Ikmēneša informācijas drošības biļetens ikvienam

# CEO krāpšana jeb biznesa e-pastu kompromitēšana

## Kas ir CEO krāpšana?

Kibernoziedznieki turpina pilnveidot e-pastu krāpniecību, ko sauc arī par CEO krāpšanu vai biznesa e-pastu kompromitēšanu (CEO Fraud / BEC). Tas ir mērķtiecīgi organizēts uzbrukums, izmantojot e-pastu, lai apmānītu upuri, liekot tam veikt darbības, ko nevajadzētu veikt. Vairumā gadījumu tiek mēģināts izkrāpt naudu. Šos uzbrukumus īpaši bīstamus padara tas, ka ļaundari pirms uzbrukuma veic potenciālā upura padziļinātu izpēti. Arī drošības risinājumi bieži vien ir bezspēcīgi šādu uzbrukumu priekšā, jo nav inficētu e-pastu pielikumu vai ļaundabīgu saišu, ko tehnoloģijas varētu atpazīt un nobloķēt. Īss uzbrukuma apraksts zemāk.

Uzbrucējs internetā veic izpēti un iegūst informāciju par potenciālo upuri un tā kontaktiem. Piemēram, ja uzbrukuma mērķis esat jūs pats, ļaundari noteikti izpētīs, kas ir jūsu priekšnieks, vai, piemēram, nekustamā īpašuma aģents, ar ko jūs sadarbojaties. Tad uzbrucējs izveido e-pastu, izliekoties par kādu no šiem cilvēkiem, un nosūta to jums. E-pasts parasti ir steidzama rakstura, un prasa no jums tulītēju rīcību, piemēram, rēķina apmaksu, sensitīvu dokumentu nosūtīšanu utml. E-pasts liek jums ātrumā kļūdīties. Tālāk daži piemēri, kā uzbrukums varētu noritēt:

**Naudas pārskatījums :** uzbrucējs vēlas izkrāpt naudu. Krāpnieki izpēta jūsu uzņēmumu, atrod atbildīgos par pārskaitījumiem vai grāmatvedību. Tad šiem darbiniekiem tiek nosūtīti pielāgoti viltus e-pasti it kā no priekšniecības. E-pasts apraksta ārkārtas situāciju, un tajā dots rīkojums nekavējoties pārskaitīt naudu uz jaunu bankas kontu, kas, protams, realitātē nozīmē naudas pārskaitījumu noziedzniekiem.

**Nodokļu krāpniecība:** uzbrucējs vēlas iegūt personas datus, ko vēlāk izmantot nodokļu krāpniecībai. To var paveikt, piemēram, nozogot datus par visiem uzņēmuma darbiniekiem. Noziedznieki identificē personāla daļas darbiniekus, kam tiek nosūtīti viltoti e-pasti it kā no priekšniecības vai no juridiskās daļas. E-pasts rada steidzamības sajūtu un prasa nekavējoties nosūtīt nodokļu informāciju par darbiniekiem.

## Kā sevi pasargāt

Ko darīt, lai sevi pasargātu? Vislabākā aizsardzība ir veselais saprāts. Šeit ir piedāvātas dažas pazīmes, pēc kurām varētu atpazīt krāpniecisku e-pastu:

**E-pasts ir īss un steidzams, un paraksts satur norādi, ka tas nosūtīts no mobilās iekārtas.**

**Ir izteikta steidzamības sajūta, kas liek jums pārkāpt ierasto darbību secību vai organizācijas politiku. Vienmēr ievērojiet procedūras un noteikto kārtību, pat ja izskatās, ka e-pasts nāk no priekšniecības.**

**Lai gan e-pasts ir saistīts ar darbu, tiek izmantota personīga e-pasta adrese, piemēram, @gmail.com vai @hotmail.com.**

**E-pasts izskatās no jūsu priekšnieka vai kolēģa, taču ziņas saturs un tonis neatbilst ierastajam.**

**Ir norādītas maksājuma instrukcijas, taču tās atšķiras no iepriekš saņemtajām un izmantotajām, piemēram, ir norādīts cits bankas konts.**

Ja jums ir aizdomas, ka esat kļuvis par šāda uzbrukuma upuri, nekavējoties pārtrauciet saziņu ar iespējamo uzbrucēju un ziņojiet priekšniecībai. Ja esat kļuvis par upuri mājās, ziņojiet bankai, tiesībsargājošām iestādēm vai CERT.LV.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

## Viesredaktors

***Don Cavender*** *ir bijušais FIB aģents ar vairāk kā 22 gadu pieredzi kibernoziegumu izmeklēšanā. Viņš nesen ir darbojies arī kā Vašingtonas BEC (business email compromise) koordinators. Viņš organizē apmācības un veic pētniecību digitālās izmeklēšanas nozarē.* @don_cavender
https://www.linkedin.com/in/donald-cavender

## Resursi

| | |
|---|---|
| Sociālā inženierija: | https://www.sans.org/u/HE3 |
| Apstādināt pikšķerēšanu: | https://www.sans.org/u/HE8 |
| Apstādināt ļaunatūru: | https://www.sans.org/u/HEd |
| Aizsargājiet savus lietotāja piekļuves datus: | https://www.sans.org/u/HEi |


*Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Tulkojums: Edgars Tauriņš*