

Tavam bērnam sola
bezmaksas balvas?

Ož pēc shēmas!



**KIBERDROŠĪBAS
EKSELENCES
FONDS**

ĢIMENĒM AR BĒRNIEM

Kibernoziedznieki mēģina ielist datoros, telefonos, interneta mākoņos un bankas kontos, lai cilvēku dati un nauda kļūtu par viņējo.

Kiberdraudi bērniem

- **Grooming:** pieaugušais uzdodas par vienaudzi un manipulē ar bērnu, lai panāktu satikšanos vai iesaistītu viņu intimās sarunās.
- **Kiberhulīgānisms:** apcelšana, izsmiešana vai draudi internetā, bieži publiski.
- **Kaitīgs saturs:** pornogrāfija, vardarbība, atkarību veicinošas spēles, kas var emocionāli traumēt.
- **Krāpniecība:** viltoti konkursi, balvas vai spēles, kurās prasa naudu vai datus.

Pašu radītie iespējamie draudi. No kā uzmanīties?

- **Privātu datu izpaušana:** vārda, adreses, skolas vai fotogrāfiju publicēšana.
- **Sekstings:** bērns nosūta savus kailfoto vai video, kas var tikt izplatīti un izmantoti šantāžai.
- **Pārmērīga ierīču lietošana:** pārlieku ilgs laiks pie ekrāniem ietekmē miegu, pašsajūtu un sociālās prasmes.

Kā pasargāt bērnu no kiberuzbrukuma?

- **Saruna.** Aicini vienmēr nākt runāt, jautāt, rādīt, pastāstīt, atzīties. Nekad nenosodi un nepārmet.
- **Virtuālās drošības ABC.** Iepazīstini bērnu ar padomiem no **drossinternets.lv**.
- **Iestatījumi.** Aktivizē piekļuves kodus, paroles, vecāku kontroli, ierobežojumus un privātuma iestatījumus. Informāciju, kā to paveikt, meklē **drossinternets.lv** sadaļā "Materiāli".
- **Cieņa.** Māci bērnam, ka nevar darīt otram to, ko negribi, lai nodara tev.
- **Domā pirms like un share.** Atgādini pārbaudīt faktus, *nešērot* visu pēc kārtas, neklikšķināt uz aizdomīgām saitēm.
- **Draudzība internetā.** Izskaidro, ka nekad nedrīkst komunicēt un apstiprināt draudzības aicinājumus no svešiniekiem.
- **Ekrāna laiks.** Uzraugi, cik daudz laika bērns pavada pie ekrāniem.

Noderīgi

Drossinternets.lv par bērnu drošību digitālajā vidē

CERT.LV padomi un brīdinājumi par Latvijā aktuālām krāpšanas kampaņām

Uzticibastālrunis.lv psihologa atbalsts bērniem problēmsituācijās

Dnsmuris.lv bezmaksas rīks individuālu lietotāju pasargāšanai no kiberapdraudējumiem

Zīņo un konsultējies

Drossinternets.lv

Uzticības tālrunis 116111
Valsts policija 110



Aizsardzības ministrija



Nacionālais
kiberdrošības
centrs



CERT.LV
Kiberincidentu
novēršanas institūcija



NCC-LV
NACIONĀLAIS KIBERDROŠĪBAS
CENTRS



ECCC
EUROPA KIBERDROŠĪBAS
KOMETENCĪJU CENTRS



Līgumdarb
Eiropas Savienība



DROSS
INTERNETS.LV

Tevi steidzina un liek
pieņemt lēmumu uzreiz?

Ož pēc shēmas!



**KIBERDROŠĪBAS
EKSELENCES
FONDS
UZŅĒMUMIEM**

Kibernoziedznieki mēģina ielist datoros, telefonos, interneta mākoņos un bankas kontos, lai cilvēku dati un nauda kļūtu par viņējo. Uzņēmumi un iestādes glabā svarīgus datus. Ja šie dati noplūst vai tiek bloķēti, sekas var būt nopietnas.

Kiberdraudi uzņēmumiem un iestādēm

- **Pikšķerēšana (phishing)** – krāpnieciski e-pasti vai ziņas, kas izliekas par banku, kolēģi vai partneri, lai iegūtu paroles vai piekļuvi sistēmām.
- **Izspiedējvīrusi (ransomware)** – bloķē datorus vai failus un pieprasa izpirkuma maksu.
- **Datu noplūdes** – neatļauta piekļuve darbinieku vai klientu datiem.
- **Caura programmatūra** – tā ir novecojusi vai netiek atjaunota un paver durvis uzbrucējiem.
- **Viltus rēķini un krāpniecība** – īpaši bieži vērsti pret iestādēm un uzņēmumiem.

Kā pasargāt uzņēmumus un iestādes no kiberuzbrukumiem?

- **Paroles** – drošas, katram kontam sava. Ieteicams lietot paroli pārvaldniekus un divfaktoru autentifikāciju (2FA).
- **Ierīču aizsargāšana** – bloķē ekrānus, nelieto svešus USB, regulāri atjaunini programmatūru.
- **Rezerves kopijas (backups)** – taisi regulāras datu rezerves kopijas un pārliecinies, ka tās darbojas, jo tas ir vienīgais drošais veids, kā atgūties pēc izspiedējvīrusa uzbrukuma.
- **Drošības politika** – noteikumi, ko visi darbinieki zina un ievēro, skaidras procedūras maksājumu apstrādei, elektroniski parakstītu dokumentu izmantošana.
- **Darbinieku apmācības** – organizē un apmeklē regulāras darbinieku apmācības par kiberdrošību.

Kā rīkoties, ja ir aizdomas par kiberuzbrukumu?

- Ja atver aizdomīgu saiti vai pielikumu – **atvieno datoru** no tīkla.
- **Ziņo** IT speciālistam vai atbildīgajam par kiberdrošību.
- **Apkopo digitālos pierādījumus** – tas palīdzēs saprast, kas notika un ko darīt, lai tas neatkārtotos nākotnē. Sazinies ar **CERT.LV**, viņi izskaidros, kā to pareizi izdarīt.

Noderīgi

CERT.LV padomi, brīdinājumi un bezmaksas pakalpojumi uzņēmumiem/iestādēm, kas ir Nacionālās kiberdrošības likuma subjekti

Financelatvia.eu finanšu drošības ieteikumi

rokasgramata.esidross.lv noderīgi kiberdrošības padomi darbiniekiem un darba devējiem

Dnsmuris.lv bezmaksas drošības rīks aizsardzībai no kiberapdraudējumiem

Ja notikusi **finanšu krāpniecība** – uzreiz operatīvi ziņo savai **bankai**, tad **Valsts policijai**

Ja noticis **kiberdrošības incidents** – sazinies ar **CERT.LV**

Tev zvana un prasa
kartes datus?

Ož pēc shēmas!



**KIBERDROŠĪBAS
EKSELENCES
FONDS
SENIORIEM**

Kibernoziedznieki mēģina ielist datoros, telefonos, interneta mākoņos un bankas kontos, lai cilvēku dati un naudiņa kļūtu par viņējo.

Kiberdraudi senioriem – populārākās situācijas

- Zvanītāji **izliekas par komunālo pakalpojumu sniedzējiem** un piedraud atslēgt elektrību vai gāzi, ja netiks veikts tūlītējs maksājums.
- Krāpnieki ar balss klonēšanas palīdzību **uzdodas par radnieku**, kuram "steidzami vajadzīgs aizdevums" drošības naudas, ārstēšanās vai ceļojuma izdevumu segšanai.
- Maldinoši e-pasti un izsiņas, kas šķiet **no bankas, valsts iestādes vai pazīstama uzņēmuma**, mudinot klikšķināt uz saitēm vai lejupielādēt pielikumus.
- Piekļājīgs cilvēks **jaukā balsi pārliecinoši aicina investēt** un sola lielu peļņu.
- Internetā iepazīti "**draugi**", kas sāk prasīt naudu.
- "**Jūs esat vinnējis loterijā**", tikai jāsamaksā nodeva.

Kā sevi pasargāt no kiberuzbrukuma?

- **Nekad nenosauc PIN kodus vai paroles**, neļauj svešiniekiem pieslēgties attālināti datoram vai telefonam.
- **Neklikšķini uz aizdomīgām saitēm** un regulāri pārlūko savus bankas izrakstus.
- Ja zvana no "bankas" vai "policijas" – noliec klausuli un **pārzvani uz oficiālo numuru**.
- **Apspried aizdomīgus zvanus ar tuviniekiem**. Bloķē aizdomīgus zvanītājus un izmanto zvanu filtrēšanu telefonā.
- **Netici pārāk labiem piedāvājumiem**, jo laimestus un mantojumus par brīvu nedod.

Kiberdrošības pamati

- **Drošas paroles**: katram kontam sava parole – gara un ar dažādiem simboliem.
- **Divu soļu pārbaude (2FA)**: parole + papildu kods telefona lietotnē (piemēram, Google Authenticator)
- **Programmu atjauninājumi**: vienmēr uzstādītas jaunākās versijas.
- **Uzmanība**: pārbaudīt sūtītāja e-pasta adresi un saiti pirms atvēršanas.
- **Drošs Wi-Fi**: lietot tikai savu vai aizsargātu tīklu vai mobilo datus.

Noderīgi

CERT.LV padomi un brīdinājumi par Latvijā aktuālām krāpšanas kampaņām

Esidross.lv video un raksti par drošību internetā

Melnsuzbalta.lv padomi dezinformācijas atpazīšanai un apkarošanai

Dnsmuris.lv bezmaksas rīks individuālu lietotāju pasargāšanai no kiberapdraudējumiem, piemēram, viltus banku tīmekļa vietnēm

Zīņo un konsultējies

CERT.LV

cert@cert.lv
+371 67085888

Valsts policija 110