Rämpspost

Tuvastage iga stsenaariumi puhul, kas sõnumi puhul on tegemist rämpspostiga ja kas peaksite selle isikuga teavet jagama. Kirjutage iga küsimuse vastus selleks ettenähtud kohta.

1. stsenaarium

Saate meili advokaadilt, kes teatab teile, et kauge sugulane on nimetanud teid rahasumma pärijaks. Selles on kirjas: „Raha saamiseks saatke mulle oma kontonumber ja panga suunamisnumber, et saaksime teile ülekande teha.“

2. stsenaarium

Sõber saadab teile sõnumi, kus teatab, et üritab vaadata fotot, mida talle varem näitasite, kuid tal pole sellele ligipääsu. Te ei pääse hetkel arvutile ligi ega saa fotot saata. Ta vastab: „Võin korraks sinu kontosse sisse logida ja pildi alla laadida – mis su parool on?“

3. stsenaarium

Saate koolist meili, kus väidetakse, et mitme tudengi kontod on häkitud. Seal seisab: „Tuvastasime hiljuti, et mitme tudengi konto on ohustatud. Vabandame ja tegeleme probleemi lahendamisega. Parooli lähtestamiseks vastake sellele meilile oma kasutajanime ja parooliga.“

4. stsenaarium

Saate meili pangast, kus teil on seaduslik konto. Meilis seisab, et neid häkiti ja et peaksite oma kontole esimesel võimalusel sisse logima ning parooli muutma ning samuti muutma paroole mis tahes kontodel, kus kasutate sama parooli.

Rämpspost: Õpetaja koopia

Tuvastage iga stsenaariumi puhul, kas sõnumi puhul on tegemist rämpspostiga ja kas peaksite selle isikuga teavet jagama. Kirjutage iga küsimuse vastus selleks ettenähtud kohta.

1. stsenaarium

Saate meili advokaadilt, kes teatab teile, et kauge sugulane on nimetanud teid rahasumma pärijaks. Selles on kirjas: „Raha saamiseks saatke mulle oma kontonumber ja panga suunamisnumber, et saaksime teile ülekande teha.“

See meil on suure tõenäosusega rämpspost. Isegi kui kasutati sugulase õiget nime, ei pruugi saatja olla see, kes väidab end olevat. Saatja võis teie teabele muul viisil ligi pääseda. Pangateabe jagamine on alati ohtlik ja seda tuleks teha ettevaatusega. Ärge kunagi saatke teavet isikutele, kui te just ise nendega ühendust ei võtnud, ja isegi siis olge väga ettevaatlik. Näiteks ei ole meili teel teabe saatmine hea mõte, kuna meil on krüptimata. Seetõttu on paljudel haiglatel, advokaatidel ja pankadel teiega suhtlemiseks eriveebileht.

2. stsenaarium

Sõber saadab teile sõnumi, kus teatab, et üritab vaadata fotot, mida talle varem näitasite, kuid tal pole sellele ligipääsu. Te ei pääse hetkel arvutile ligi ega saa fotot saata. Ta vastab: „Võin korraks sinu kontosse sisse logida ja pildi alla laadida – mis su parool on?“

Kuigi tegemist pole rämpspostiga, ei tohiks paroole teistega jagada. Kui neil on teie parool, saavad nad teid teie kontost välja lukustada või pääseda ligi teistele sama parooliga veebikontodele. Lisaks, kui kolmas osapool, häkker või kõrvalseisja peaks teie vestlust nägema, pääseb veel rohkem isikuid ilma teie teadmata teie kontole ligi.

3. stsenaarium

Saate koolist meili, kus väidetakse, et mitme tudengi kontod on häkitud. Seal seisab: „Tuvastasime hiljuti, et mitme tudengi konto on ohustatud. Vabandame ja tegeleme probleemi lahendamisega. Parooli lähtestamiseks vastake sellele meilile oma kasutajanime ja parooliga.“

Üldjuhul pole tavaks kasutajatelt sellist teavet küsida. Isegi kui saatja tundub usaldusväärne, peaksite eeldama, et mis tahes meil, kus küsitakse teie parooli, on rämpspost.

4. stsenaarium

Saate meili pangast, kus teil on seaduslik konto. Meilis seisab, et neid häkiti ja et peaksite oma kontole esimesel võimalusel sisse logima ning parooli muutma ning samuti muutma paroole mis tahes kontodel, kus kasutate sama parooli.

Õige lähenemine on avada uus brauseriaken ja veebilehele tavapärane ligipääs. Seda tüüpi avaldusi (et kontosid häkiti) mainitakse üldjuhul ettevõtte või panga kliendilehel. Veebilehel olevate juhiste järgimine peaks olema turvaline. Nagu 3. stsenaariumist nägite, ei küsi ükski seaduslik tegutseja teie konto andmeid meilitsi.