# 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.

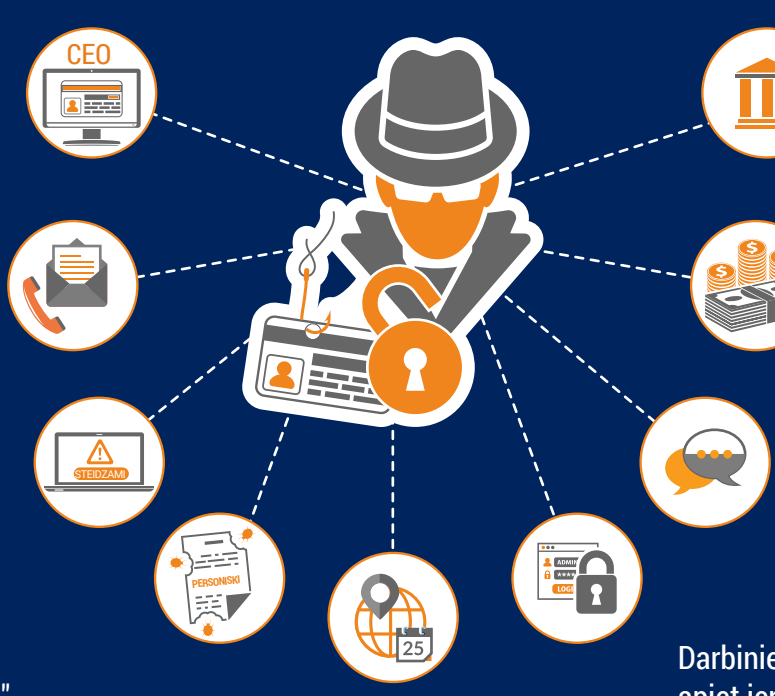
## KĀ TAS NOTIEK?

Krāpnieks piezvana vai sūta e-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 sniegt cita persona vai tie var tikt atsūtīti e-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** e-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 e-pasta adreses**.

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

**Neatveriet** e-pastā saņemtās **aizdomīgas saites vai pielikumus**. Jo īpaši uzmanieties, pieslēdzoties privātajam e-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 e-pastu, informējiet IT struktūrvienību.

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

#CyberScams