်းတို့ကို မည်သို့ကာကွယ်ရမည်ကို နားလည်ရန် ကူညီလိမ့်မည်။

✓ **သင့်လုပ်ငန်းကို ACSC မိတ်ဖက်အစီအစဉ်တွင် မှတ်ပုံတင်ပါ။**

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်
ဤလမ်းညွှန်တွင် ပါဝင်သော အချက်အလက်များသည် ယေဘုယျသဘောသဘာဝဖြစ်ပြီး တရားဝင်အကြံဉာဏ်အဖြစ် မမှတ်ယူသင့်ပါ သို့မဟုတ် သီးသန့်အခြေအနေ သို့မဟုတ် အရေးပေါ်အခြေအနေတစ်ခုခုတွင် အကူအညီအတွက် မမှီခိုသင့်ပါ။ အရေးကြီးသော ကိစ္စရပ်တစ်ခုခုတွင် သင်၏ ကိုယ်ပိုင်အခြေအနေများနှင့် ပတ်သက်၍ သင့်လျော်သော သီးခြားလွတ်လပ်သည့် ပညာရှင်တစ်ဦး၏ အကြံဉာဏ်ကို ရယူသင့်သည်။

ဤလမ်းညွှန်တွင် ပါဝင်သော သတင်းအချက်အလက်များအပေါ် မှီခိုမှု၏ ရလဒ်အနေဖြင့် ပျက်စီးမှု၊ ဆုံးရှုံးမှု သို့မဟုတ် ကုန်ကျစရိတ်အတွက် နိုင်ငံတော်သည် တာဝန် သို့မဟုတ် ပေးဆပ်ရမည့်တာဝန်ကို လက်ခံမည်မဟုတ်ပါ။

ပိုမိုသိရှိလိုပါက သို့မဟုတ် ဆိုက်ဘာလုံခြုံရေး ဖြစ်ရပ်တစ်ခုကို သတင်းပို့ရန် ကျွန်ုပ်တို့ထံ ဆက်သွယ်ပါ-
cyber.gov.au | 1300 CYBER1 (1300 292 371)

ဤနံပါတ်ကို ဩစတြေးလျနိုင်ငံအတွင်းသာ အသုံးပြုနိုင်ပါသည်။

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre