എന്താണ് ഫിഷിംഗ് ?

സ്വകാര്യ വിവരങ്ങൾ വെളിപ്പെടുത്തുന്നതിനോ ransomware പോലുള്ള മാൽവെയർ ഇൻസ്റ്റാൾ ചെയ്യുന്നതിനോ ഹാക്കർസ് ആളുകളെ വഞ്ചിക്കുന്ന സോഷ്യൽ എഞ്ചിനീയറിംഗിന്റെ ഒരു രൂപമാണ് **ഫിഷിംഗ്**.ടാർഗറ്റ് ചെയ്ത വ്യക്തിയുടെ താല്പര്യം മനസിലാക്കി അതിനനുസരിച്ചുള്ള വ്യാജ വെബ്സൈറ്റ് നിർമിക്കുകയും ഇമെയിൽ വഴിയോ അതുപോലുള്ള മറ്റു വഴികളിലൂടെ ടാർഗറ്റ് ആക്കിയിട്ടുള്ള വ്യക്തിക്ക് ഹാക്കർ വെബ്സൈറ്റ് ലിങ്ക് അയക്കുകയും ചെയ്യുന്നു.2020-ലെ കണക്കനുസരിച്ച്, ഇത് ഏറ്റവും കൂടുതൽ കണ്ടു വന്ന സൈബർ കുറ്റകൃത്യമാണ്, എഫ്ബിഐയുടെ ഇന്റർനെറ്റ് ക്രൈം കംപ്ലയിന്റ് സെന്റർ മറ്റേതൊരു തരത്തിലുള്ള കമ്പ്യൂട്ടർ കുറ്റകൃത്യങ്ങളേക്കാളും കൂടുതൽ ഫിഷിംഗ് സംഭവങ്ങൾ റിപ്പോർട്ട് ചെയ്യുന്നു.

"ഫിഷിംഗ്" എന്ന പദം ആദ്യമായി രേഖപ്പെടുത്തിയത് 1995-ൽ ക്രാക്കിംഗ് ടൂൾകിറ്റ് **AOHell** ലാണ്, എന്നാൽ നേരത്തെ 2600 എന്ന ഹാക്കർ മാഗസിനിൽ ഇത് ഉപയോഗിച്ചിരിക്കാം. ഇത് മത്സ്യബന്ധനത്തിന്റെ ഒരു വ്യതിയാനമാണ്, കൂടാതെ സെൻസിറ്റീവ് വിവരങ്ങൾക്കായി "മത്സ്യം" എന്നതിലേക്ക് ആകർഷിക്കുന്നതിനെ സൂചിപ്പിക്കുന്നു.

ഫിഷിംഗ് ചില ഉദാഹരണം :-

ഇമെയിൽ ഫിഷിംഗ്

ഫിഷിംഗ് ആക്രമണങ്ങൾ, പലപ്പോഴും ഇമെയിൽ സ്പാം വഴി വിതരണം ചെയ്യുന്നു.സ്വകാര്യ വിവരങ്ങൾ നൽകാനോ ലോഗിൻ വിവരങ്ങൾ നൽകാനോ വ്യക്തികളോട് പറഞ്ഞു കബളിപ്പിക്കാൻ ശ്രമിക്കുന്നു. മിക്ക ആക്രമണങ്ങളും "ബൾക്ക് അറ്റാക്കുകൾ" ആണ്(ടാർഗെറ്റ് ചെയ്യപ്പെടാത്തവയാണ്).വൻതോതിൽ റാൻഡം ആയി എല്ലാവരിലേക്കും അയക്കുന്നു .സാമ്പത്തിക സ്ഥാപനങ്ങൾ, ഇമെയിൽ, ക്ലൗഡ് ഉൽപ്പാദനക്ഷമത ദാതാക്കൾ, സ്ട്രീമിംഗ് സേവനങ്ങൾ എന്നിവയുൾപ്പെടെയുള്ള പൊതുവായ ലക്ഷ്യങ്ങൾ ഉപയോഗിച്ച് ഹാക്കരുടെ ലക്ഷ്യം വ്യത്യാസപ്പെടാം.മോഷ്ടിച്ച വിവരങ്ങളും ആക്സസുകളും പണം മോഷ്ടിക്കാനും മാൽവെയർ ഇൻസ്റ്റാൾ ചെയ്യാനും ടാർഗെറ്റ് ഓർഗനൈസേഷനിൽ മറ്റുള്ളവരെ ഫിഷ് ചെയ്യാനും

ഉപയോഗിച്ചേക്കാം.മോഷ്ട്ടിച്ച സ്ട്രീമിംഗ് സേവന അക്കൗണ്ടുകൾ ഡാർക്ക്നെറ്റ് മാർക്കറ്റുകളിലും വിൽക്കപ്പെടാം.

സ്പിയർ ഫിഷിംഗ്

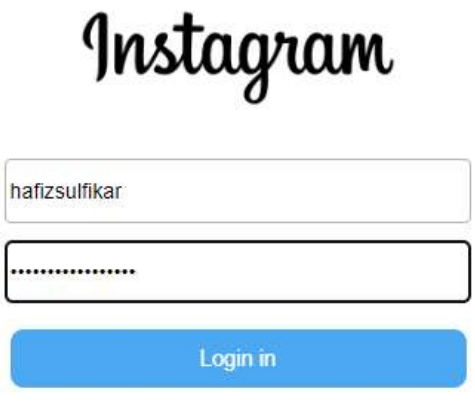
ഒരു പ്രത്യേക വ്യക്തിയെയോ സ്ഥാപനത്തെയോ കബളിപ്പിച്ച് അവ നിയമാനുസൃതമാണെന്ന് വിശ്വസിക്കാൻ വ്യക്തിഗതമാക്കിയ ഇമെയിലുകൾ ഉപയോഗിക്കുന്ന ഒരു ടാർഗെറ്റഡ് ഫിഷിംഗ് ആക്രമണമാണ്. വിജയസാധ്യത വർദ്ധിപ്പിക്കുന്നതിന് അവതരിപ്പിക്കുന്ന കാര്യത്തിന്റെ ഒർജിനൽ വ്യക്തിഗത വിവരങ്ങൾ ഉപയോഗിക്കുന്നു.സെൻസിറ്റീവ് ഫിനാൻഷ്യൽ ഡാറ്റയിലേക്കും സേവനങ്ങളിലേക്കും ആക്സസ് ഉള്ള എക്സിക്യൂട്ടീവുകളെയോ സാമ്പത്തിക വകുപ്പുകളിലെ ആളുകളെയോ ഈ ആക്രമണങ്ങൾ പലപ്പോഴും ലക്ഷ്യമിടുന്നു. അക്കൗണ്ടൻസി, ഓഡിറ്റ് സ്ഥാപനങ്ങൾ അവരുടെ ജീവനക്കാർക്ക് ആക്സസ് ചെയ്യുന്ന വിവരങ്ങളുടെ മൂല്യം കാരണം ഫിഷിംഗിന് പ്രത്യേകിച്ച് ഇരയാകുന്നു.

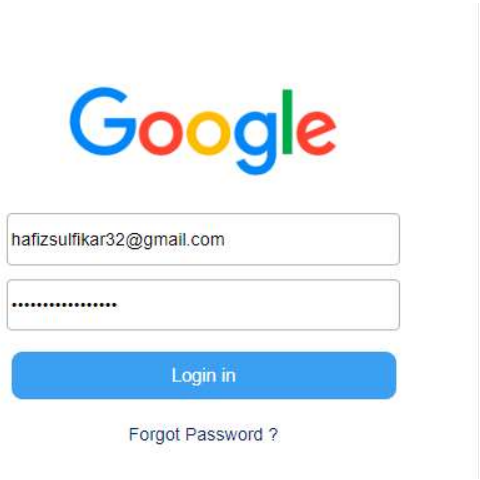
1,800-ലധികം ഗൂഗിൾ അക്കൗണ്ടുകളിൽ സ്പിയർ ഫിഷിംഗ് ആക്രമണം നടത്തി, ടാർഗെറ്റുചെയ്ത ഉപയോക്താക്കളെ ഭീഷണിപ്പെടുത്തുന്നതിനായി accounts-google.com ഡൊമെയ്ൻ ഉപയോഗിച്ച് ത്രെറ്റ് ഗ്രൂപ്പ്-4127 ഫാൻസി ബിയർ (റഷ്യൻ ചാരവൃത്തി ഗ്രൂപ്പ്)ഹിലരി ക്ലിന്റന്റെ കാമ്പെയ്നെ (മുൻ അമേരിക്കൻ സെക്രട്ടറി) ലക്ഷ്യമാക്കി.

വ്യത്യസ്ത പ്രായക്കാർക്കിടയിലുള്ള സ്പിയർ ഫിഷിംഗ് സാധ്യതയെക്കുറിച്ചുള്ള ഒരു പഠനത്തിൽ, 100 യുവാക്കളിൽ 43% പേരും പ്രായമായ 58 പേരും 21 ദിവസങ്ങളിലായി പ്രതിദിന ഇമെയിലുകളിലെ സിമുലേറ്റഡ് ഫിഷിംഗ് ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്തതായി കണ്ടെത്തി.
തിമിംഗലവേട്ടയും സിഇഒ വഞ്ചനയും
തിമിംഗല ആക്രമണങ്ങൾ മുതിർന്ന എക്സിക്യൂട്ടീവുകളെയും മറ്റ് ഉന്നത വ്യക്തികളെയും ലക്ഷ്യമിടാൻ സ്പിയർ ഫിഷിംഗ് ടെക്നിക്കുകൾ ഉപയോഗിക്കുന്നു[23] കസ്റ്റമൈസ് ചെയ്ത ഉള്ളടക്കം, പലപ്പോഴും ഒരു സബ്പോണ അല്ലെങ്കിൽ ഉപഭോക്തൃ പരാതിയുമായി ബന്ധപ്പെട്ടതാണ്.[24]

ഒരു ഓഫ്ഷോർ അക്കൗണ്ടിലേക്ക് പണമയക്കുന്നതിനായി ജീവനക്കാരെ കബളിപ്പിക്കാൻ മുതിർന്ന എക്സിക്യൂട്ടീവുകളിൽ നിന്ന് വ്യാജ ഇമെയിലുകൾ അയക്കുന്നത് സിഇഒ വഞ്ചനയിൽ ഉൾപ്പെടുന്നു.[25] ഇതിന് വിജയശതമാനം കുറവാണ്, പക്ഷേ സ്ഥാപനങ്ങൾക്ക് വലിയ തുക നഷ്ടമാകാൻ ഇടയാക്കും.[26]

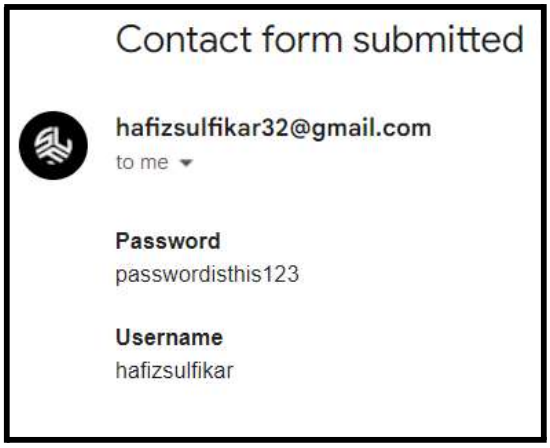
ഫിഷിങ് വെബ്സൈറ്റിന്റെ പ്രവർത്തനം

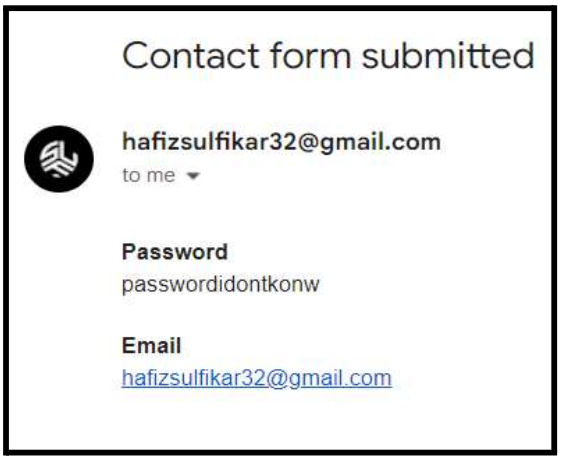




ഇമെയിൽ,പാസ്സ്വേർഡ് പോലുള്ള വിവരങ്ങൾ ടൈപ് ചെയ്ത ലോഗിൻ ബട്ടൺ ക്ലിക്ക് ചെയ്യുമ്പോൾ ഹാക്കർസിന് ലോഗിൻ ഡീറ്റെയിൽസ് ലഭിക്കുന്നു.

ഇതുപോലെ ⬇





എങ്ങനെ ഫിഷിങ് വെബ്സൈറ്റിനെ മനസിലാക്കാം?

1.യു.ആർ.എൽ പരിശോധിക്കുക

ഫിഷിംഗ് URL-കൾ എങ്ങനെ തിരിച്ചറിയാമെന്ന് മനസിലാക്കാൻ, നിങ്ങൾ വെബ് വിലാസത്തിന്റെ ആധികാരികത പരിശോധിക്കേണ്ടതുണ്ട്. ഇത് 'https://' എന്നതിന് പകരം 'http://' എന്നതിൽ ആരംഭിക്കുകയാണെങ്കിൽ, ജാഗ്രത പാലിക്കുക. വെബ്സൈറ്റ് എൻക്രിപ്റ്റുചെയ്ത് ഒരു SSL സർട്ടിഫിക്കറ്റ് ഉപയോഗിച്ച് സുരക്ഷിതമാക്കിയിരിക്കുന്നു എന്നാണ് അധിക 'എസ്' അർത്ഥമാക്കുന്നത്. ഒരു SSL സർട്ടിഫിക്കറ്റ് ഓൺലൈൻ ആശയവിനിമയങ്ങൾക്ക് അധിക സുരക്ഷ പ്രോത്സാഹിപ്പിക്കുന്ന ഒരു കോഡ് പോലെയാണ്.

എന്നിരുന്നാലും, ഇക്കാലത്ത്, ഫിഷർമാരും 'https://' ഉപയോഗിക്കാൻ തുടങ്ങിയിരിക്കുന്നു, അതിനാൽ ഈ വശം ഒരു വിഡ്ഢിത്തമായ അടയാളമല്ല .

ഫിഷിംഗ് ലിങ്കുകൾ പരിശോധിക്കുന്നതിനുള്ള മറ്റ് ചില വഴികൾ സൂക്ഷ്മമായി ശ്രദ്ധിക്കുക:

സാധാരണയായി, വ്യാജ വെബ്സൈറ്റുകൾക്ക് സ്പെല്ലിംഗിൽ ഒരു അധിക അക്ഷരം 'S' അല്ലെങ്കിൽ 'A' ഉണ്ടായിരിക്കും. ഉദാഹരണത്തിന്, www.walmarts.com അല്ലെങ്കിൽ www.flipkaart.com. 'O' പകരം '0' (പൂജ്യം) നൽകിയിട്ടുണ്ടെങ്കിൽ. ഉദാഹരണത്തിന്, "www.yah00.com."URL-ൽ അധികമോ നഷ്ടമായതോ ആയ പ്രതീകങ്ങളോ ചിഹ്നങ്ങളോ ഉണ്ടെങ്കിൽ. ഉദാഹരണത്തിന്, ഒരു നിയമാനുസൃത URL www.coca-cola.com ആണ് (ഒരു ഹൈഫൻ ഉള്ളത്), എന്നാൽ വ്യാജമായത് www.cocacola.com (ഹൈഫൻ ഇല്ലാതെ) ആകാം.

2. ഉള്ളടക്കത്തിന്റെ ഗുണനിലവാരം താരതമ്യം ചെയ്യുക

യഥാർത്ഥ വെബ്സൈറ്റിന്റെ ഉള്ളടക്കം മികച്ചതും നന്നായി എഴുതിയതും വ്യാകരണ, വിരാമചിഹ്നങ്ങൾ, അക്ഷരപ്പിശകുകൾ എന്നിവയില്ലാത്തതും ആയിരിക്കും. വ്യാജ സൈറ്റ് യഥാർത്ഥ സൈറ്റിന്റെ കാർബൺ പകർപ്പാണെങ്കിലും, ദൃശ്യങ്ങൾ കുറഞ്ഞ റെസല്യൂഷനായിരിക്കാം.

3. ഉള്ളടക്കം നഷ്ടപ്പെട്ടിട്ടുണ്ടോയെന്ന് പരിശോധിക്കുക

ഒരു ക്ലിക്കിലൂടെ ഫിഷിംഗ് URL-കൾ എങ്ങനെ തിരിച്ചറിയാമെന്ന് നിങ്ങൾക്കറിയാമോ? "Contact Us" എന്ന പേജിലേക്ക് പോകുക. വിശ്വസനീയമായ കോൺടാക്റ്റ് വിശദാംശങ്ങളൊന്നും ഇല്ലെങ്കിൽ, അത് ഒരു ഫിഷിംഗ് വെബ്സൈറ്റായിരിക്കാം.

4.വ്യക്തിഗത വിവരങ്ങൾ ആവശ്യപ്പെടുന്നുണ്ടോ?

നിങ്ങളുടെ ഫോൺ നമ്പർ, ഇമെയിൽ വിലാസം, പാസ്വേഡ്, റസിഡൻഷ്യൽ വിലാസം, ബാങ്കിംഗ് വിശദാംശങ്ങൾ, ഐഡി നമ്പർ മുതലായവ പോലുള്ള വ്യക്തിഗത വിശദാംശങ്ങൾ ആവശ്യപ്പെടുന്ന ഒരു പോപ്പ്-അപ്പ് ദൃശ്യമാകുകയാണെങ്കിൽ, ഇത് ചുവന്ന പതാകയായി പരിഗണിക്കുക.

ഈ സാഹചര്യത്തിൽ, ഏതെങ്കിലും തരത്തിലുള്ള വിവരങ്ങൾ നൽകുന്നതിൽ നിന്ന് എപ്പോഴും വിട്ടുനിൽക്കുക. ഒരു ഫിഷിംഗ് വെബ്സൈറ്റ് എങ്ങനെ തിരിച്ചറിയാമെന്ന് അറിയാൻ ആഗ്രഹിക്കുന്ന പരിചയക്കാർ, ജോലി ചെയ്യുന്ന സഹപ്രവർത്തകർ, ജീവനക്കാർ എന്നിവരുമായി നിങ്ങൾക്ക് ഈ ഉപദേശം പങ്കിടാം.

5. ഇത് സുരക്ഷിതമല്ലാത്ത വെബ്സൈറ്റാണോ?

ചില സമയങ്ങളിൽ, നിങ്ങൾ ഒരു വെബ്സൈറ്റ് സന്ദർശിക്കാൻ ശ്രമിക്കുന്നു, പക്ഷേ നിങ്ങൾക്ക് ഒരു സുരക്ഷാ അലേർട്ട് ലഭിക്കും-'Connection Not Secured.' അത്തരമൊരു സാഹചര്യത്തിൽ, ഫിഷിംഗ് ലിങ്കുകൾ എങ്ങനെ തിരിച്ചറിയാമെന്ന് മനസിലാക്കേണ്ടത് വളരെ പ്രധാനമാണ്. ആദ്യം, URL-ന്റെ ഇടതുവശത്ത് ദൃശ്യമാകുന്ന പാഡ്ലോക്ക് ഐക്കണിൽ ക്ലിക്കുചെയ്യുക.

ഇതുവഴി, സുരക്ഷാ സർട്ടിഫിക്കറ്റുകളുമായും കുക്കികളുമായും ബന്ധപ്പെട്ട വിവരങ്ങൾ നിങ്ങൾക്ക് സ്വയം പ്രയോജനപ്പെടുത്താം. ഒരു ഉപയോക്താവിന്റെ ഡാറ്റ സംഭരിക്കുകയും വെബ്സൈറ്റ് ഉടമയ്ക്ക് അയയ്ക്കുകയും ചെയ്യുന്ന ഒരു ഫയലാണ് കുക്കി.

മിക്ക കേസുകളിലും, ഇത് മികച്ച ഉപയോക്തൃ അനുഭവം നൽകുന്നു; എന്നിരുന്നാലും, ഫിഷർമാർ പലപ്പോഴും ഈ വിവരങ്ങൾ ദുരുപയോഗം ചെയ്യാറുണ്ട്.

6. ഒരു വ്യാജ പാസ്വേഡ് ഉപയോഗിക്കുക

സംശയാസ്പദമായ ഒരു വെബ്സൈറ്റ് പാസ്വേഡ് ആവശ്യപ്പെടുകയാണെങ്കിൽ, തെറ്റായ ഒന്ന് നൽകുക. നിങ്ങൾ ഇപ്പോഴും സൈൻ ഇൻ ചെയ്തിരിക്കുകയോ ശരിയായ പാസ്വേഡ് നൽകിയെന്ന് സൂചിപ്പിക്കുന്ന പോയിന്റ് കാണുകയോ ചെയ്താൽ, അത് 100% വ്യാജ വെബ്സൈറ്റാണ്. ഈ സോഷ്യൽ എഞ്ചിനീയറിംഗ് ആക്രമണങ്ങളിൽ നിന്ന് രക്ഷപ്പെടാൻ ഈ ട്രിക്ക് നിങ്ങളെ സഹായിക്കും.

7. പേയ്മെന്റ് രീതി പരിശോധിക്കുക

ഡെബിറ്റ് കാർഡുകൾ, ക്രെഡിറ്റ് കാർഡുകൾ, പേപാൽ പോലുള്ള പേയ്മെന്റ് ഓപ്ഷനുകൾ എന്നിവയ്ക്ക് പകരം ഒരു വെബ്സൈറ്റ് നേരിട്ട് ബാങ്ക് ട്രാൻസ്ഫർ ആവശ്യപ്പെടുകയാണെങ്കിൽ, നിങ്ങൾ ജാഗ്രത പാലിക്കേണ്ടതുണ്ട്. വെബ്സൈറ്റ് ഡൊമെയ്നിനായി ഒരു ബാങ്കും ക്രെഡിറ്റ് കാർഡ് സൗകര്യം അംഗീകരിച്ചിട്ടില്ലെന്നും അവർക്ക് ക്ഷുദ്രകരമായ പ്രവർത്തനങ്ങൾ പരിശീലിക്കാമെന്നും ഇത് സൂചിപ്പിക്കാം.

പ്രത്യേകിച്ചും ഡെലിവറി വേഗത്തിലല്ലാത്ത സോഫ്റ്റ്വെയർ അധിഷ്ഠിത സേവനങ്ങൾക്കായി വലിയ തുകകൾ ചെലവഴിക്കുമ്പോൾ, ഒരു പ്രൊപ്പോസലിനായി ഒരു അഭ്യർത്ഥന പരിശോധിക്കുക.

ഒരു ഫിഷിംഗ് വെബ്സൈറ്റ് എങ്ങനെ റിപ്പോർട്ട് ചെയ്യാം

ഒരു ലിങ്ക് ഒരു ഫിഷിംഗ് URL ആണോ എന്ന് എങ്ങനെ അറിയാമെന്നതിനെക്കുറിച്ച് ഇപ്പോൾ നിങ്ങൾക്ക് ന്യായമായ ധാരണയുണ്ട്, ഒരു ഫിഷിംഗ് വെബ്സൈറ്റ് റിപ്പോർട്ടുചെയ്യാനുള്ള ലളിതമായ മാർഗവും നിങ്ങൾ പഠിക്കണം.

ആഗോള പാൻഡെമിക്, ലോക്ക്ഡൗൺ പരമ്പരകൾ, വർദ്ധിച്ചുവരുന്ന തൊഴിലില്ലായ്മ എന്നിവ തട്ടിപ്പുകാരുടെ എണ്ണം കൂട്ടി. 2020-ൽ ഓരോ ആഴ്ചയും ശരാശരി 46,000 പുതിയ ഫിഷിംഗ് വെബ്സൈറ്റുകൾ Google റിപ്പോർട്ട് ചെയ്യുന്നു.

അത്തരം സംശയാസ്പദമായ വെബ്സൈറ്റുകൾ നിങ്ങൾ കണ്ടാൽ, Google-ന്റെ റിപ്പോർട്ട് ഫിഷിംഗ് പേജിലേക്ക് പോകുക. URL കൊടുത്ത് കൂടുതൽ വിവരങ്ങൾ ചേർക്കുക.

https://safebrowsing.google.com/safebrowsing/report_phish/?rd=1&hl=en