Kiberhigiēnas pamati

Tīkls

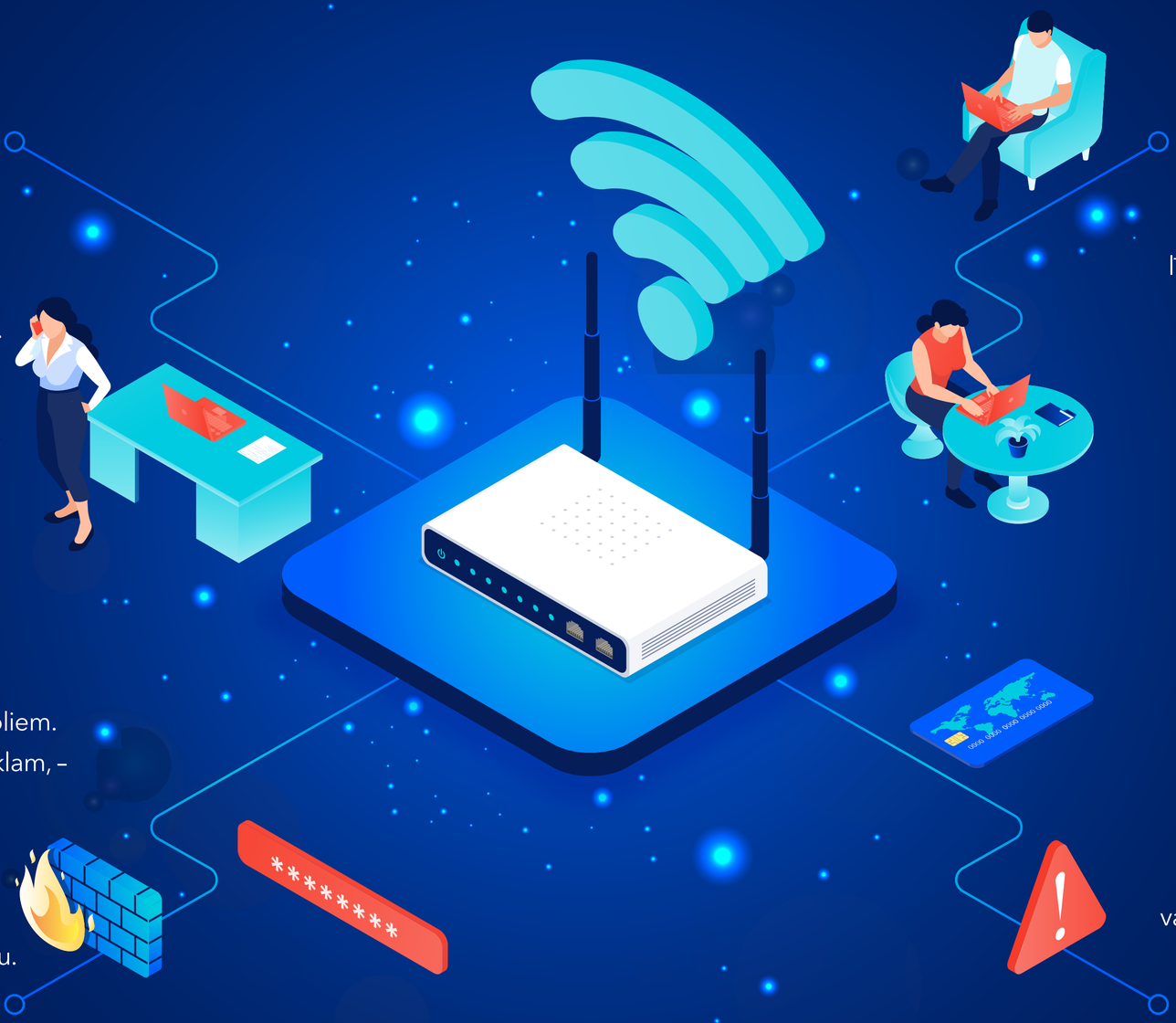
WiFi tīkla konfigurācija un drošības uzstādījumi

Mūsdienu pasaulē gandrīz ikvienam ir vismaz viena ar internetu savienota ierīce, un parasti savienojums tiek veidots, izmantojot WiFi tīklu.

Pieaugot šo ierīču skaitam, ir svarīgi pievērst uzmanību mājas un darba WiFi tīkla minimālajai drošībai un pareizai konfigurācijai, kas var uzlabot kopējo bezvadu tīkla drošību un mazināt drošības riskus.

Ieteikumi

- Nomaini noklusējuma paroles WiFi rūterī.
- Izveido garu WiFi paroli no dažādiem simboliem.
- Ierobežo iekārtas, kas var pieslēgties WiFi tīklam, – ieslēdz MAC filtrēšanu.
- Šifrē WiFi datu pārraidi (WPA2, WPA3).
- Izvēlies unikālu WiFi tīkla nosaukumu.
- Ieslēdz ugunsmūra funkciju.
- Regulāri atjaunini WiFi rūtera operētājsistēmu.



Publisko tīklu riski

Gandrīz ceturtā daļa pasaules publisko WiFi tīklu neizmanto nekāda veida šifrēšanu, līdz ar to padarot tos par vieglu mērķi hakeriem.

Lielākais drauds publisko un bezmaksas WiFi tīklu drošībai ir hakera spēja pozicionēt sevi starp tavu iekārtu un WiFi savienojuma punktu. Rezultātā tā vietā, lai sazinātos tieši ar publisko WiFi tīklu, tu sūti savu informāciju hakerim, kurš to saglabā un izmanto pret tevi.

Ieteikumi

- Atvērtos jeb publiskos WiFi tīklus izmanto tikai izklaides mērķiem, neveic tajos finanšu darījumus.
- Ja iespējams, izmanto VPN pieslēgumu, lai aizsargātos no datu pārraides pārtveršanas/iejaukšanās.
- Pievērs uzmanību, vai darbojas HTTPS un vai www adresē visas zīmes un burti ir pareizi.

tet

Attālinātais darbs un piekļuve tīklam

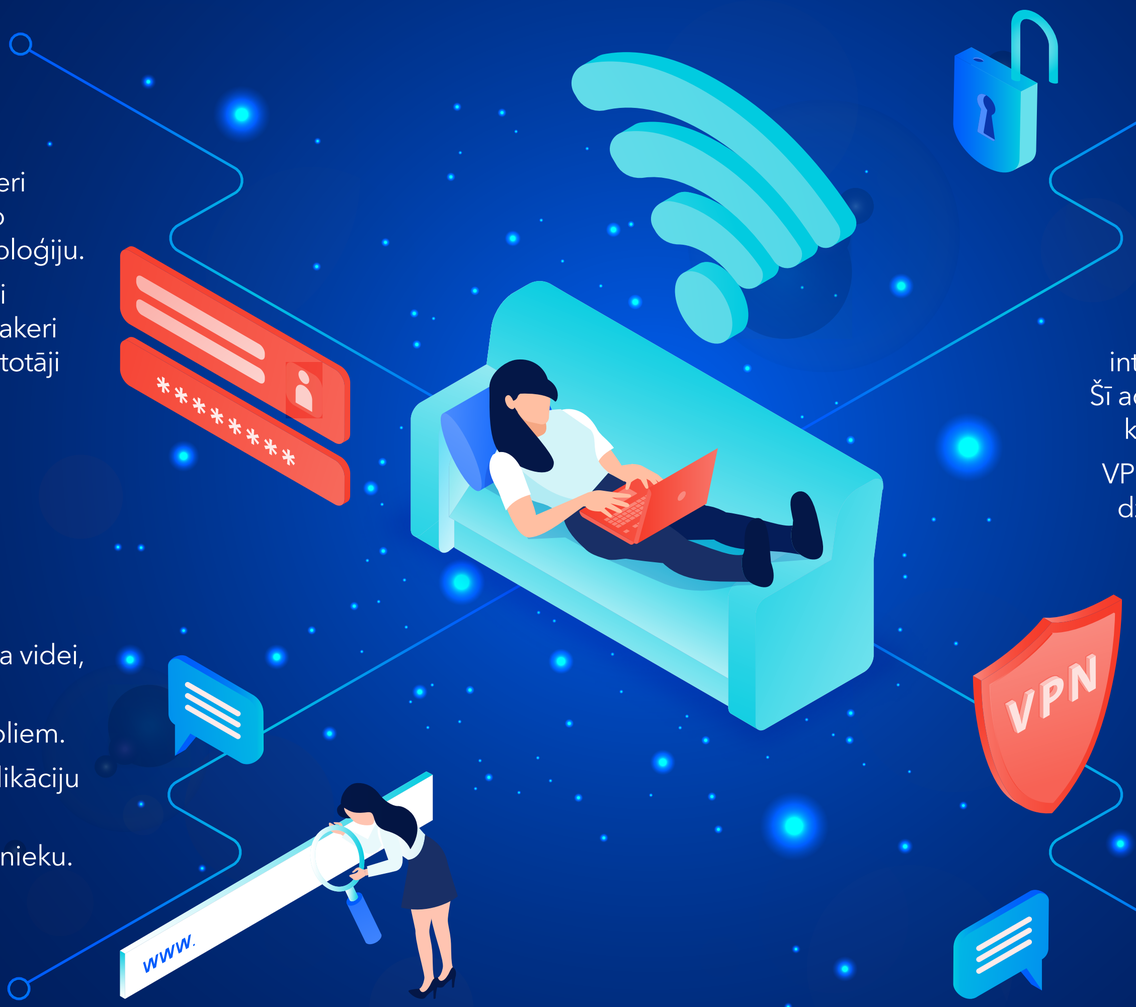
Autentifikācija, paroles un lietotāja dati

Lai vājinātu drošību un piekļūtu sistēmām, hakeri izmanto vairākas metodes. Viena no tām ir vājo paroļu uzlaušana, izmantojot Brute Force tehnoloģiju.

Tas nozīmē, ka astoņu vienkāršo simbolu paroli ļaundari var uzlauzt piecu stundu laikā. Tāpat hakeri izmanto arī standarta sākotnējās paroles, ko lietotāji iekārtās nenomaina.

Ieteikumi

- Regulāri maini paroles, lai piekļūtu gan darba videi, gan privātajiem kontiem.
- Izveido garu WiFi paroli no dažādiem simboliem.
- Izmanto vairāku faktoru autentifikāciju ar aplikāciju jeb lietotni, sms vai zvanu.
- Paroļu saglabāšanai izmanto paroļu pārvaldnieku.
- Pārliecinies, ka paroli ievadi pareizā vietnē un ka ir pareiza www adrese.



Attālinātās sesijas (VPN, darbs no mājām)

Ja attālinātā darba vieta uzņēmuma sistēmai pieslēdzas, izmantojot publisko WiFi tīklu vai neaizsargātu mājas WiFi tīklu, hakeri var sabotēt šādu pieslēgumu un izmantot to nelikumīgām darbībām.

Katru reizi, kad lieto internetu darbam vai izklaidei, interneta pakalpojuma sniedzējs piešķir tavai ierīcei IP adresi. Šī adrese ir viss, kas nepieciešams ļaundariem, lai veiktu uzbrukumus un citas nelikumīgas aktivitātes attālinātajos resursos.

VPN tunelis izveido drošu savienojumu ar citu tīklu, un, pieslēdzoties no mājām, tu aizsargā savas darbības un informāciju.

Ieteikumi

- Attālinātajām sesijām ar darba devēja IT infrastruktūru izmanto VPN.
- Attālinātajām sesijām izmanto vairāku faktoru autentifikāciju.
- Pieslēdzoties attālināti, neizmanto Remote Desktop Protocol, TeamViewer un līdzīgus rīkus bez papildu aizsardzības, piemēram IP adrešu ierobežošanas.

tet

E-pasts un komunikācija

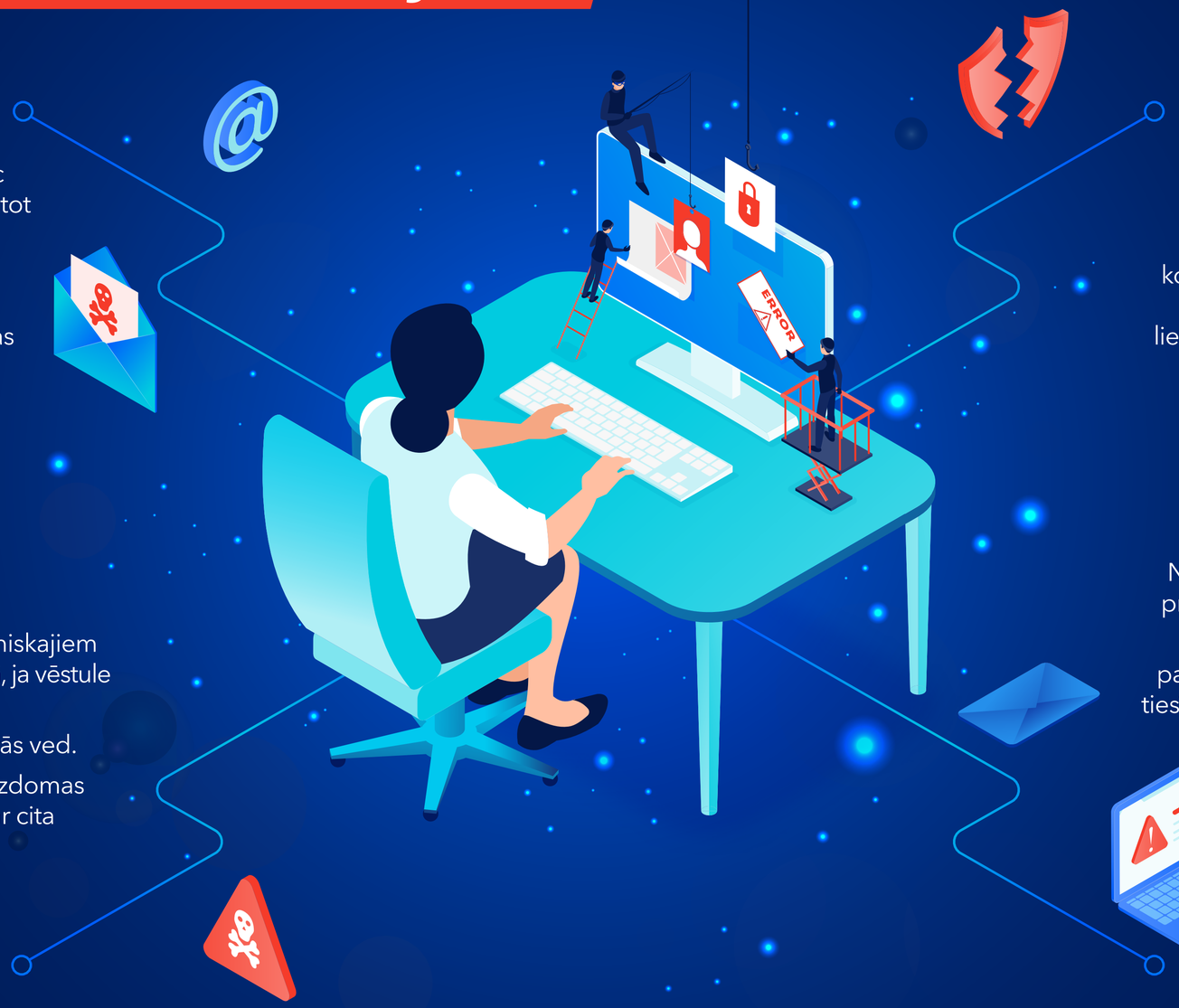
E-pasta drošība

E-pasts tika izveidots pirms 30 gadiem un pēc būtības nav drošs, kas ļauj uzbrucējiem izmantot to kā peļņas veidu (rēķinu samainīšana, šifrēšanas vīrusi, izspiedējvīrusi utt.).

Nedrošs e-pasts ļauj uzbrucējiem izmantot to kā peļņas veidu (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. Never tos vaļā, ja vēstule ir no nezināma sūtītāja.
- Neklikšķini uz saitēm e-pastā, ja nezini, kur tās ved.
- Ja e-pasts ir no zināma sūtītāja, bet radās aizdomas par to, ka tas nav drošs, sazinies ar sūtītāju ar cita kanāla palīdzību.
- Izmanto antivīrusu programmu, kas veic e-pasta vīrusu pārbaudi.



Pikšķerēšana

Pikšķerēšana ir e-pasta krāpniecības veids, ar ko var nozagt personīgo informāciju.

Kibernoziedznieki izmanto pikšķerēšanu konfidenciālu ziņu iegūšanai (maksājumu karšu dati, paroles, pasūtījumu informācija, lietotāju vārdi u.c.), izliekoties, ka viņi ir uzticamu organizāciju vai personu pārstāvji.

Ieteikumi

- Noskaidro, vai mājaslapa un e-pasts, kur tiek prasīts ievadīt datus (it īpaši sensitīvus), ir īsts.
- Atinstalē nevajadzīgus pārlūkprogrammas paplašinājumus un neizmanto administratora tiesības, veicot ikdienišķus darbus vai vienkārši pārlūkojot internetu.

tet

Iekārtas darbam un privātām vajadzībām

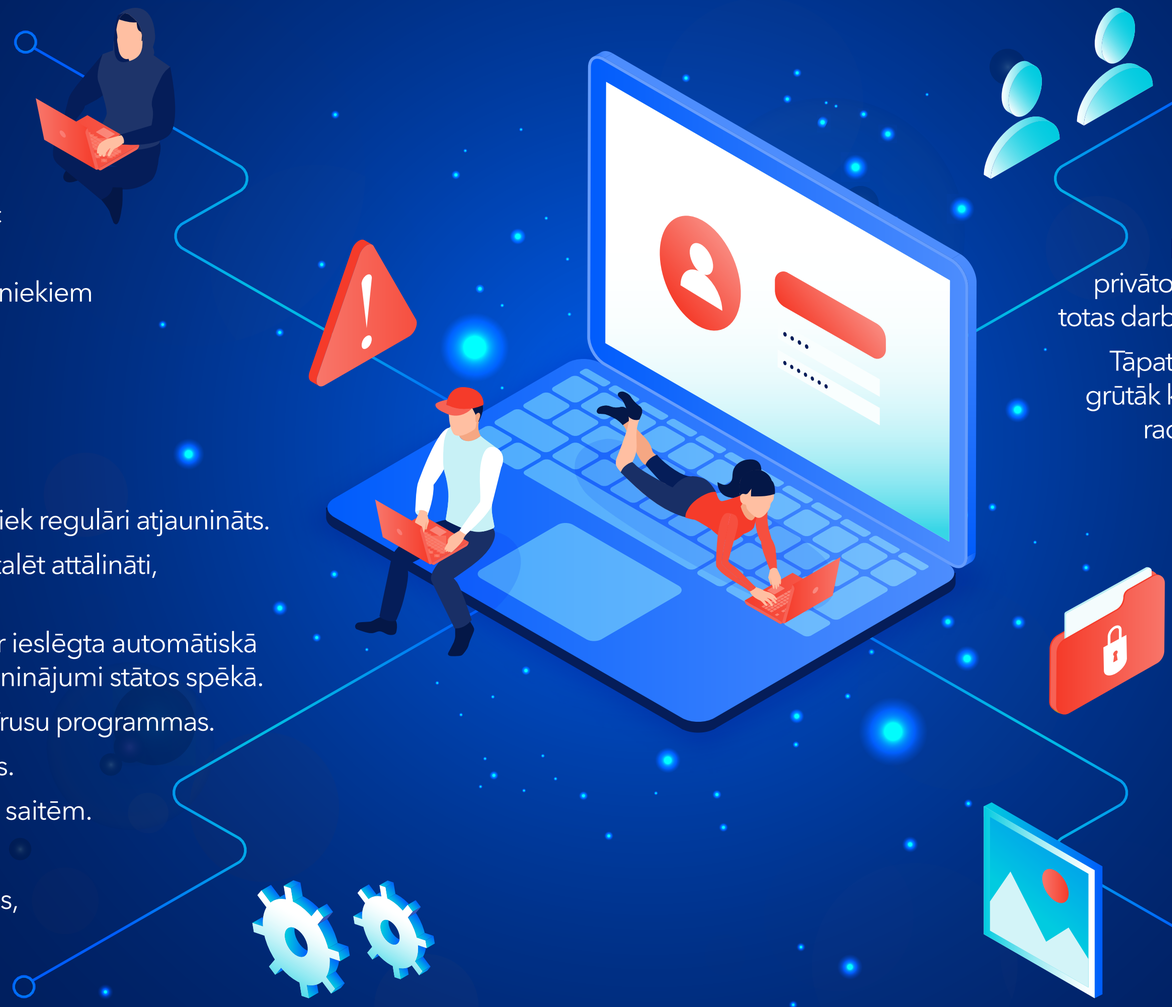
Iekārtu konfigurācija un drošība

Pēc ražotāja iestatītā noklusējuma ierīce ir konfigurēta tādējādi, lai to varētu sākt lietot pēc iespējas ātrāk un vieglāk.

Taču tas mēdz nebūt droši un ļauj kibernoziedzniekiem ātri un salīdzinoši viegli piekļūt ierīcēm.

Ieteikumi

- Rūpējies, lai gan privātais, gan darba dators tiek regulāri atjaunināts.
- Ja atjauninājumus darba datoram nevari instalēt attālināti, tad ir jāapmeklē birojs.
- Regulāri atjaunini pārlūkprogrammu, pat ja ir ieslēgta automātiskā atjaunināšana. Restartē programmu, lai atjauninājumi stātos spēkā.
- Pilnvērtīgai aizsardzībai izmanto maksas antivīrusu programmas.
- Neinstalē nezināmas aplikācijas jeb lietotnes.
- Neinstalē aplikācijas no nezināmām e-pasta saitēm.
- Izdzēs liekas aplikācijas un lietotāju profilus.
- Ikdienā izmanto nevis administratora tiesības, bet gan limitētās parastā lietotāja 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 darbam, tagad var kalpot izglītības, izklaides un citiem nolūkiem.

Tāpat bieži vien tās izmanto arī ģimenes locekļi, tāpēc kļūst arvien grūtāk kontrolēt, kas datorā tiek instalēts un izdzēsts. Šī situācija gan rada datu noplūdes risku, gan arī veicina drošības vājināšanos.

Ieteikumi

- Neizmanto darba ierīces privātiem nolūkiem un otrādi – privātas ierīces darbam.
- Ievēro uzņēmuma konfidencialitātes politiku, darba datorā neinstalē programmatūru bez saskaņošanas ar uzņēmuma IT.
- Neglabā privātu informāciju darba datorā – dokumentu kopijas, sensitīvu informāciju (piemēram, analīžu rezultātus), privātas fotogrāfijas utt.
- Nesinhronizē pārlūkprogrammas datus starp privāto un darba ierīcēm.

tet

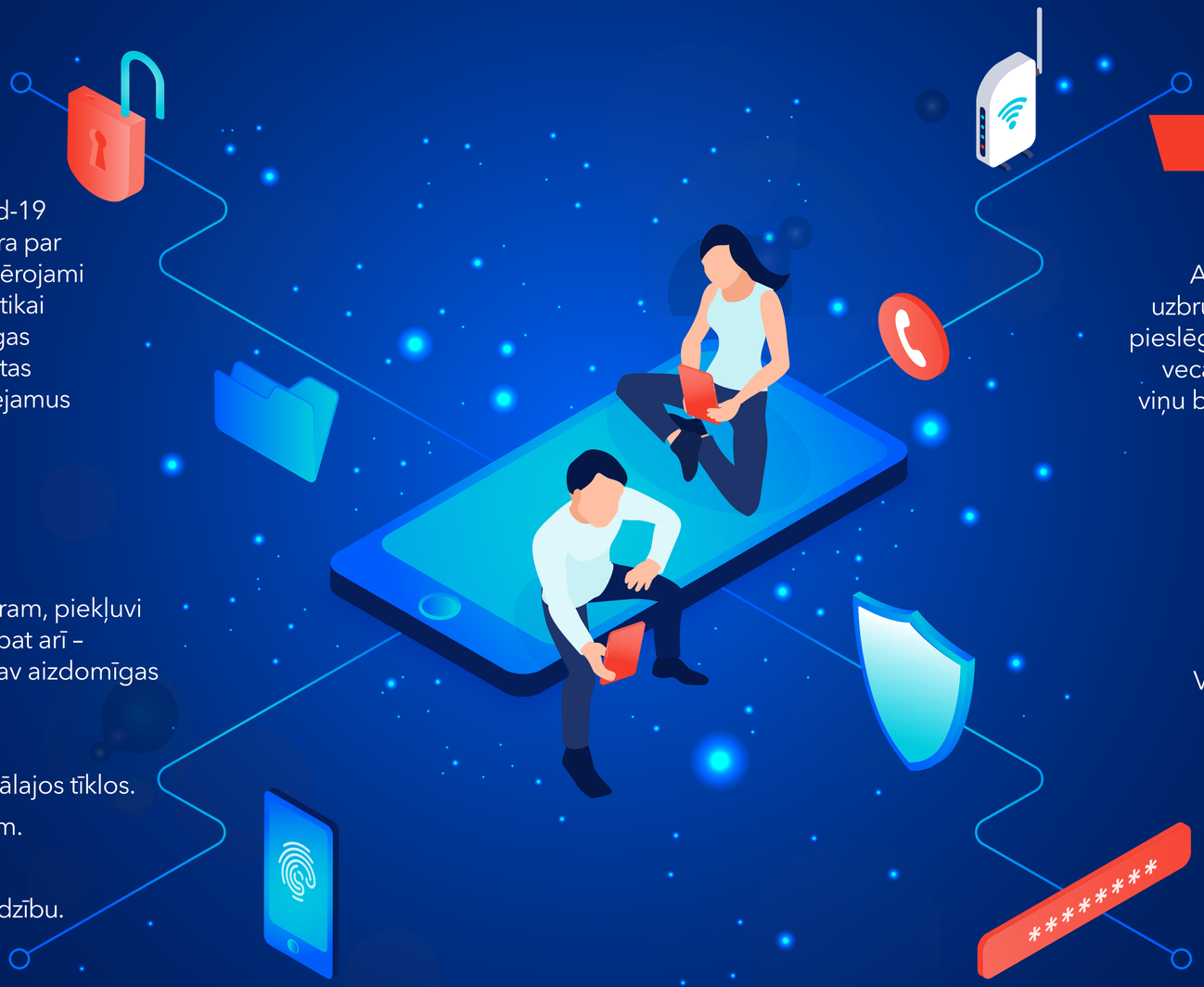
Mobilās ierīces un gudrās iekārtas

Viedierīces un lietotāja dati

Attālinātā darba popularitāte, reaģējot uz Covid-19 pandēmiju un mājsēdi, daudziem ierīces padara par ērtāko izvēli. Tomēr mobilajām ierīcēm ir arī ievērojami drošības riski – neatkarīgi no tā, vai tās izmanto tikai darbam vai arī privātām lietām. Vīrusi, aizdomīgas aplikācijas jeb lietotnes un neatjauninātas iekārtas rada riskus drošībai un padara tavus datus pieejamus kibernoziedzniekiem.

Ieteikumi

- Pārskati lietotnēm piešķirtās atļaujas, piemēram, piekļuvi kontaktiem, atrašanās vietai, kamerai utt., tāpat arī – kā tās izmanto internetu: cik patērē un vai nav aizdomīgas lietošanas gadījumu.
- Izmanto antivīrusu programmas.
- Rūpīgi izvērtē netipiskus pieprasījumus sociālajos tīklos.
- Neinstalē aplikācijas no nezināmiem avotiem.
- Atjaunini iekārtas.
- Izmanto drošas paroles un biometrisko aizsardzību.



Gudro iekārtu savienojamība ar internetu (lietu internets jeb IoT)

Aptuveni 80% IoT ierīču ir neaizsargāti pret plašu uzbrukumu klāstu. Pret hakeriem ir neaizsargāti pat pieslēgtie bērnu monitori: ir zināmi vairāki stāsti, kad vecāki novēloti atklājuši ļaundaru komunikāciju ar viņu bērniem, izmantojot uzlauztas vai nepietiekami aizsargātas IoT ierīces.

Ieteikumi

- Izvēlies pareizo ierīci – izpēti ražotāju un ierīces dzīves ciklu.
- Veido garas paroles, izmanto vairāku faktoru autentifikāciju.
- Izmanto IoT iekārtas tikai privātajā tīklā.
- Regulāri atjaunini ierīces.
- Ļauj piekļūt mājas tīklam tikai autorizētiem lietotājiem un ierīcēm.

tet

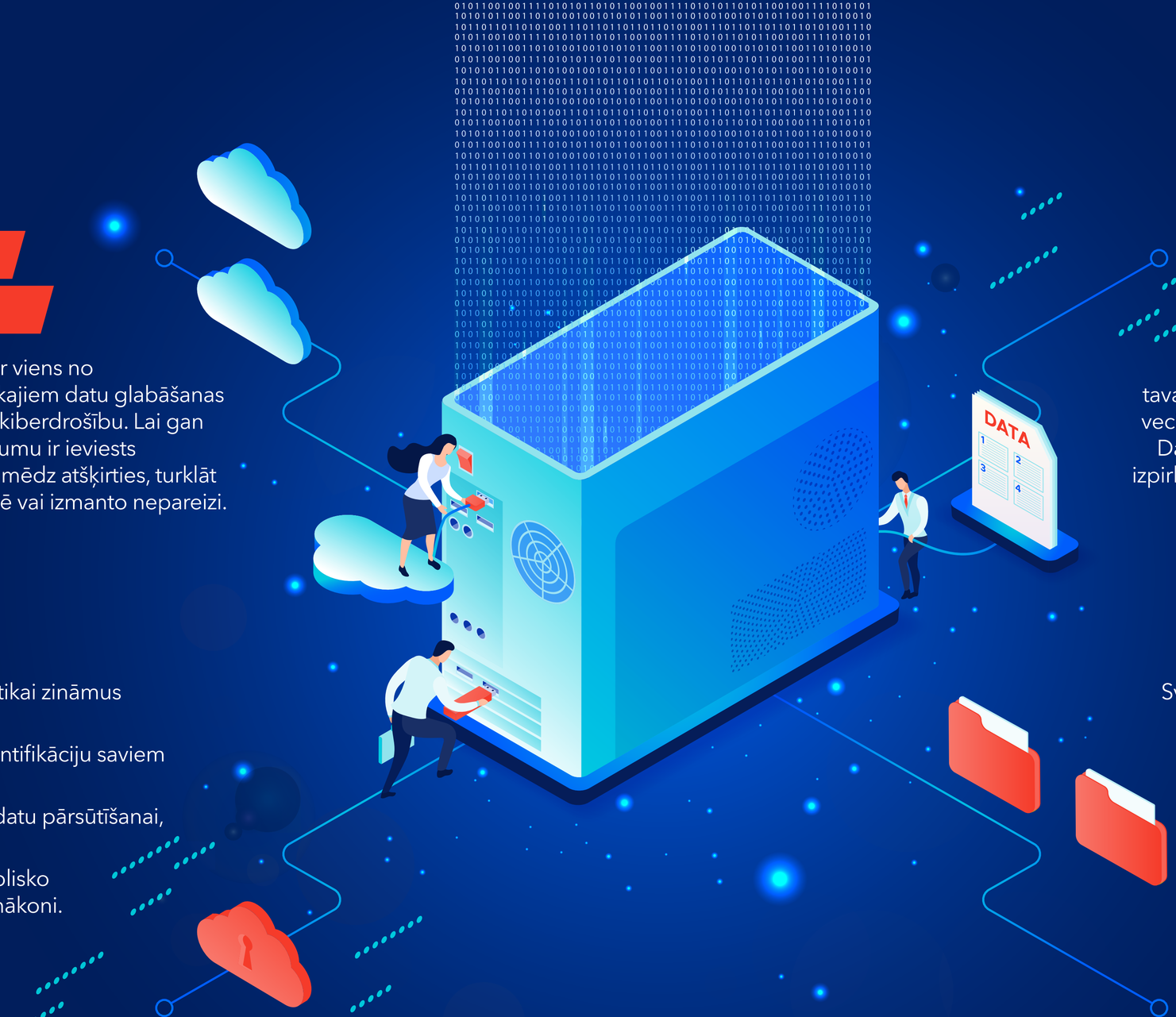
Dati

Datu glabāšana (kur un kā glabāt)

Neskatoties uz to, ka mākonis ir viens no efektīvākajiem un mūsdienīgākajiem datu glabāšanas veidiem, ir jāpārliecinās par tā kiberdrošību. Lai gan lielākajai daļai mākoņpakalpojumu ir ieviests pienācīgs drošības līmenis, tie mēdz atšķirties, turklāt dažreiz gala lietotājs tos aktivizē vai izmanto nepareizi.

Ieteikumi

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



Datu rezerves kopēšana

Datora bojāejas, vīrusa vai citu iemeslu dēļ no tavas digitālās atmiņas var tikt pilnībā izdzēsti gan veci, gan aktuāli un gan privāti, gan arī darba dati. Datu zādzība savukārt var novest pie šantāžas ar izpirkuma pieprasīšanu. Tāpēc ir būtiski nodrošināt datu rezerves kopēšanu!

Ieteikumi

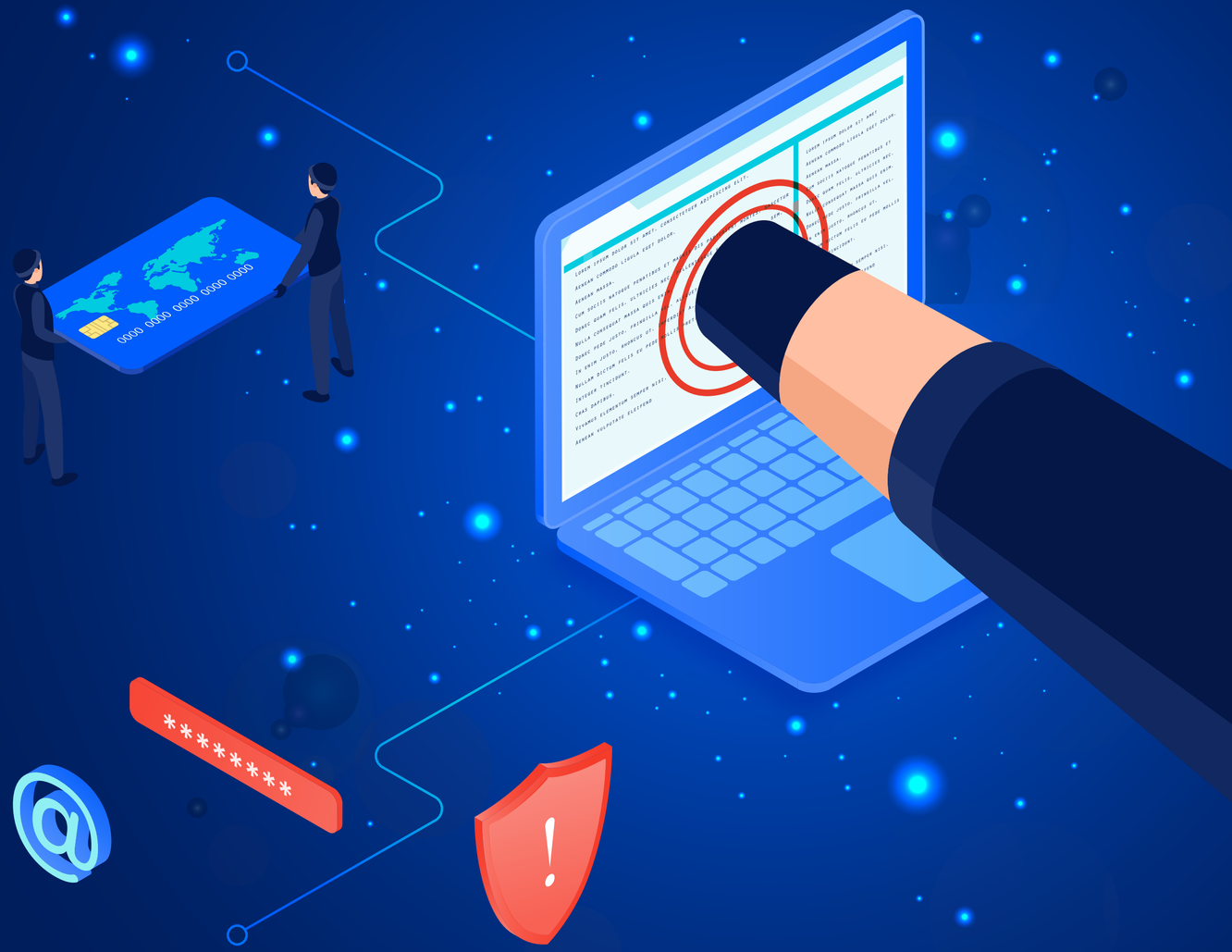
- Svarīgajai informācijai veido rezerves kopijas.
- Neglabā un neapstrādā trešo pušu personīgo informāciju, ja tev tam nav juridiska pamatojuma.
- Apsver mākoņpakalpojumu izmantošanu informācijas glabāšanai no pazīstamiem drošiem pakalpojuma sniedzējiem, bet tāpat izvērtēmākoņa drošību.

tet

Kiberzināšanas pret kiberkrāpniecību

Kiberkrāpniecība un kiberzināšanas (izpirkuma maksa, sociālā inženierija, kriptovalūta)

Kibernoziedznieku aktivitātes vēršas plašumā. Tet un CERT.LV novēro būtisku pieaugumu gan pikšķerēšanas e-vēstuļu, gan vīrusu izplatīšanas jomā, gan arī izspiedējvīrusu uzbrukumos Latvijas uzņēmumiem un privātpersonām. Pikšķerēšana ir visefektīvākais veids, kā piekļūt taviem personas datiem un izspiest no tevis naudu. Esošā Covid-19 situācija un attālinātais darbs rada labvēlīgu augsni visu veidu krāpniecībai un uzbrukumiem.



Ieteikumi

- Veido rezerves kopijas.
- Neglabā sensitīvu informāciju par sevi e-pastā, neaizsargātā mākonī un datorā, kur nav atbilstošas kiberaizsardzības.
- Regulāri maini paroles un izmanto garas paroles.
- Lieto antivīrusu programmas.
- Rūpīgi lasi e-pasta vēstules un izvērtē, vai ir nepieciešams atvērt saites un failus no nepazīstamiem sūtītājiem.
- Rūpīgi izvērtē netipiskus pieprasījumus sociālajos tīklos.
- Seko līdzi CERT.LV un citu drošības ekspertu jaunumiem un regulāri pilnveido savas zināšanas.
- Nebaidies celt trauksmi par aizdomīgām darbībām (piemēram, aizdomīgi zvani, e-vēstules, kā arī pieprasījumi sociālajos tīklos).

tet