എപ്പോഴും സ്വീകരിക്കേണ്ട ഒമ്പത് അത്യാവശ്യ സൈബർ സുരക്ഷാ ശീലങ്ങൾ

1. ക്ലിക്ക് ചെയ്യുന്നതിന് മുമ്പ് ഒരു നിമിഷം ശ്രദ്ധിക്കൂ!

താങ്കൾക്ക് അറിയാവുന്ന വ്യക്തി / സോഴ്സിൽ നിന്നാണെന്ന് ബോധ്യമുണ്ടെങ്കിലും, ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യുന്നതിനു മുമ്പ് രണ്ടു തവണ ചിന്തിക്കൂ.

- അജ്ഞാത ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യുന്നതിന് പകരം, വെബ്സൈറ്റുകളിലേക്ക് അറിയപ്പെടുന്ന, നിയമാനുസൃതമായ (ഉദാ. HTTPS) ഒരു ഉറവിടത്തിലൂടെ എല്ലായ്പ്പോഴും പ്രവേശിക്കുക.
- അപ്രതീക്ഷിതമായി ഒരു അറ്റാച്ച്മെന്റ് കണ്ടാൽ, വിശ്വസനീയമായ ഒരു രീതി ഉപയോഗിച്ച് അയച്ചയാളിലൂടെ അതു സ്ഥിരീകരിക്കുക, അല്ലെങ്കിൽ സുരക്ഷിതരായിരിക്കാനായി ആ അറ്റാച്ച്മെന്റിൽ ക്ലിക്ക് ചെയ്യാതിരിക്കുക.

2. വ്യക്തിഗത വിവരങ്ങൾക്കായുള്ള അഭ്യർത്ഥനകൾ പരിശോധിക്കുക.

താങ്കളുടേതോ മറ്റാരുടേതെങ്കിലുമോ സ്വകാര്യ വിവരങ്ങൾ ആവശ്യപ്പെട്ടുള്ള അഭ്യർത്ഥനകൾ എപ്പോഴും സ്ഥിരീകരിക്കുക.

- തട്ടിപ്പുകാർക്ക് വിശ്വസനീയ കോൺടാക്റ്റുകൾ എന്ന രീതിയിൽ എളുപ്പത്തിൽ ആൾമാറാട്ടം നടത്താനാകും.
- അസാധാരണമായ പ്രവർത്തികൾ കണ്ടെത്താനായി സാമ്പത്തിക സ്റ്റേറ്റുമെന്റുകളും, ക്രെഡിറ്റ് റിപ്പോർട്ടുകളും പതിവായി പരിശോധിക്കുക.
- പല ഫിഷിംഗ് സന്ദേശങ്ങളിലും അക്ഷരപ്പിശകുകളും, വ്യാകരണ പിശകുകളും അടങ്ങിയിട്ടുണ്ടാകും.
- അഭ്യർത്ഥന നിയമാനുസൃതമാണോ എന്ന് പരിശോധിക്കുക. ആ വ്യക്തിക്കോ, സ്ഥാപനത്തിനോ നമ്മുടെ 'ആ വിവരം' ആവശ്യമായി വരാൻ സാധ്യതയുണ്ടോ? എന്ന കാര്യവും പരിശോധിക്കുക.

3. താങ്കളുടെ പാസ്‌വേഡുകൾ നിയന്ത്രിക്കുക

താങ്കളുടെ അക്കൗണ്ടുകൾ സുരക്ഷിതമായി സൂക്ഷിക്കുന്നതിന് ശക്തവും, സങ്കീർണ്ണവുമായ പാസ്‌വേഡുകൾ സൃഷ്ടിക്കുകയും അവ വിവേകത്തോടെ കൈകാര്യം ചെയ്യുകയും ചെയ്യേണ്ടത് അത്യാവശ്യമാണ്.

- വ്യത്യസ്ത അക്കൗണ്ടുകൾക്കായി വെവ്വേറെ പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക.
- ജോലി ആവശ്യത്തിനും, വ്യക്തിഗത ആവശ്യങ്ങൾക്കും വെവ്വേറെ പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക.
- ഒരിക്കലും പാസ്‌വേഡുകൾ പങ്കിടരുത്.
- പാസ്‌വേഡ് ഇടയ്ക്കിടെ മാറ്റുക.
- ബ്രൗസറുകളിൽ പാസ്‌വേഡുകൾ സേവ് ചെയ്യുന്നത് ഒഴിവാക്കുക.
- അധിക സുരക്ഷയ്ക്കായി മൾട്ടി-ഫാക്ടർ ഓതന്റിക്കേഷൻ പ്രവർത്തനക്ഷമമാക്കുക.

4. താങ്കളുടെ ഉപകരണങ്ങൾ സുരക്ഷിതമാക്കുക

പുറത്തുപോകുമ്പോൾ താങ്കളുടെ വർക്ക്സ്പെയ്സ് ലോക്ക് ചെയ്ത് ഉപകരണങ്ങൾ സംരക്ഷിക്കുക.

- താങ്കളുടെ കമ്പ്യൂട്ടർ സ്ക്രീൻ എപ്പോഴും ലോക്ക് ചെയ്യുക.
- താങ്കളുടെ ഫോണും, പോർട്ടബിൾ ഉപകരണങ്ങളും എപ്പോഴും താങ്കളോടൊപ്പം സൂക്ഷിക്കുക, അല്ലെങ്കിൽ സുരക്ഷിതമായി സൂക്ഷിക്കുക.
- സാധ്യമാകുമ്പോഴെല്ലാം ശക്തമായ ഓതന്റിക്കേഷൻ രീതികൾ ഉപയോഗിക്കുക.

5. പ്രധാനപ്പെട്ട ഫയലുകൾ ബാക്കപ്പ് ചെയ്യുക

താങ്കളുടെ സുപ്രധാന ഡാറ്റകൾ പതിവായി ബാക്കപ്പ് ചെയ്യുന്നുണ്ടെന്ന് ഉറപ്പാക്കുക.

- ബാക്കപ്പുകൾ പ്രത്യേകമായി സൂക്ഷിക്കുക.
- താങ്കളുടെ സ്ഥാപനം അംഗീകരിച്ചിട്ടുള്ള സ്റ്റോറേജ് സൊല്യൂഷനുകൾ ഉപയോഗിക്കുക.
- ശരിയായി പ്രവർത്തിക്കുന്നുണ്ടെന്ന് ഉറപ്പാക്കാൻ ബാക്കപ്പുകൾ പതിവായി പരിശോധിക്കുക.

6. സംശയാസ്പദമായ പ്രവർത്തനങ്ങൾ റിപ്പോർട്ട് ചെയ്യുക.

എന്തെങ്കിലും സംശയാസ്പദമായി തോന്നുകയാണെങ്കിൽ, താങ്കളുടെ ബുദ്ധിയെ വിശ്വസിക്കുക-അത് റിപ്പോർട്ട് ചെയ്യുക!

- തട്ടിപ്പുകൾ, സംശയാസ്പദമായ പ്രവർത്തനങ്ങൾ എന്നിവ ശ്രദ്ധയിൽപെട്ടാൽ, താങ്കളുടെ സൂപ്പർവൈസർക്ക് മുന്നറിയിപ്പ് നൽകുകയും, താങ്കളുടെ സ്ഥാപനത്തിന്റെ റിപ്പോർട്ടിംഗ് പ്രോട്ടോക്കോൾ അനുസരിച്ച് പ്രവർത്തിക്കുകയും ചെയ്യുക.

7. സ്വയം പഠിക്കുകയും, മറ്റുള്ളവരെ പഠിപ്പിക്കുകയും ചെയ്യുക.

ഏറ്റവും പുതിയ സൈബർ സുരക്ഷാ ഭീഷണികളെയും, ട്രെൻഡുകളെയും കുറിച്ച് അറിഞ്ഞിരിക്കുക.

- താങ്കൾക്ക് അവസരം ലഭിക്കുമ്പോൾ പരിശീലന പരിപാടികളിൽ പങ്കെടുക്കുകയും, സഹപ്രവർത്തകരുമായി അറിവ് പങ്കിടുകയും ചെയ്യുക.
- നല്ല അറിവുള്ള ഒരു ടീം, സൈബർ ഭീഷണികൾക്കെതിരായ താങ്കളുടെ ആദ്യ പ്രതിരോധ നിരയാണ്.

8. സുരക്ഷിത നെറ്റ്‌വർക്കുകൾ ഉപയോഗിക്കുക

എല്ലായ്പ്പോഴും, പ്രത്യേകിച്ചും സെൻസിറ്റീവ് വിവരങ്ങൾ ആക്സസ് ചെയ്യുമ്പോൾ, സുരക്ഷിത നെറ്റ്‌വർക്കുകളിലേക്ക് കണക്റ്റു ചെയ്യു.

- സാമ്പത്തിക ഇടപാടുകൾ ചെയ്യുമ്പോഴും, സെൻസിറ്റീവ് ജോലികൾ ചെയ്യുമ്പോഴും പൊതു വൈഫൈ ഒഴിവാക്കുക.
- കൂടുതൽ സുരക്ഷിതത്വത്തിനായി, ആവശ്യമുള്ളപ്പോൾ ഒരു വെർച്വൽ പ്രൈവറ്റ് നെറ്റ്‌വർക്ക് (VPN) ഉപയോഗിക്കുക.

9. സോഷ്യൽ മീഡിയയിൽ ജാഗ്രത പാലിക്കുക

താങ്കൾ ഓൺലൈനിൽ പങ്കിടുന്ന വ്യക്തിഗത വിവരങ്ങൾ നിയന്ത്രിക്കുക. അപ്പോൾ താങ്കൾക്ക് സ്വകാര്യത പരിരക്ഷിക്കാനും, സുരക്ഷ വർദ്ധിപ്പിക്കാനും, കൂടുതൽ മികച്ച ഓൺലൈൻ അനുഭവം സൃഷ്ടിക്കാനും കഴിയും.

- സോഷ്യൽ മീഡിയ പ്ലാറ്റ്ഫോമുകളിലെ സ്വകാര്യതാ ക്രമീകരണങ്ങൾ പരിശോധിക്കുക.
- സൗഹൃദ അഭ്യർത്ഥനകളും, താങ്കളുടെ വിവരങ്ങളിലേക്ക് ആക്സസ് ഉള്ളവരെയും ശ്രദ്ധിക്കുക; ലോക്ക് ചെയ്തിട്ടുള്ള പ്രൊഫൈലുകളിൽ നിന്നുള്ള അഭ്യർത്ഥനകൾ സ്വീകരിക്കരുത്.
- അപകടസാധ്യതകൾ കുറയ്ക്കുന്നതിനായി താങ്കളുടെ ഓൺലൈൻ സാന്നിധ്യം പതിവായി പരിശോധിക്കുക.

ഓർക്കുക: സൈബർ സുരക്ഷ എല്ലാവരുടെയും ഉത്തരവാദിത്വമാണ് !