

KIBERDROŠĪBAS EKSELENCES CEĻVEDIS



Kampanu
organizē:



Aizsardzības ministrija



Nacionālais
kiberdrošības
centrs



NCC-LV

LATVIJAS KIBERDROŠĪBAS
KOORDINĀCIJAS CENTRS



ECCC

EIROPAS KIBERDROŠĪBAS
KOMPETENCĀU CENTRS



Līdzfinansē
Eiropas Savienība

Kas ir kiberdrošība?

Kiberdrošība ir spēja nezaudēt modrību, lai neviens tevi nevarētu viegli apvest ap stūri.

Kibernoziedznieki ir tie, kuri mēģina ielīst datoros, telefonos, tavos interneta mākoņos un bankas kontos.

Ko viņi tur dara? Vienkārši – grib, lai tavi dati un naudiņa kļūst par viņējo.

Kiberdrošības uzdevumi:

1. Pasargāt savu naudu – bankas kontu, maksājumu kartes, visu, kas ir “makā”.
2. Nosargāt savu privātumu no paroles zagļiem, datu noplūdes vai izspiedējiem.
3. Sargāt bērnus no krāpniekiem, kaitīga satura un viltus draudzībām internetā.
4. Saglabāt tavas bildes, dokumentus un kontaktus, jo ļaunatūra var tos vienkārši izdzēst.
5. Glābt savu reputāciju – uzlauzts profils var pārvērsties par tevi, tikai ļoti muļķīgā versijā.

Kas ir kiberuzbrukums?

Kiberuzbrukums ir ļoti sliktas ziņas, ja vien neesi tam gatavs. Iedomājies, ka tavā mājā laužas iekšā krimināli personāži. Kamēr tu pats turpat vienā mierā cep pankūkas vai plūncājies vannā, viņi rakņājas pa tavām atvilktnēm un seifu. Tieši tāpat kiberuzbrukums var notikt tavā telefonā vai datorā.

Kas ir viņu mērķis?

- Tava naudiņa
- Tavi dati, lai tiktu pie tavas naudiņas
- Tava ierīce, lai to pievienotu "zombiju tīklam", ar ko uzbrukt citām iekārtām



Biežāk sastopamie kiberuzbrukumu veidi

Pikšķerēšana

Krāpnieki uzdodas par uzticamu personu vai organizāciju, lai iegūtu tavas paroles, bankas datus vai kredītkartes numuru.

Kā tas notiek:

Tu saņem e-pastā ziņu: "Tavs bankas konts tiks bloķēts, ja nepieslēgsies tūlīt." E-pastā ir viltota saite, kas izskatās kā īsta banka, bet nav. Tu ievadi savus datus, un tie nonāk krāpnieku rokās.

Vikšķerēšana

Krāpnieki zvana, uzdodoties par kādu banku, valsts iestādi vai pakalpojumu sniedzēju.

Kā tas notiek:

Tu saņem zvanu: "Labdien, no jūsu konta notiek aizdomīgs maksājums. Lūdzu, pasakiet kartes numuru un PIN kodu, lai to apturētu." Ja tu pasaki šos datus, naudu var nozagt.

Smikšķerēšana

Krāpnieciski teksta ziņojumi (SMS, *WhatsApp*, *Slack*, *iMessage*, *Facetime* u. c.).

Kā tas notiek:

Tu saņem īsziņu: "Jūsu pakas piegāde aizkavēta. Spiediet šeit, lai apstiprinātu: [viltota saite]" Ja tu uzspied, var notikt divas lietas: 1) tu ievadi savus datus, un tie nonāk pie krāpniekiem. 2) tiek lejupielādēta ļaunatūra, kas apdraud tavu ierīci.

Apmaksāti meklēšanas rezultāti

Krāpnieki pērk reklāmas meklētājos (*Google, Bing*), lai viņu viltotās vietnes parādītos pašā augšā, uzdodoties par bankām vai pazīstamiem uzņēmumiem.

Kā tas notiek:

Tu ieraksti meklētājā savu mīļāko bikšu zīmolu un klikšķini uz pirmā rezultāta. Lapa izskatās īsta, bet ir viltota. Tu gribi nopirkt vēl vienas bikses, ievadi savus datus, un tie nonāk pie krāpniekiem.

Krāpnieciskas reklāmas sociālajos tīklos

Sociālajos tīklos parādās apmaksātas reklāmas, kas sola ātru peļņu, "izdevīgus ieguldījumus" vai neparastus piedāvājumus.

Kā tas notiek:

Tu redzi reklāmu ar piedāvājumu, kurš ir tik labs, ka neliekas īsts. Tieši tā arī ir – tas nav īsts. Tu noklikšķini un nonāc krāpnieku lapā. Tur tu ievadi datus vai atstāj kontakthinformāciju, ko krāpnieki izmanto savā labā.

Ļaunatūra

Tā ir ļaundabīga programmatūra, kas inficē lietotāja ierīci, lai zagtu paroles, izspiegotu darbības, šifrētu failus vai rādītu nevēlamas reklāmas.

Kā tas notiek:

Tu atver aizdomīgu pielikumu vai saiti, un tavā datorā nonāk

vīruss. Tas var izspiegot tavas darbības (*spyware*), bloķēt failus un pieprasīt izpirkumu (*ransomware*) vai piespiedu kārtā rādīt reklāmas (*adware*).

Botneti

Botnets ir robotu tīkls, ko veido ar ļaunatūru inficētas ierīces, kuras darbojas uzbrucēja kontrolē.

Kā tas notiek:

Tavs dators kļūst par "zombiju" un bez tavas ziņas piedalās ļaunprātīgās darbībās – izsūta spama vēstules, izplata vīrusus vai veic DDoS uzbrukumus, kas var bloķēt, piemēram, ziņu portāla pieejamību.

Wi-Fi novērošana (*Wi-Fi Eavesdropping*)

Publiskos un neaizsargātos Wi-Fi tīklos ļaundari var pārtvert lietotāju informāciju.

Kā tas notiek:

Tu pieslēdzies kafejnīcas Wi-Fi un ievadi savus piekļuves datus. Ja savienojums nav šifrēts, ļaundaris var tos pārtvert un piekļūt tavām parolēm vai pat datoram. Drošībai ieteicams lietot VPN.

Kāpēc kiberdrošība ir svarīga arī tev

Filmās un seriālos bieži rāda, ka kiberdrošība ir valdību, banku un hakeru karš tumšos pagrabos. Bet realitātē – tu esi mērķis. Jā, tieši tu.

Kibernoziedzniekiem nevajag īpaši izvēlēties – viņi vienkārši šauj pa masām. Viens e-pasts aiziet tūkstošiem cilvēku, un pietiek, ka daži uzķeras, lai krāpnieki tiktu pie naudas vai tavas identitātes.



Kā pamanīt, ka esi cietis no kiberuzbrukuma?

1. Paroles pēkšņi vairs nestrādā, un pa tavu kontu šiverē kāds cits.
2. Telefons vai dators paliek aizdomīgi lēns.
3. Saņem rēķinus par lietām, ko neesi pircis.
4. Tavi draugi sūdzas par dīvainām ziņām, kas it kā nosūtītas no tevis.
5. Uz ekrāna parādās šantāža: "Maksā vai faili būs čau!"



Ko darīt, ja esi kļuvis par kiberuzbrukuma upuri?

1. Rikojies nekavējoties

- Atvieno ierīci no interneta.
- Pārtrauc saziņu ar krāpniekiem.
- Ja esi nodevis maksājumu vai konta datus – nekavējoties informē savu banku.

2. Nodrošini ierīces un kontus

- Pārbaudi ierīci ar antivīrusu.
- Nomaini paroles (īpaši e-pastam, bankai, sociālajiem tīkliem) no drošas ierīces.
- Aktivizē divfaktoru autentifikāciju (2FA).

3. Seko līdz finansēm

- Regulāri pārbaudi bankas kontu.
- Par aizdomīgiem darījumiem ziņo bankai un lūdz bloķēt pieeju.

4. Saglabā pierādījumus

- Fiksē datumu, laiku, notikušo.
- Saglabā e-pastus, īsziņas, ekrānšāviņus un citus pierādījumus.

5. Ziņo atbildīgajām iestādēm

- CERT.LV, Valsts policijai, savai bankai, sociālo tīklu atbalsta dienestiem.

Pārbaudi, cik pasargāts esi

- ☐ Man ir sarežģīta un gara parole ar vismaz 15 lielajiem, mazajiem burtiem, cipariem un simboliem.
- ☐ Katram kontam man ir sava parole.
- ☐ Es izmantoju divfaktoru autentifikāciju (2FA) ar kodu SMS vai lietotnē.
- ☐ Es neatveru e-pastus un saites no svešiem sūtītājiem.
- ☐ Es regulāri veicu atjauninājumus un esmu iestatījis automātisku atjaunināšanu.
- ☐ Es izmantoju atsevišķu bankas karti pirkumiem internetā, kurā ikdienā neglabājas lielas naudas summas.
- ☐ Manā ierīcē ir uzstādīts DNS uguns mūris, kas pasargā no viltus banku lapām, krāpnieciskām tirdzniecības platformām un vīrusus izplatošām vietnēm.
- ☐ Es zinu, ka DNS uguns mūri var izmantot bez maksas vietnē DNSmuris.lv.

BĒRNU drošības riski internetā



leivilināšana lamatās (*grooming*) – svešinieks izliekas par bērna vienaudzi, iegūst uzticību un pēc tam izmanto, lai iegūtu kailfoto, video vai piespiestu satikties.

Kibermobings – bērna sistemātiska apcelšana internetā ar aizvainojošiem komentāriem, bildēm vai video, bieži publiski.

Kaitīgs saturs – pornogrāfija, vardarbība, rupjības, maldinoša vai bīstama informācija, kas var nobiedēt, radīt trauksmi vai sagrozīt izpratni par attiecībām.

Krāpniecība – viltoti konkursi, pikšķerēšanas e-pasti, viltus paziņojumi spēlēs, lai izkrāptu naudu vai paroles.

Privātu datu izpaušana – vārda, adreses, skolas vai fotogrāfiju publicēšana, kas var apdraudēt bērna drošību.

Sekstings – bērns pats nosūta savus kailfoto vai video, kas var tikt izplatīti tālāk un izmantoti šantāžai.

Pārmērīga ierīču lietošana – pārlietu ilga sēdēšana pie ekrāna, kas ietekmē miegu, mācības, pašsajūtu un sociālās prasmes.

Kā pasargāt bērnu no kiberuzbrukuma?

1. Saruna

Sarunājies ar bērnu, stāsti par drošību internetā un aicini vienmēr nākt pie tevis – jautāt, rādīt, pastāstīt vai atzities.

2. Izlasiet virtuālās drošības ABC

Reizē ar pirmo viedtālruni iepazīstini bērnu ar elementāriem padomiem no vietnes: Drossinternets.lv

3. Drošības un privātuma iestatījumi

Pārlicinies, ka visās bērna lietotajās viedierīcēs ir ieslēgti drošības un privātuma aizsardzības rīki: piekļuves kods vai parole, vecāku kontroles iespējas, lietotņu lejupielādes ierobežojumi un droši privātuma iestatījumi sociālajos tīklos.

4. Cieņa

Izskaidro, cik svarīgi arī internetā izturēties ar cieņu, nedarīt otram to, ko negribi, lai nodara tev.

5. Domā pirms *like* un *share*

Labāk būt piesardzīgam nekā apdraudētam. Iemāci bērnam pārbaudīt faktus, nešērot visu pēc kārtas un neklikšķināt uz aizdomīgām saitēm.

6. **Draudzība internetā**

Skarbi, bet vajadzīgi – paskaidro, ka internetā uzturas arī ļauni tipi un ka nekad, nekad nevajag uzticēties svešiniekiem internetā, apstiprināt draudzības un sūtīt savas bildes.

7. **Ekrāna laiks**

Uzraugi, cik daudz laika bērns pavada pie ekrāniem, lai viņam neveidotos atkarība un piekļuve viedierīcēm nekļūtu nekontrolēta.

Kam ziņot?

Ziņo un konsultējies ar **Drossinternets.lv**

Uzticības tālrunis **116111**



Kiberdrošības riski senioriem

- Internetā iepazīti "draugi", kas sāk prasīt naudu.
- "Jūs esat vinnējis loterijā", tikai jāsamaksā nodeva.
- Zvanītāji uzdodas par komunālo pakalpojumu sniedzējiem un piedraud atslēgt elektrību vai gāzi, ja netiks veikts tūlītējs maksājums.
- Krāpnieki ar balss klonēšanas palīdzību uzdodas par radniekiem vai mazbērniem, kuriem "steidzami vajadzīga nauda" drošības naudas, ārstēšanās vai ceļojuma izdevumu segšanai.
- Maldinoši e-pasti un īsziņas, kas šķiet no bankas, valsts iestādes vai pazīstama uzņēmuma, mudinot klikšķināt uz saitēm vai lejupielādēt pielikumus.
- Pieklājīgs cilvēks ar jauku balsi aicina investēt un sola lielu peļņu.

Kā sevi pasargāt?

1. Nekad nenosauc PIN kodus vai paroles.
2. Ja zvana "banka" – noliec klausuli un pārzvani uz bankas oficiālo numuru.
3. Ja piedāvājums šķiet pārāk labs – tā ir krāpniecība.
4. Vienmēr pārrunā aizdomīgus zvanus ar tuviniekiem.
5. Neļauj svešiniekiem attālināti pieslēgties tavam datoram vai telefonam.
6. Bloķē aizdomīgus zvanītājus un izmanto zvanu filtrēšanas iespējas telefonā.
7. Regulāri pārlūko savus bankas izrakstus, lai savlaicīgi pamanītu aizdomīgus darījumus.

Kiberdrošība uzņēmumā

Biežākie riski

- Pikšķerēšana un darbinieku datu noplūde.
- Šifrējošie izspiedējvīrusi.
- Viltus rēķini un maksājumu krāpšana.

Kā pasargāties?

- Lieto drošas paroles un divfaktoru autentifikāciju (2FA).
- Organizē regulāras darbinieku apmācības par kiberdrošību.
- Veido regulāras datu rezerves kopijas un pārliedzinies, ka tās darbojas.
- Aizsargā ierīces – bloķē ekrānus, nelieto svešus USB, regulāri atjaunini programmatūru.
- Izveido skaidras procedūras maksājumu apstrādei, lai novērstu krāpnieciskus pārskaitījumus.
- Izmanto elektroniski parakstītus dokumentus, lai izvairītos no viltojumiem.
- Ja atver aizdomīgu saiti vai pielikumu – atvieno datoru no tīkla un nekavējoties ziņo IT speciālistam.

Kur vērsties, ja noticis kiberuzbrukums

1. Krāpnieku e-pasts vai SMS

Saņēmi krāpniecisku e-pastu vai SMS (pikšķerēšana, viltus saites).

Redzi viltotu timekļa vietni, kas izliekas par banku, e-parakstu u. c.

Tava ierīce uzvedas aizdomīgi vai, iespējams, ir inficēta ar vīrusu.

Ziņo CERT.LV:

- raksti uz cert@cert.lv

- zvani uz 24/7 tālruni 67085888

- pārsūti krāpnieciskus SMS un telefona numurus uz +371 23230444 (telefona zvani netiek apstrādāti)

2. Izspiešana, šantāža

Ir nozagti vai ļaunprātīgi izmantoti tavi personas dati vai identitāte.

Uzbrucējs draud, izspiež vai publicē tavu personīgo informāciju.

Ziņo Valsts policijai:

- zvani 110

- raksti ziņu e-adresē, sūti elektroniski parakstītu e-pastu <https://www.vp.gov.lv/lv/ka-zinot-policijai>

3. Draudi bērnam

Apdraudēts bērns internetā (mobings, seksuāla rakstura sarakstes u. c.).

Nepieciešams atbalsts un padomi, kā runāt ar bērnu par drošību internetā.

Sazinies ar Latvijas Drošāka interneta centru:

- konsultatīvais tālrunis 116111 (bērnu un jauniešu uzticības tālrunis)

- ziņo par saturu ziņot.drossinternets.lv

4. Valsts drošība

Ja ir aizdomas par valsts drošības apdraudējumu kibertelpā.

Ja zini par mēģinājumiem spiegot, apdraudēt valsts informācijas sistēmas vai par pretvalstisku darbību internetā.

Ziņo Satversmes aizsardzības birojam:

raksti uz pasts@sab.gov.lv

5. Naida runa un terorisms

Ja ir aizdomas par radikalizāciju internetā, aicinājumiem uz vardarbību, terorismu vai naida runu.

Ja redzi, ka sociālajos tīklos kāds izplata dezinformāciju, kas apdraud valsti, vai darbojas pret Latvijas interesēm.

Ziņo Valsts drošības dienestam:
raksti uz vdd@vdd.gov.lv

6. Krāpniecība interneta veikalā

Ja interneta veikalā:

- esi apkrāpts kā pircējs (piemēram, nesaņem preci)
- redzi nepatiesu vai maldinošu reklāmu
- tiek pārkāptas tavas kā patērētāja tiesības

Ja digitālie pakalpojumi (abonementi, lietotnes utt.) nepilda solīto vai pārkāpj noteikumus.

Ziņo Patērētāju tiesību aizsardzības centram:
raksti uz ptac@ptac.gov.lv

7. Datu un identitātes zādzība

Ja tavi personas dati (vārds, adrese, personas kods u. c.) ir noplūduši vai nozagti.

Ja kāds izmanto tavu identitāti.

Ja kāds bez tavas atļaujas izmanto tavu informāciju.

Ja tu nevari piekļūt saviem datiem, kurus glabā uzņēmums vai iestāde.

Ja vēlies, lai datu pārvaldītājs izdzēs tavu informāciju, bet viņi to nedara.

Ziņo Datu valsts inspekcijai:

raksti pasts@dvi.gov.lv

8. Dezinformācija

Ja ikdienā pamani maldinošu informāciju, sagrozītus faktus vai mērķtiecīgus centienus manipulēt, lai veiktu krāpnieciskas darbības.

Ziņo platformai "Meln uz balta": aizpildi anketu lietotnē <https://melnsuzbalta.lv/zino-par-dezinformaciju/>

9. Finansiāla krāpniecība

Ja ir notikusi finansiāla krāpšana, piemēram, esi pārskaitījis naudu krāpniekiem.

Sazinies ar savu banku un ziņo Valsts policijai:

zvani 110

Noderīgas vietnes

- Drossinternets.lv – par bērnu drošību.
- CERT.LV – padomi un brīdinājumi.
- Esidross.lv – video un raksti par drošību.
- Financelatvia.eu – finanšu drošības ieteikumi.
- Uzticibastalrunis.lv – psihologa atbalsts bērniem interneta problēmsituācijās.
- Naudasskola.lv – finanšu drošība.
- Melnusuzbalta.lv – Valsts kancelejas padomi dezinformācijas atpazīšanai un apkarošanai.
- Manadrosiba.lv – Valsts policijas padomi drošībai internetā.
- lvrtc.lv/digituvi/catins/ – LVRTC (Latvijas Valsts radio un televīzijas centrs) padomi drošai viedtālrunu lietošanai.
- Dnsmuris.lv – drošības rīks aizsardzībai pret kiberapdraudējumiem.

Informatīvi
atbalsta:



DROSS
INTERNETS.LV

FINANŠU
NOZARĒS
ASOCIĀCIJA



Pasts



NARVESEN

Imt



NESTE