CEO/UZŅĒMUMA E-PASTA KOMPROMITĒŠANAS (UEK) KRĀPŠANA

CEO/UEK krāpšana izpaužas kā darbinieka, kurš pilnvarots veikt maksājumus apmānīšana pamudinot veikt neautorizētu maksājumu vai neīsta rēķina apmaksu.

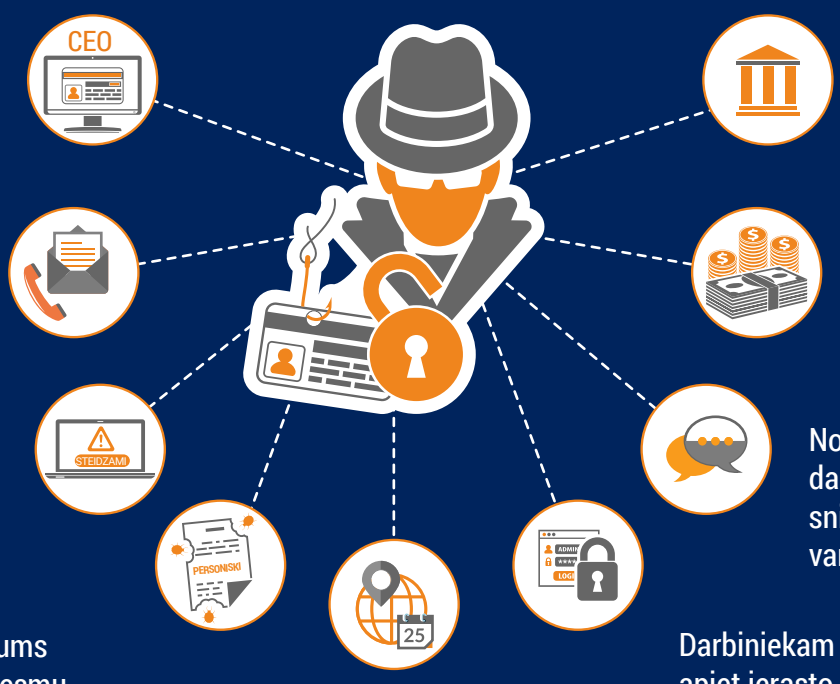
KĀ TAS NOTIEK?

Krāpnieks piezvana vai sūta ē-pastu uzdodoties par uzņēmuma augsta līmeņa darbinieku.

Viņi ir sagatavojušies un zina, kā uzņēmums darbojas.

Viņi prasa nekavējoties veikt maksājumu.

Viņi lieto šādas frāzes: "Konfidenciāli", "Uzņēmums Tev uzticas", "Es šobrīd esmu aizņemts".



Nereti tiek prasīts veikt maksājumu uz bankas kontu ārpus Eiropas.

Darbinieks pārskaita naudu uz krāpnieku kontrolē esošu kontu.

Norādījumus par tālākajām darbībām vēlāk var tikt sniegti cita persona vai tie var tikt atsūtīti ē-pastā.

Darbiniekam tiek pieprasīts apiet ierasto maksājumu apstiprināšanas procesu.

Viņi atsaucas uz situācijas jūtīgumu (piemēram, nodokļu pārbaude, apvienošanās, uzņēmuma pārdošana).

KAM JĀDARA UZMANĪGU?

- Neierasts e-pasts/tālruņa zvans
- Tieša augstāka līmeņa amatpersonas saziņa, ar kuru ikdienā nekontaktējaties
- Prasība ievērot pilnīgu slepenību
- Spiediens un steidzamība
- Neparasts pieprasījums, kas ir pretrunā iekšējām procedūrām
- Draudi vai neierasti slavinājumi/solījumi par atlīdzību

KĀ JUMS RĪKOTIES?

KĀ UZŅĒMUMAM

Apzinieties riskus un parūpējieties, lai **darbinieki ir informēti un arī apzinātos riskus**.

Iedrošiniet darbiniekus pret **maksājumu pieprasījumiem izturēties ar piesardzību.**

Izveidojet iekšēju maksājumu **apstrādes kārtību.**

Izveidojiet procedūru ē-pastā saņemtu maksājumu pamatotības pārbaudei.

Izveidojiet **ziņošanas kārtību** krāpšanas pārvaldībai.

Pārskaties informāciju, kas pieejama jūsu uzņēmuma tīmekļa vietnē. **Ierobežojiet detalizāciju un esiet piesardzīgi** izmantojot sociālos tīklus.

Pilnveidojiet un atjauniniet tehnisko drošību.

! Krāpšanas mēģinājumu gadījumos vienmēr informējiet policiju, arī tad ja nekļuvāt par upuri.

KĀ DARBINIEKS

Precīzi sekojiet procedūrām attiecībā uz maksājumiem un iepirkumiem. **Neizlaidiet nevienu soli un neļaujieties steidzināšanai**.

Darbojoties ar sensitīvu informāciju/naudas pārskaitījumiem, **vienmēr rūpīgi pārbaudiet ē-pasta adreses**.

Rodoties šaubām par maksājuma pieprasījumu, **sazinieties ar pieredzējušu kolēģi**.

Neatveriet ē-pastā saņemtas **aizdomīgas saites vai pielikumus**. Jo īpaši uzmanieties, pieslēdzoties privātajam ē-pastam no uzņēmuma datora.

Ierobežojiet informāciju un esiet piesardzīgi izmantojot sociālos tīklus.

Nedalieties ar informāciju par uzņēmuma struktūru un drošības procedūrām.

! Ja saņemat aizdomīgu zvanu vai ē-pastu, informējiet IT struktūrvienību.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · Latvijas Valsts Policija · Finanšu Nozares Asociācija

#CyberScams

IEGULDĪJUMU KRĀPŠANA

Izplatītākās ieguldījumu krāpšanas var ietvert ienesīgas ieguldījumu iespējas, piemēram, akcijas, obligācijas, kriptovalūtas, retos metālus, aizjūras zemes ieguldījumus vai alternatīvu enerģiju.

KAS PAR TO LIECINA?

- Jums tiek apsolīta ātra peļņa un apgalvots, ka ieguldījums ir drošs.
- Piedāvājums ir spēkā ierobežotu laiku.
- Jūs atkārtoti saņemat zvanus, ko negaidāt.
- Piedāvājums ir personalizēts un jums tiek prasīts ar to nedalīties.

KĀ JUMS RĪKOTIES?

- Pirms nododat jebkādu naudu vai veicat ieguldījumu **vienmēr saņemiet objektīvus finanšu padomus.**
- **Noraidiet negaidītus zvanus**, kas saistīti ar investīciju iespējām.
- **Izturieties aizdomīgi** pret piedāvājumiem, kas sola drošu ieguldījumu, garantētu atdevi un lielu peļņu.
- **Uzmanieties no turpmākajām krāpšanām.** Ja jūs jau esat ieguldījis krāpšanā, krāpnieki, visticamāk, atkal vērsīsies pie jums vai pārdos jūsu datus citiem noziedzniekiem.
- **Sazinieties ar policiju,** ja jums radušās aizdomas.

EUROPOL EC3 European Cybercrime Centre

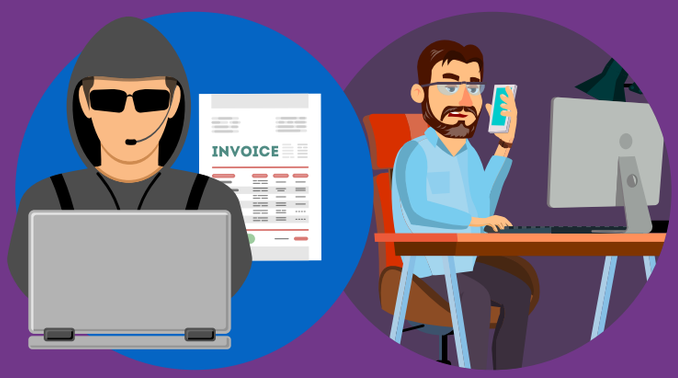
EBF European Banking Federation

LATVIJAS VALSTS POLICIJA

FINANŠU NOZARES ASOCIĀCIJA

#CyberScams

RĒĶINU VILTOŠANA



KĀ TAS NOTIEK?

- Uzņēmumā vēršas, kāds kurš izliekas par piegādātāja/ pakalpojumu sniedzēja/ kreditora pārstāvi.
- Var tikt kombinētas dažādas metodes: tālrunis, vēstule, ē-pasts u.c.
- Krāpnieks pieprasa mainīt maksājuma bankas informāciju (t.i., saņēmēja bankas konta informāciju) nākamajiem rēķiniem. Piedāvāto jauno kontu kontrolē krāpnieks.

KĀ JUMS RĪKOTIES?

KĀ UZŅĒMUMAM

Pārliecinieties, ka **darbinieki ir informēti** par šo krāpšanas veidu un apzinās riskus.

Instruējiet darbiniekus, kas atbild par rēķinu apmaksu, lai **vienmēr pārbaudītu to atbilstību noteiktajam.**

Ieviesiet **procedūras** maksājumu pieprasījumu pamatotības pārbaudei.

Pārskatiet uzņēmuma tīmekļa vietnē publicēto informāciju, jo īpaši kontaktinformāciju un piegādātājus. Nodrošiniet, ka darbinieki ierobežo savos kontos par uzņēmumu publicēto.

KĀ DARBINIEKS

Pārbaudiet visus pieprasījumus, kas saistīti ar kreditoriem, jo īpaši, ja viņi lūdz mainīt bankas informāciju turpmākajiem rēķiniem.

Izveidojiet procedūru korekta bankas konta un saņēmēja apstiprināšanai maksājumiem virs noteiktas summas (piemēram, tikšanos).

Saziņā neizmantojiet kontaktinformāciju, kas norādīta vēstulē/faksā/ē-pastā, kurā prasīts veikt izmaiņas. Izmantojiet to, kas atrodama **iepriekšējā sarakstē**.

Kad tiek apmaksāts **rēķins nosūtiet ē-pastu, lai informētu saņēmēju**. Drošībai norādiet saņēmējbankas vārdu, kā arī konta, par kuru esat vienojušies, pēdējos četrus ciparus.

Izveidojiet **īpašu vienotu saziņas punktu** uzņēmumiem kuriem regulāri veicat maksājumus.

Ierobežojiet informāciju par darba devēju ar kura dalāties sociālajos tīklos.

! Ziņojiet policijai konstatējot krāpšanu, pat ja neesat cietis.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · Latvijas Valsts Policija · Finanšu Nozares Asociācija

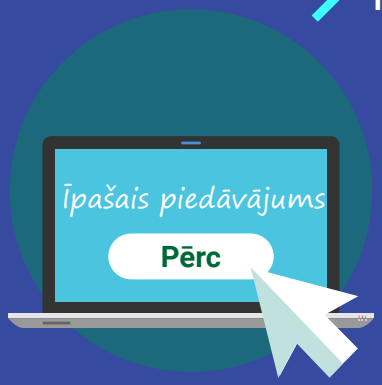
#CyberScams

TIEŠSAISTES IEPIRKŠANĀS KRĀPŠANA

Tiešsaistes darījumi bieži vien ir labs pirkums, bet uzmanieties no krāpšanas.

KĀ JUMS RĪKOTIES?

- Ja iespējams, **izmantojiet vietējās mazumtirdzniecības tīmekļa vietnes** – būs lielāka iespēja, ka jūs varēsiet atrisināt problēmas.
- **Veiciet izpēti** - pārbaudiet atsauksmes pirms pirkšanas
- **Izmantojiet norēķinu kartes** - jūsu iespējas atgūt naudu būs lielākas.
- **Maksājiet tikai izmantojot drošu norēķinu pakalpojumu** - Vai viņi lūdz naudas pārveduma pakalpojumu vai pārskaitījumu? Padomājiet divreiz!
- Maksājiet tikai esot pieslēgts **drošam internet savienojumam** - izvairieties izmantot atvērtu, publisku WiFi.
- **Maksāšanai izmantojiet drošu ierīci** - jauniniet jūsu operētājsistēmu un drošības programmatūru.



- **Uzmanieties no reklāmām, kas piedāvā neprātīgus darījumus vai brīnumproduktus**. Ja tas izklausās pārāk labi, lai tā būtu, tā droši vien arī ir!
- Uznirstošā reklāma, kurā norādīts, ka esat laimējis balvu? **Padomājiet divreiz**, jūs varētu laimēt ļaunatūru.
- Ja produkts netiek piegādāts, sazinieties ar tirgotāju. Ja nav atbildes, **sazinieties ar savu banku**.

! Ziņojiet policijai par aizdomām par krāpšanu, pat ja neesat cietis.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

LATVIJAS VALSTS POLICIJA

FINANŠU NOZARES ASOCIĀCIJA

#CyberScams

BANKU PIKŠĶERĒŠANAS Ē-PASTI

Pikšķerēšana nozīmē krāpnieciskus ē-pastus, kas saņēmēju mudina dalīties ar personas, finansiālu vai drošības informāciju.

KĀ TAS NOTIEK?

Šie ē-pasti:

var izskatīties līdzīgi tai saziņai, kādu sūta īstas bankas.

atdarinot īstā ē-pastā redzamo logo, izkārtojumu un stilu.

prasa lejupielādēt pievienoto failu vai sekot saitei.

veidoti tā, lai radītu steidzamības sajūtu.

KĀ JUMS RĪKOTIES?

- **Regulāri jauniniet programmatūru**, pārlūku, antivīrusu, operētājsistēmu.
- Esiet īpaši **piesardzīgs**, ja "bankas" ē-pasts no jums pieprasa sensitīvu informāciju (piemēram, jūsu internetbankas konta paroli).
- **Rūpīgi aplūkojiet ē-pastu**, salīdziniet adreses ar iepriekš no bankas saņemtajām ziņām. Pārbaudiet gramatikas un valodas kļūdas.
- **Neatbildiet un aizdomīgo ē-pastu**, tā vietā pārsūtiet to uz banku pašrocīgi ievadot bankas adresi.
- **Nesekojiet saitei vai nelejupielādējiet pielikumu**, tā vietā ievadiet adresi pārlūkā.
- Ja rodas šaubas, **pārbaudiet informāciju** bankas tīmekļa vietnē vai telefoniski.

Noziedznieki paļaujas uz cilvēku aizņemtību. Virspusēji novērtējot viltotie ē-pasti izskatās kā īsti.

Uzmanieties izmantojot mobilās iekārtas. Pamanīt pikšķerēšanas mēģinājumu telefonā, vai planšetdatorā būs grūtāk.

#CyberScams

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

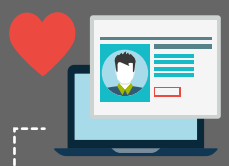
LATVIJAS VALSTS POLICIJA

FINANŠU NOZARES ASOCIĀCIJA

ROMANTISKĀ KRĀPŠANA

Krāpnieki meklē upurus tiešsaistes iepazīšanās vietnēs, bet var izmantot arī sociālos tīklus vai sazināties ē-pastā.

KAM JĀDARA UZMANĪGU?



Kāds, ko nesen sastapāt tiešsaistē, izrāda spēcīgu pieķeršanos un aicina tērzēt privāti.

Viņu sūtītās ziņas bieži ir ar kļūdām un neskaidras.

Izveidotais profils tiešsaistes vietnē īsti neatbilst tam, ko viņi stāsta.

Viņi var lūgt jūs nosūtīt intīma rakstura fotogrāfijas vai video.

Iesākumā viņi iegūst jūsu uzticēšanos, tad prasa naudu, dāvanas, bankas piekļuves vai norēķinu kartes datus.

Ja nedosiet viņiem naudu, viņi var jūs šantažēt. Ja dosiet, viņi prasīs vēl.

ESI KĻUVIS PAR UPURI?

Nesamulsti!
Nekavējoties pārtrauc jebkādu saziņu.
Ja iespējams, saglabā saziņu, piemēram, ierakstus tērzētavā.
Iesniedz pieteikumu policijā.
Informē vietni, kur pirmo reizi krāpnieki ar Tevi sazinājās
Ja esi izpaudis bankas datus, sazinies ar savu banku.

KĀ JUMS RĪKOTIES?

- **Rūpīgi izvērtējiet** cik daudz informācijas par sevi publicējat sociālajos tīklos un iepazīšanās vietnēs.
- **Apzinieties iespējamo risku.** Krāpnieki darbojas visās pazīstamākajās vietnēs.
- **Nesteidzieties** un uzdodiet jautājumus
- **Izpētiet,** vai profila fotogrāfijas un informācija nav izmantota citur.
- **Pievērsiet** uzmanību rakstības un gramatikas kļūdām, nesakritībām stāstos un atrunām, tādām, kā nestrādājoša kamera.
- **Nedalieties** ar jebkādu materiālu, ko vēlāk varētu izmantot jūsu šantāžai.
- Ja piekrītat satikties, **informējiet draugus un radiniekus**, kurp dodaties.
- **Uzmanieties naudas prasīšanas gadījumā.** Nekad nesūties naudu, nenododiet norēķinu karšu datus, konta piekļuves datus, vai dokumentu kopijas.
- **Izvairieties no priekšapmaksas maksājumiem.**
- **Neveiciet pārskatījumus** pēc kāda līguma. Naudas atmazgāšana ir noziedzīgs nodarījums.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | Latvijas Valsts Policija | Finanšu Nozares Asociācija

#CyberScams

BANKU PIKŠĶERĒŠANAS SMS

Smikšķerēšana (vārdu SMS un pikšķerēšana kombinācija) ir krāpnieku mēģinājums iegūt personīgu, finansiālu vai drošības informāciju, izmantojot īsziņas.

KĀ TAS NOTIEK?

Īsziņā parasti būs aicinājums sekot saitei vai zvanīt uz norādīto tālruņa numuru, lai "pārbaudītu", "atjauninātu" vai "atkārtoti aktivizētu" jūsu kontu. Bet... saite ved uz fiktīvu tīmekļa vietni, un telefona numurs noved pie krāpnieka, kas izliekas par patieso uzņēmumu.

KĀ JUMS RĪKOTIES?

- **Neklikšķiniet uz saitēm, pielikumiem vai attēliem**, ko saņemat negaidītās īsziņās pirms pārliecinieties par sūtītāja identitāti.r.
- **Nesasteidziet.** Pirms reaģēšanas veltiet laiku un veiciet atbilstošas pārbaudes.
- **Nekad neatbildiet uz īsziņu**, kas pieprasa jūsu PIN vai jūsu internetbankas paroli vai citus piekļuves datus.
- Ja domājat, ka, iespējams, esat atbildējis uz smikšķerēšanas īsziņu un, izpaudis bankas informāciju, **nekavējoties sazinieties ar savu banku**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

LATVIJAS VALSTS POLICIJA

FINANŠU NOZARES ASOCIĀCIJA

#CyberScams

VILTOTA BANKAS TĪMEKĻA VIETNE

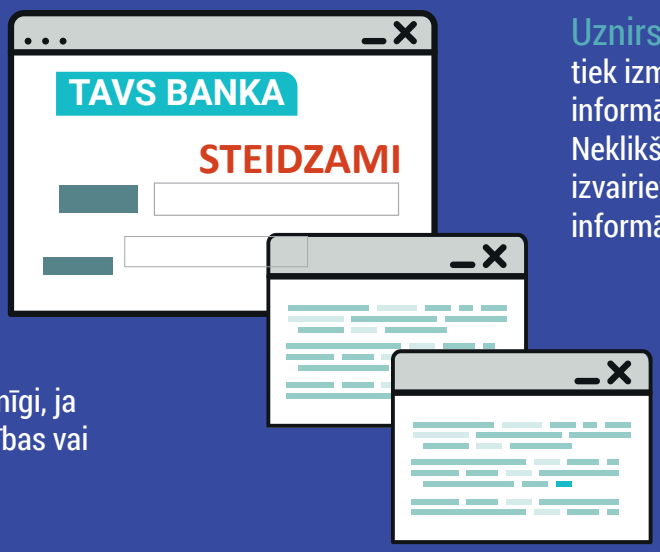
Pikšķerēšanas ē-pasti bankas vārdā parasti satur saites uz viltotu bankas tīmekļa vietni, kur visbiežāk prasīs izpaust personīgu vai finansiālu informāciju.

KAM JĀDARA UZMANĪGU?

Viltotas banku tīmekļa vietnes izskatās gandrīz identiskas īstajām. Šādās vietnēs bieži tiek izmantoti uznirstošie logi, prasot ievadīt bankas piekļuves informāciju. Īstas bankas šādi nerīkojas.

Šajās tīmekļa vietnēs parasti ieraudzīsiet:

Steidzamību: šādas ziņas neatradīsiet īstās vietnēs.



Uznirstošie logi: tie parasti tiek izmantoti sensitīvas informācijas pieprasīšanā. Neklikšķiniet uz tiem un izvairieties no personīgās informācijas ievades tajos.

Nepilnīgs izskats: esiet uzmanīgi, ja vietnes izskatā manāmas nepilnības vai redzamas rakstības kļūdas.

KĀ JUMS RĪKOTIES?

Neklikšķiniet uz ē-pastos ietvertajām saitēm uz bankas tīmekļa vietni.

Vienmēr ievadiet saiti pats, vai izvēlieties iepriekš izmantotu saiti no jūsu "favorītu" saraksta.

Izmantojiet pārlūku, kas ļauj **bloķēt uznirstošos logus**.

Par to, kas tiešām svarīgs, saņemsiet paziņojumu, **kad pieslēgsieties jūsu bankas tiešsaistes vietnei**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

Latvijas Valsts Policija

FINANŠU NOZARES ASOCIĀCIJA

#CyberScams

BANKU VIKŠĶERĒŠANAS ZVANI

Vikšķerēšana (vārdu balss (voice) un pikšķerēšanas apvienojums) ir telefona krāpšana, kurā krāpnieki mēģina pierunāt upuri personiskās, finanšu vai drošības informācijas izpaušanai vai naudas pārskaitīšanai.

KĀ JUMS RĪKOTIES?

- **Uzmanieties** no neiederīgiem telefona zvaniem.
- **Pierakstiet zvanītāja numuru** un piedāvājiet atzvanīt.
- Lai pārliecinātos par zvanītāja identitāti, **sameklējiet organizācijas telefona numuru** un sazvaniet to.
- **Nepārbaudiet zvanītāju, izmantojot jums sniegto tālruņa numuru** (tas varētu būt neīsts nepatiess numurs).
- Krāpnieki var atrast pamata informāciju par jums tiešsaistē (piemēram, sociālajos tīklos). **Nepieņemiet, ka zvanītājs ir īsts** tikai tāpēc, ka viņi zina detaļas.
- **Nedalieties** ar norēķinu kartes PIN kodu vai internetbankas paroli. Jūsu banka nekad neprasīs šādu informāciju.
- **Nepārskaitiet naudu** uz svešu kontu pēc šāda pieprasījuma. Jūsu banka nekad neprasīs, lai jūs to darāt.
- Ja jūs domājat, ka zvans ir fiktīvs, informējiet par to **savu banku.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

Latvijas Valsts Policija

FINANŠU NOZARES ASOCIĀCIJA

#CyberScams