


# Trīs izplatītākie kiberuzbrukumu veidi

## Pārskats

Sociālās inženierijas uzbrukumi, kuros ļaundari ar viltu piespiež cilvēkus darīt kaut ko tādu, ko nevajadzētu darīt, ir viena no izplatītākajām metodēm, ko kiberuzbrucēji izmanto, lai vērstos pret cilvēkiem. Šo koncepciju afēristi un krāpnieki ir izmantojuši jau tūkstošiem gadu. Jaunums ir tas, ka internets ļauj kibernoziedzniekam jebkurā pasaules vietā ļoti viegli izlikties par jebkuru personu, par kuru vēlas, un vērsties pret jebkuru personu, kuru vēlas. Turpmāk ir aprakstīti trīs visbiežāk sastopamās sociālās inženierijas metodes, ko kiberuzbrucēji izmantos, lai mēģinātu iesaistīt un apmānīt.

## Pikšķerēšana

Pikšķerēšana ir tradicionālākais sociālās inženierijas uzbrukums; tas ir tad, kad kiberuzbrucēji jums nosūta e-pasta vēstuli, mēģinot ar viltu piespiest veikt darbības, kuras jums nevajadzētu darīt. To dēvē par pikšķerēšanu, jo tā līdzinās makšķerēšanai ezerā: jūs izmetat auklu un āķi, bet nezināt, ko noķersiet. Šīs taktikas stratēģija bija tāda, ka, jo vairāk pikšķerēšanas e-pasta vēstuļu kibernoziedznieki nosūtīja, jo vairāk cilvēku kļuva par upuriem. Mūsdienās pikšķerēšanas uzbrukumi ir kļuvuši daudz sarežģītāki un mērķtiecīgāki (dažkārt tos dēvē par mērķētu pikšķerēšanu), un kiberuzbrucēji pirms nosūtīšanas bieži vien pielāgo savus pikšķerēšanas e-pastus.

## Smikšķerēšana

Smikšķerēšana būtībā ir uz SMS balstīta pikšķerēšana, kad e-pasta vēstules vietā tiek nosūtīta īsziņa. Kiberuzbrucēji sūta īsziņas uz jūsu tālruni, izmantojot tādas lietotnes kā Facebook, Google vai WhatsApp. Ir vairāki iemesli, kāpēc smikšķerēšana ir kļuvusi populāra. Pirmkārt, ir daudz grūtāk filtrēt ziņojumapmaiņas uzbrukumus nekā e-pasta uzbrukumus. Otrkārt, kiberuzbrucēju sūtītās ziņas bieži ir ļoti īsas, tajās ir ļoti maz konteksta, tāpēc ir daudz grūtāk noteikt, vai ziņa ir leģitīma vai ne. Treškārt, ziņojumapmaiņa bieži ir neformālāka un vairāk balstīta uz rīcību, tāpēc cilvēki ir pieraduši ātri atbildēt uz ziņām vai rīkoties saskaņā ar tām. Visbeidzot, cilvēki arvien labāk un labāk pamana pikšķerēšanas e-pasta uzbrukumus, tāpēc kiberuzbrucēji vienkārši pāriet uz jaunu metodi– ziņojumapmaiņu.

## Vikšķerēšana

Vikšķerēšana jeb balss pikšķerēšana ir taktika, kurā tiek izmantots tālruņa zvans vai balss ziņa, nevis e-pasts vai īsziņa. Vikšķerēšanas uzbrukumiem uzbrucējam ir nepieciešams daudz vairāk laika, lai tos īstenotu, jo uzbrucējs runā tieši ar upuri un mijiedarbojas ar viņu. Tomēr šāda veida uzbrukumi ir arī daudz efektīvāki, jo pa tālruni ir daudz vieglāk radīt spēcīgas emocijas, piemēram, steidzamības sajūtu. Tiklīdz kiberuzbrucējs jūs uzrunās pa tālruni, viņš/viņa neļaus jums pārtraukt sarunu, kamēr nesaņems vēlamo.

### Ziņojumapmaiņas uzbrukumu pamanīšana un apturēšana

Par laimi, nav svarīgi, kuru no šīm trim metodēm kiberuzbrucēji izmanto, ir kopīgas norādes, kuras jūs varat pamanīt:

- **Steidzamība**: Jebkura ziņa, kas rada izteiktu steidzamības sajūtu, ar kuru uzbrucēji cenšas jūs piespiest ātri rīkoties un kļūdīties. Kā piemēru var minēt ziņu, kas apgalvo, ka ir no valdības iestādes un ka jūsu nodokļu maksājumi ir nokavēti, un, ja tos tūlīt nesamaksāsiet, nonāksiet cietumā.

- **Spiediens**: Jebkura ziņa, kas piespiež darbinieku ignorēt vai apiet uzņēmuma drošības politiku un procedūras.

- **Šaubas**: Jebkura ziņa, kas izraisa milzīgu šaubu sajūtu vai šķiet pārāk laba, lai būtu patiesa, piemēram, nepiegādāta DPD, Omniva paka vai paziņojums, ka saņemat Amazon atmaksu.

- **Tonis**: Jebkura ziņa, kas šķietami nāk no jums pazīstamas personas, piemēram, kolēģa, bet tās formulējums neizklausās pēc viņa vai arī kopējais tonis vai paraksts ir neatbilstošs.

- **Jūsu informācija**: Jebkura ziņa, kurā tiek pieprasīta ļoti sensitīva informācija, piemēram, jūsu parole vai kredītkartes dati.

- **Vispārīgums**: Ziņa nāk no uzticamas organizācijas, bet tajā izmantota vispārīga uzruna, piemēram, "Cienījamais klient". Ja jums ir sūtījums no Amazon vai tālruņa pakalpojumu sniedzējam ir problēmas ar rēķinu, viņi zina jūsu vārdu un uzvārdu.

- **Personīgā e-pasta adrese**: Jebkurš e-pasts, kas šķietami saņemts no leģitīmas organizācijas, pārdevēja vai kolēģa, bet tajā izmantota personīgā e-pasta adrese, piemēram, janis@gmail.com vai janis@hotmail.com.

Meklējot šīs kopīgās pazīmes, jūs varat sevi pasargāt.

## Viesredaktors

Mērija Džeina Suaresa Parteina (Mary Jane Suarez Partain) ir programmas "Sievietes kiberdrošībā" (WiCyS) direktore. Viņas galvenais uzdevums ir nodrošināt resursus, iniciatīvas un programmas, kas paredzētas, lai pieņemtu darbā, noturētu un attīstītu sievietes kiberdrošības jomā. Viņa aizrautīgi cenšas radīt iekļaujošu vidi, kurā visi jūtas novērtēti, gaidīti un pamanīti.

## Resursi

**Pārtraukt tālruņa zvanu krāpšanu:** https://www.sans.org/newsletters/ouch/stop-phone-call-scams
**Pikšķerēšanas uzbrukumi kļūst viltīgāki:** https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/
**Emocionālie ierosinātāji – kā kiberuzbrucēji piemāna cilvēkus:** https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you
**Esmu hakeru upuris, ko tagad darīt:** https://www.sans.org/newsletters/ouch/im-hacked-now-what/

**Tulkojums: CERT.LV**