# Kiberhigiēnas pamati

# Tīkls

## WiFi tīklu konfigurācija un drošības uzstādījumi

Mūsdienu pasaulē ikvienam no mums ir vairākas ar internetu savienotas ierīces, un parasti šādas ierīces tiek savienotas, izmantojot WiFi tīklus. Pieaugot šo ierīču skaitam, ir svarīgi pievērst uzmanību mājas vai darba WiFi tīklu drošībai un korektai konfigurācijai, kas var uzlabot kopējo tīkla drošību un mazināt drošības riskus.

## Ieteikumi

- Nomaini noklusējuma paroles WiFi rūterī.
- Izvēlies garu WiFi paroli no dažādiem simboliem.
- Ierobežo iekārtas, kas var pieslēgties WiFI tīklam – ieslēdz MAC filtrāciju.
- Šifrē WiFi datu pārraidi (WPA2, WPA3).
- Izvēlies unikālu WiFi tīkla nosaukumu.
- Ieslēdz ugunsmūra funkciju.
- Veic regulāru WiFi rūtera operētājsistēmas atjaunināšanu.


## Publisko tīklu riski

Gandrīz ceturtā daļa pasaules publisko WiFi tīklu neizmanto nekāda veida šifrēšanu, līdz ar to padarot šos tīklus par vieglu mērķi hakeriem.
Lielākais drauds publisko un bezmaksas WiFi tīklu drošībai ir hakera spēja pozicionēt sevi starp Tavu iekārtu un WiFi savienojuma punktu. Tā vietā, lai "runātu" tieši ar publisko WiFi tīklu, Tu sūti savu informāciju hakerim, kurš pēc tam to saglabā un izmanto pret Tevi.

## Ieteikumi

- Atvērtos publiskos WiFi tīklus izmanto tikai izklaides mērķiem, nepieraksties svarīgos profilos vai kontos.
- Ja ir iespējams, izmanto VPN pieslēgumu, lai aizsargātos no datu pārraides pārtveršanas /iejaukšanās.
- Pievērs uzmanību, vai HTTPS darbojas, un web adrese tiek korekti atspoguļota.
- Neveic finanšu darbības publiskajos tīklos!

# Darbs attālināti

## un piekļuves pārvaldība

### Autentifikācija un paroles

Hakeri izmanto vairākas metodes, lai kompromitētu drošību un piekļūtu sistēmām. Viena no tām ir vājo paroļu uzlaušana, izmantojot Brute Force tehnoloģiju. Tas nozīmē, ka astoņu vienkāršu simbolu paroli, kas nesatur simbolus, ļaundari var uzlauzt piecu stundu laikā. Tāpat ļaundari izmanto arī standarta paroles, ko lietotāji aizmirst nomainīt iekārtās. Šo problēmu risināšanai, vienlaicīgi neradot traucējumus lietotājiem, labākais papildus risinājums ir MFA (vairāku faktoru autentifikācija).

### Ieteikumi

- Katrā sistēmā, kur tas iespējams, noteikti izmanto vairāku faktoru autentifikāciju
- Regulāri (vismaz reizi 3 mēnešos) maini savas paroles gan darba vides piekļuvei, Izvēlies garas un sarežģītas paroles no dažādiem simboliem un cipariem.
- Izmanto paroļu pārvaldnieku paroļu saglabāšanai.
- Pārliecinies, ka paroles ievadīšana notiek korektā vietnē un www. adrese ir pareiza.


### Attālinātās sesija
**(VPN, darbs no mājām)**

Pieslēdzoties pie attālinātās darba vides, izmantojot publiskos WiFi tīklus vai neaizsargātos mājas WiFi tīklus, hakeri var sabotēt šādus pieslēgumus un izmantot tos nelikumīgo darbību veikšanai. Katru reizi, kad izmanto internetu darbam vai izklaidei, interneta pakalpojuma sniedzējs piešķir Tavai ierīcei IP adresi. Tava IP adrese ir viss, kas ir nepieciešams ļaundariem, lai veiktu uzbrukumus un citas nelikumīgas aktivitātes attālinātājos resursos. VPN tunelis izveido drošu savienojumu ar citu tīklu internetā un, pieslēdzoties no mājām, Tu pasargā savu darbību un informāciju.

### Ieteikumi

- Izmanto VPN visām attālinātām sesijām ar darba devēja IT infrastruktūru.
- Izmanto vairāku faktoru autentifikāciju attālinātajām sesijām.
- Izvairies no Remote Desktop Protocol, TeamViewer un citu līdzīgo rīku izmantošanas, pieslēdzoties attālināti.
- Izmanto antivīrusa ražotāja piedāvāto VPN pakalpojumu.

# Esi gatavs uzbrukumiem

## Piekļuves atteices uzbrukumi (DDoS)

Uzbrucēji var kaitēt tava uzņēmuma darbam arī tad, ja nespēj iekļūt tajā – piekļuves atteices uzbrukums izmanto inficētu iekārtu tīklu, lai sūtītu viltus pieprasījumus internetā pieejamiem resursiem un tādējādi traucētu vai pilnībā bloķētu to darbību. Līdz ar to – uzņēmuma vai iestādes pieejamība klientiem un darbiniekiem tiek pārtraukta uz nenoteiktu laiku.

### Ieteikumi

- Izmanto ugunsmūri, kas spēj analizēt pakešu saturu, lai automātiski noraidītu viltus/bojātus pieprasījumus
- Publiski pieejamos resursus pārvieto uz mākoni, kas ļauj mainīt serveru jaudu, atbildot uz slodzi.
- Izstrādā plānu atļauto sūtītāju filtrēšanai – Eiropas, Baltijas vai tikai Latvijas līmenī.
- Izmanto automatizētos DDoS aizsardzības rīkus.
- Izmanto CDN pakalpojumus satura izplatīšanai, lai samazinātu slodzi iekšējiem resursiem.


## Nulles uzticēšanās modelis (zero trust)

Drošības modeļi pirms-mākoņa vidē fokusējās uz uzņēmuma tīkla aizsardzību pret pasauli, ieviešot stipru perimetru. Mūsdienu vide ir izkliedēta, gan darbiniekiem strādājot no mājām, gan arī izmantojot dažādus mākoņu pakalpojumus – darba vides, e-pastu, projektu vadības un citas programmatūras. Tādēļ arī drošības mēriem jābūt ieviestiem katrā elementā un ierīcē, nepieņemot, ka uzņēmuma iekšienē valda perfekta drošība.

### Ieteikumi

- Identificē visus aizsargājamos resursus un sistēmas.
- Konfigurē katru sistēmu tā, it kā tā būtu publiski pieejama un pieprasītu autentifikāciju.
- Lai samazinātu lietotāju neērtības, izmanto SSO kur iespējams.
- Ļoti rūpīgi uzraugi datu plūsmu tīklā, lai laicīgi pamanītu anomālijas.

# Kiberkrīzes vadība

## Izstrādā kiberuzbrukuma novēršanas plānu

Lielākā daļa drošības risinājumu un pūļu to ieviešanā ir vērsti uz to, lai negadījumi nenotiktu – novērst vīrusus infekcijas un hakeru uzbrukumus. Tomēr riski pastāv un katram darbiniekam ir jāzina, ko darīt noteiktos scenārijos.

## Ieteikumi

- Noskaidro IT atbalsta kontaktinformāciju – vai uzņēmuma palīdzības, vai kādas iekārtas ražotāja.
- Izstrādā plānus populārākajiem uzbrukumu veidiem – DDoS, izspiedējvīrusi, bojāts serveris vai tīkls – un paredzi, kuru darbinieku jāinformē, kurš uzņemsies krīzes plāna realizāciju.
- Regulāri pārbaudi šos plānus – vai nav mainījušies darbinieki vai kontaktinformācija vai jāatjauno rīcības vadlīnijas.
- Regulāri pārbaudi dublējumkopijas – vai tās ir izolētas no pārējā tīkla, pieejamas un tiek veidotas atbilstoši plānam.

# E-pasti un komunikācija

## E-pastu drošība

E-pasts tika izstrādāts tā, lai tas būtu pēc iespējas atvērtāks un pieejamāks, bet ne vienmēr tas ir drošs. Nedrošais e-pasts ļauj uzbrucējiem izmantot to kā veidu peļņas iegūšanai (rēķinu samainīšana, šifrēšanas vīrusi, izspiedējvīrusi utt.).

## Ieteikumi

- Never vaļā aizdomīgas vēstules un failus. Uzmanīgi lasi saturu, kas atnāk uz e-pastu.
- Atceries, ka vīrusus var izplatīt arī ar elektroniskajiem dokumentiem .edoc un .asice. Nevar tos vaļā, ja e-pasts ir no nezināmā sūtītāja.
- Neklikšķini uz saitēm e-pastā, ja nezini, kur tā saite ved.
- Izmanto antivīrusa programmatūru, kas veic e-pastu vīrusu pārbaudi.


## Pikšķerēšana
**(kiberdrošības prātība)**

Pikšķerēšanas kampaņa ir e-pasta krāpniecības kampaņa, kas paredzēta, lai nozagtu personīgo informāciju. Kibernoziedznieki izmanto pikšķerēšanu konfidenciālās informācijas iegūšanai (maksājumu karšu dati, paroles, pasūtījumu informācija, lietotāju vārdi u.c.), izliekoties, ka viņi ir uzticamo organizāciju vai personu pārstāvji.

## Ieteikumi

- Pievērs uzmanību, vai mājas lapa, vai e-pasts, kur tiek prasīts ievadīt datus (it īpaši sensitīvus) ir īsts.
- Ierobežo nevajadzīgo pārlūkprogrammas paplašinājumu izmantošanu un neizmanto administratora tiesības, veicot ikdienišķos darbus vai pārlūkojot internetu.
- Ja esi uzņēmuma IT vai drošības vadītājs – veic regulārus pikšķerēšanas testus uzņēmumā, lai pievērstu lietotāju uzmanību riskiem.

# Iekārtas darbam un privātām vajadzībām

## Datora iekārtu konfigurācija un drošība

Datoru tehnikas ražotāji iestata noklusējuma konfigurācijas, lai ierīci varētu sākt lietot pēc iespējas ātrāk un vieglāk. Taču šīs konfigurācijas mēdz nebūt drošas un ļauj kibernoziedzniekiem ātri un salīdzinoši viegli piekļūt iekārtām.

### Ieteikumi

- Pārliecinies, ka dators saņem regulārus atjauninājumus.
- Ja atjauninājumus nevari uzinstalēt attālināti darba datoram, tad ir jāapmeklē birojs.
- Regulāri atjaunini pārlūkprogrammu, pat ja ir ieslēgta automātiska atjaunināšanas funkcija.
- Izmanto maksas antivīrusa programmatūru pilnvērtīgai aizsardzībai.
- Neuzstādini nezināmas aplikācijas.
- Izdzēs liekos lietotāju profilus.
- Neizmanto administratora tiesības ikdienā, bet gan parastā lietotāja limitētās tiesības.

## Ierīču pārizmantošana (viens dators gan darba, gan privātajām vajadzībām)

Darbs no mājām arvien vairāk izjauc robežas starp darbu un privāto dzīvi gan fiziski, gan tehniski. Ierīces, kas iepriekš tika izmantotas ar darbu saistītām funkcijām, tagad var tikt izmantotas izglītības, izklaides vai citiem nolūkiem. Šī situācija var radīt gan datu noplūdes riskus, gan arī veicināt drošības ievainojamības.

### Ieteikumi

- Neizmanto darba ierīces privātajiem nolūkiem un otrādi.
- Ievēro uzņēmuma konfidencialitātes politiku.
- Neinstalē programmatūru uz darba datora bez saskaņošanas ar uzņēmuma IT.
- Neglabā privātu informāciju darba datorā.

# Viedierīces

## Mobilās ierīces

Hibrīdā darba organizācija padara mobilās ierīces par ērtāko izvēli daudziem darbiniekiem. Tomēr mobilajām ierīcēm ir arī ievērojami drošības riski, neskatoties uz to, vai tās izmantojam tikai darba vajadzībām vai arī savā privātajā dzīvē. Vīrusi, aizdomīgas aplikācijas un neatjaunotas iekārtas rada riskus drošībai un padara Tavus datus pieejamus kibernoziedzniekiem.

## Ieteikumi

- Pārskati lietotnēm piešķirtās atļaujas, piemēram, pieeju kontaktiem, atrašanas vietai, kamerai utt.
- Izmanto antivīrusu programmatūru.
- Izvērtē, vai ir nepieciešams atvērt saites vai failus no nepazīstamiem sūtītājiem.
- Rūpīgi izvērtē netipiskus pieprasījumus sociālajos tīklos.
- Neuzstādini aplikācijas no nezināmiem avotiem.
- Regulāri atjaunini iekārtas.
- Uzstādini drošas paroles un biometriskos aizsardzības mehānismus.


## Gudro iekārtu savienojamība ar internetu
**(lietu internets jeb IoT)**

Aptuveni 80% IoT ierīču ir neaizsargāti pret plašu uzbrukumu klāstu. Pat pieslēgtie bērnu monitori ir neaizsargāti pret hakeriem: ir zināmi vairāki stāsti, kad vecāki novēloti atklāja, ka ļaundari runāja ar viņu bērniem, izmantojot uzlauztas vai nepietiekami nokonfigurētas IoT ierīces, kas bija pievienotas internetam.

## Ieteikumi

- Izvēlies uzticamu ierīci – izpēti iekārtas ražotāju un iekārtas dzīves ciklu.
- Izveido garās  paroles, izmanto vairāku faktoru autentifikāciju.
- Palielini tīkla drošību ar SSL/VPN.
- Neizmanto publisko WiFi IoT iekārtu darbībai.
- Regulāri atjaunini ierīces.
- Ļauj piekļūt tīklam tikai autorizētiem lietotājiem un ierīcēm.

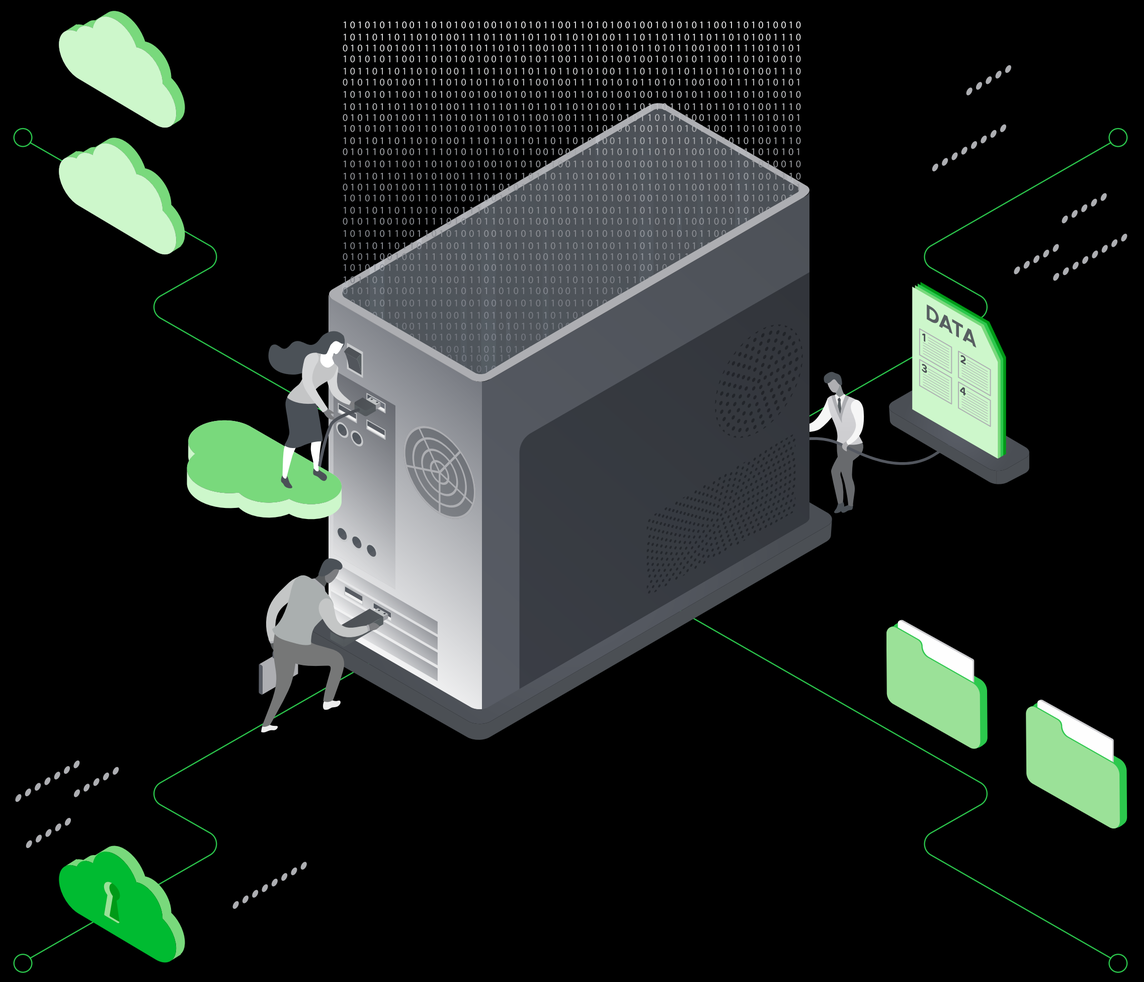
# Dati

## Datu glabāšana
**(kur un kā glabājam)**

Neskatoties uz to, ka mākonis ir viens no efektīvākajiem un mūsdienīgākajiem datu glabāšanas veidiem, ir jāatceras par tā kiberdrošību. Lai gan lielākajai daļai mākoņu pakalpojumu sniedzējiem ir ieviesti pienācīgi drošības līmeņi, tie mēdz atšķirties, un dažreiz gala lietotājs nepareizi tos aktivizē vai izmanto.

## Ieteikumi

- Izmanto datu šifrēšanu gan datu pārsūtīšanai, gan uzglabāšanai.
- Izmanto vairāku faktoru autentifikāciju saviem mākoņa datu glabāšanas resursiem.
- Neizmanto neaizsargātu publisko WiFi tīklu datu sūtīšanai uz mākoni.
- Autorizē tikai zināmus sev lietotājus un iekārtas piekļuvei mākonim.




## Datu rezerves kopēšana

Datu zaudēšana datora avārijas, vīrusa vai cita incidenta dēļ var faktiski pilnībā izdzēst Tavas "digitālās atmiņas", vecus un aktuālus gan privātus, gan arī darba datus. Datu nozagšana savukārt var vest pie šantāžās un izpirkuma maksas. Tāpēc ir būtiski nodrošināt datu rezerves kopēšanu!

## Ieteikumi

- Veido rezerves kopijas svarīgajai informācijai.
- Neglabā un neapstrādā trešo pušu personīgo informāciju, ja Tev nav tam juridiskā pamatojuma.
- Apsver iespēju izmantot mākoņa pakalpojumus informācijas glabāšanai no pazīstamiem drošiem pakalpojuma sniedzējiem, bet tāpat izvērtē mākoņa drošību.

# Kiberzināšanas pret kiberkrāpniecību

## Kiberkrāpniecība un kiberzināšanas
**(izpirkuma maksas, sociālā inženierija, kriptovalūtas)**

Kibernoziedznieku aktivitāte turpina augt.
Tet un CERT.LV redz būtisku pieaugumu gan pikšķērēšanas e-pastu kampaņās, gan vīrusu izplatīšanas kampaņās, gan arī izspiedējvīrusu uzbrukumos Latvijas uzņēmumiem un privātpersonām. Pikšķērēšanas uzbrukums ir visefektīvākais veids kā piekļūt Taviem personas datiem un izspiest finansiālus līdzekļus. Esoša Covid-19 situācija un attālinātais darbs rada labvēlīgu augsni visu veidu krāpšanai un uzbrukumiem.

## Ieteikumi

- Neglabā sensitīvu informāciju par sevi e-pastos, neaizsargātajos mākoņos un datoros, kur nav atbilstošas kiberaizsardzības.
- Regulāri maini paroles un izmanto garās paroles.
- Izmanto antivīrusu programmatūru.
- Rūpīgi lasi e-pastu saturu, izvērtējot, vai ir nepieciešams atvērt saites vai failus no nepazīstamajiem sūtītājiem.
- Rūpīgi izvērtē netipiskus pieprasījumus sociālajos tīklos.
- Veic rezerves kopijas.
- Seko līdzi Cert.lv un citu drošības ekspertu aktualitātēm un regulāri pilnveido savas zināšanas.
- Nebaidies celt trauksmi par aizdomīgajām darbībām (piemēram, aizdomīgi zvani vai e-pasti, vai pieprasījumi sociālos tīklos).
- Seko līdzi Cert.lv un citu drošības ekspertu aktualitātēm un regulāri pilnveido savas zināšanas.
- Nebaidies celt trauksmi par aizdomīgajām darbībām (piemēram, aizdomīgi zvani vai e-pasti, vai pieprasījumi sociālos tīklos).