Digitālās drošības ceļvedis izglītības jomas darbiniekiem

Sagatavots pamatskolu, vidusskolu skolotājiem
un izglītības pārvalžu speciālistiem

Aizsardzības ministrija

Nacionālais kiberdrošības centrs

CERT.LV Kiberincidentu novēršanas institūcija

NCC-LV Latvijas kiberdrošības koordinācijas centrs

ECCC Eiropas kiberdrošības kompetenču centrs

Līdzfinansē Eiropas Savienība

DROSS INTERNETS.LV

Ievads

Digitālā pasaule šodien ir neatņemama mācību procesa daļa. Skolotāji ikdienā izmanto tiešsaistes platformas – no E-klases līdz Google Classroom, Teams un citām –, un skolēnu darbi, vērtējumi un saziņa arvien biežāk notiek digitāli.

Mācību vide kļūst elastīgāka un pieejamāka, taču kopā ar ērtībām nāk arī jauni izaicinājumi un riski. Pazaudētas paroles, krāpnieciskas vēstules, nejauši kopīgoti dokumenti vai neapdomīgi ieraksti sociālajos tīklos var radīt problēmas gan skolotājiem, gan skolēniem, gan skolai kopumā.

Digitālā drošība ir kā fiziskā drošība skolā – bez tās nav drošas, uzticamas un cieņpilnas mācību vides. Drošība tiešsaistē sākas ar zināšanām, ieradumiem un apzinātu rīcību.

Šī ceļveža mērķis ir palīdzēt skolotājiem orientēties digitālajā vidē droši un pārliecinoši, sniedzot atbalstu gan ikdienas darbā, gan mācot skolēniem drošu uzvedību tiešsaistē.

Šeit atradīsi:

- vienkāršus, saprotamus drošības principus, kas noder katram skolotājam neatkarīgi no tehniskajām zināšanām;
- praktiskus piemērus no skolas dzīves – kā atpazīt krāpniecību, droši glabāt datus un pasargāt skolēnus;
- konkrētus padomus dažādām skolotāju grupām – pamatskolas, vidusskolas un Datorikas skolotājiem;
- vadlīnijas skolu vadībai un izglītības pārvaldēm, kā veidot drošības kultūru un sagatavoties incidentiem;
- resursus pašizglītībai, lai turpinātu stiprināt savas un skolēnu digitālās un kiberdrošības prasmes.

Paroļu drošība

Paroles ir kā digitālās atslēgas. Ja tā ir vāja, noziedznieks var piekļūt taviem datiem tikpat viegli, kā atvērt durvis ar universālu atslēgu. Tāpēc ir svarīgi, lai tās būtu unikālas, drošas un regulāri atjauninātas.

Drošas paroles pamatprincipi:

Noteikums	Kāpēc tas svarīgi?	Padoms
Vismaz 15 rakstzīmes	Garākas paroles ir eksponenciāli grūtāk uzlauzt.	Izmanto teikumus vai frāzes (piemēram, "ManPatīkLasītGrāmatas!"
Lielie/mazie burti + cipari + simboli	Daudzveidība sarežģī uzlaušanas algoritmus.	Kombinē simbolus ar vārdiem: Mār@2025_Skol!" – satur īpašās rakstzīmes, lielos/mazos burtus, nav viegli uzminama.
Neizmanto vārdus vai dzimšanas datus	Tie ir pirmie, ko pārbauda uzbrucēji.	Nekad "Janis1980" vai "Skola2020". Viegli uzminama, satur tikai vienu vārdu un ciparus. Tādu var uzminēt ar vārdnīcas uzbrukumu vai sociālās inženierijas palīdzību.
Katram kontam sava parole	Viena noplūdusi parole var radīt piekļuvi visiem kontiem.	Atšķirīgas paroles, – īpaši e-pastam un E-klasei.
Regulāra maiņa (ik pēc 6–12 mēnešiem)	Samazina risku, ja parole bijusi apdraudēta.	Atjauno arī pēc aizdomām par noplūdi.

****

Bieži sastopamās kļūdas

- Vienas un tās pašas paroles izmantošana vairākos kontos.
- Nedaudz mainītas paroles: "Skola2024", "Skola2025" – uzbrucējs var uzminēt.
- Paroles pierakstīšana uz lapiņas pie monitora vai klades vāka.
- Īsas vai vienkāršas paroles izmantošana ("Mācības1", "Parole123").

Paroļu pārvaldnieki – droša palīdzība skolotājiem

Tā kā skolotāji izmanto vairākas sistēmas (E-klase, e-pasts, *Zoom, Mykoob, Google, Microsoft Teams* u. c.), paroļu pārvaldnieks palīdz droši un ērti pārvaldīt visas paroles.

Populāri un uzticami risinājumi

- **Bitwarden** – bezmaksas, drošs, arī pārlūka paplašinājumā.
- **1Password** – lietotājam draudzīgs, ērts koplietošanai darba vidē.
- **NordPass** – intuitīvs dizains, piedāvā automātisku paroļu pārbaudi.
- **KeePass** – bezmaksas, darbojas lokāli (drošāks, bet vajag vairāk iestatījumu).

Ko tie dara?

- Šifrē un droši glabā paroles (ar spēcīgu galveno paroli).
- Automātiski ģenerē unikālas, stipras paroles.
- Automātiski aizpilda paroles tīmekļa vietnēs un lietotnēs.
- Sinhronizē paroles starp ierīcēm (ja iestatīts).

Padoms: galvenajai parolei (*master password)* jābūt īpaši stiprai, bet tādai, ko viegli atcerēties.

Ja ir aizdomas, ka parole varētu būt noplūdusi:

- nomaini to nekavējoties visos saistītajos kontos;
- ieslēdz divfaktoru autentifikāciju (2FA), ja vēl nav aktivizēta;
- pārbaudi e-pasta adresi vietnē haveibeenpwned.com

Divfaktoru autentifikācija (2FA)

Pat tad, ja tava parole kādam no taviem kontiem tiek uzminēta vai nozagta, divfaktoru autentifikācija (2FA) var pasargāt kontu no nesankcionētas piekļuves. Tā pieprasa vēl vienu apstiprinājumu, piemēram:

- SMS kodu uz tavu tālruni;
- kodu no autentifikācijas lietotnes (piemēram, *Google Authenticator, Microsoft Authenticator*);
- biometriskos datus (sejas atpazīšana, pirkstu nospiedums).

Kur izmantot 2FA?

Skolotājiem ieteicams aktivizēt 2FA šādās sistēmās:

- e-pasts: *Gmail, Outlook*, skolas domēns;
- mācību un vērtēšanas sistēmas: *E-klase, Mykoob, Google Classromm*, u. c. ;
- mākoņpakalpojumi: *Google Workspace for Education / Microsoft 365, Dropbox, Onedrive;*
- paroļu pārvaldnieki: ja izmanto, tiem noteikti jābūt aizsargātiem ar 2FA;
- sociālie tīkli un saziņas rīki: *WhatsApp Web, Facebook, Instagram* u. c., ja tos izmanto ar skolas profilu vai saziņai ar vecākiem.

Padomi paroļu drošībai

- Saglabā rezerves kodus drošā vietā (ne datorā, bet, piemēram, uzrakstītus un glabātus slēgtā mapē mājās).
- Nekad nesūti apstiprinājuma kodus citiem! Ne IT speciālistiem, ne kolēģiem.
- Ja maini telefonu, pārliecinies, ka pārcel autentifikācijas lietotni un rezerves kodus uz jauno ierīci.
- Ja nav iespējams aktivizēt 2FA, izmanto vismaz unikālu, garu paroli un regulāri to maini.

Drossinternets.lv izstrādāta

Instrukcija 2FA uzstādīšanai →

Pikšķerēšana un krāpniecība

Pikšķerēšana ir visbiežāk izmantotā kibernoziedznieku metode skolās. Krāpnieki nosūta e-pastu, ziņu vai tīmekļa saiti, lai izliktos par uzticamu personu vai institūciju un izvilinātu paroles, personas datus vai pat naudu. Skolas personālam šim krāpniecības veidam ir jāpievērš īpaša uzmanība, jo skolās ir piekļuve dažādiem sensitīviem datiem (personas dati, atzīmes, veselības ieraksti) un ikdienā skolotāji saņem daudz e-pastu no jauniem kontaktiem (vecāki, sadarbības partneri).

Kā atpazīt viltojumu?

Pazīme	Kam pievērst uzmanību?	Kā atpazīt viltojumu?	Ko darīt?
Nepazīstams sūtītājs	Vārds izskatās pareizs, bet domēna vārds atšķiras	Pārvieto kursoru virs adreses, parādi pilno e-pastu (*View full headers*). Piemērs: **E-pasts saņemts no direktors@skola-support.com (nevis direktors@skola.lv).**	Neatbildi uzreiz. Salīdzini ar oficiālo e-pasta adresi.
Steidzinošs tonis	Mēģina radīt paniku, lai tu rīkotos bez domāšanas.	Tekstā jūtama pārspīlēta steiga vai draudi. Piemērs: **"Rīkojies tūlīt vai zaudēsi piekļuvi!"**	Ignorē spiedienu, pārsūti e-pastu skolas IT speciālistam.
Valodas/stila kļūdas	Gramatikas kļūdas vai neparastas frāzes – bieži automātiskās tulkošanas pazīmes.	Meklē neparastus vārdu salikumus, pieturzīmes. Piemērs: **"Lūdzu atjauniniet jūs konts tūlīt."**	Ja izskatās aizdomīgs, pārsūti e-pastu skolas IT speciālistam vai izmanto "Report phishing" funkciju savā e-pastā.
Aizdomīgas saites	Teksta saite rāda vienu domēna vārdu, bet adrese ved uz citu saiti.	Uzejot uz saites (bet neklikšķinot), redzams cits domēna vārds. Piemērs: **Saite: "skola.lv/iesniegums", bet īstenībā ved uz "bit.ly/skola"**	Ja izskatās aizdomīgi, pārsūti e-pastu skolas IT speciālistam vai kiberincidentu novēršanas institūcijai CERT.LV
Bezpersoniska vēstule	Bezpersoniska vēstule ar standarta uzrunu, ko varētu izsūtīt visiem.	Pārbaudi, vai e-pastā ir minēts tavs vārds vai cita konkrēta informācija, pievērs uzmanību bezpersoniskai uzrunai. Piemēram: **"Cienījamais lietotāj!"**	Ja izskatās aizdomīgi, pārbaudi sūtītāja identitāti.

Pazīme	Kam pievērst uzmanību?	Kā atpazīt viltojumu?	Ko darīt?
Tiek piedāvāta "balva" vai "dāvana"	Solījums par dāvanu karti, atlaidi vai bezmaksas ieguvumiem.	Pievērs uzmanību, ja kaut kas tiek piedāvāts bez maksas. Piemēram: **"Akcijas tikai skolotājiem – iespēja pieteikties bezmaksas prezentāciju komplektam ar Google kontu!"**	Ja piedāvājums izklausās pārāk labs, lai būtu patiesība, – visticamāk, tā ir krāpšana. Lejupielādes veic tikai no oficiāliem avotiem.
Nepieciešama konta atjaunošana vai drošības pārbaude	Krāpnieki sūta viltotus e-pastus, kuros tiek lūgts "atjaunot" kontu vai veikt drošības pārbaudi savam kontam.	Saņemts e-pasts, kur ātri jārīkojas un saite ved uz viltotu lapu. Piemērs: **"Ātri atjauno E-klases paroli šeit – www.eklases.lv/paroles-maina".**	Neklikšķini uz saites – atver sev zināmo vietni pats, ierakstot adresi pārlūkā.
Kalendāra ielūgumi ar saiti (*Calendar phishing*)	Pikšķerēšanas mēģinājumi var tikt izplatīti caur kalendāra ielūgumiem, kuros iekļautas viltotas saites vai reģistrācijas formas.	Kalendārā pēkšņi parādās neparasti uzaicinājumi. Piemērs: **"Tikšanās ar Izglītības un zinātnes ministriju ar saiti "reģistrēties"".**	Neatver ielūgumos sūtītās saites, ja neesi bijis informēts par tikšanos. Pārbaudi informāciju, izmantojot citu saziņas formu.
Kvadrātkodu pikšķerēšana (*Quishing*)	QR kodi jeb kvadrātkodi var novirzīt uz viltotām lapām, kas prasa pieteikšanās datus, vai lejupielādēt ļaunprogrammatūru.	QR jeb kvadrātkods uz plakāta. Piemērs: **norādīts "Materiāli skolotājiem", kas ved uz pieteikšanās lapu, kurā prasa ievadīt E-klases konta piekļuves datus.**	Skenē kvadrātkodus tikai no uzticamiem avotiem.
Dokumenta pielikums ar ļaunatūru	E-pastiem pievienoti dokumenti ar nezināmu saturu var inficēt datoru, ja tos atver.	Saņemts kolēģa e-pasts ar "stundu sarakstu" vai "vecāku sapulces protokolu" .docm/.xlsm formātā, kas pēc atvēršanas prasa veikt papildu darbības.	Neatver nezināmas izcelsmes e-pasta pielikumus. Ja e-pasts vai tā pielikums izskatās aizdomīgs, – sazinies ar kolēģi citās saziņas vietnēs un noskaidro situāciju.

Atjauninājumi un ierīces

Viens no vienkāršākajiem, bet visbiežāk aizmirstajiem digitālās drošības pasākumiem ir regulāri sistēmu un programmu atjauninājumi. Tie novērš zināmas drošības ievainojamības un uzlabo ierīču darbību un stabilitāti.

Kāpēc tas ir svarīgi?

- Ražotāji regulāri publicē drošības ielāpus, lai aizsargātu datorus, planšetes un telefonus pret jaunākajiem kiberuzbrukumiem.
- Novecojušas sistēmas – tas ir visbiežākais iemesls, kāpēc ļaunprātīga programmatūra spēj iekļūt datorā. Uzbrucēji izmanto zināmas kļūdas, lai iekļūtu tajā bez lietotāja ziņas.
- Neatjauninātas programmas bieži kļūst nesaderīgas ar jaunām platformām (piemēram, E-klase, *Google Meet*).
- Skolotāja datorā vai telefonā glabājas sensitīvi dati par skolēniem un vērtējumiem, tāpēc ierīces drošība nozīmē arī datu drošību.

Ko vajadzētu atjaunināt?

- Operētājsistēmu (*Windows, macOS, iOS, Android* u. c.);
- Interneta pārlūkprogrammas (*Chrome, Firefox, Edge*);
- Antivīrusu programmatūru;
- Biroja lietotnes (*Microsoft Office, Google Docs* papildinājumi);
- Mobilās lietotnes, ko izmanto darbam (piemēram, *Zoom, Google Meet, MS Teams*).

Kategorija	Piemēri	Ieteikums
Operētājsistēma	*Windows, macOS, iOS, Android*	Ieslēdz automātiskos atjauninājumus; pārbaudi reizi mēnesī.
Interneta pārlūkprogrammas	*Chrome, Edge, Firefox, Safari*	Pārlūkprogrammas parasti sevi atjauno pašas – ļauj tām atjaunoties automātiski.
Antivīrusu un drošības risinājumi	*Windows Defender, Avast, Bitdefender*	Aktivizē reāllaika aizsardzību.
Darba un mācību lietotnes	*Microsoft Office, Google Docs* papildinājumi, *LibreOffice*	Pārbaudi, vai instalētā versija ir jaunākā.
Tiešsaistes saziņas un mācību rīki	*Zoom, Google Meet, MS Teams*	Atjauninājumi bieži labo drošības un audio vai video kļūdas.
Mobilās lietotnes	*WhatsApp, Gmail,* E-klase u. c.	Aktivizē automātiskos atjauninājumus.
Pārlūku paplašinājumi un spraudņi	PDF failu skatīšanās programmas, tulkošanas vai reklāmu bloķētāji	Reizi mēnesī pārskati un izdzēs tos, kas vairs nav vajadzīgi.

Ieteikumi drošai ierīču pārvaldībai

- Aktivizē automātiskos atjauninājumus datorā, planšetē un telefonā.
- Pārbaudi manuāli reizi mēnesī, īpaši tad, ja izmanto privāto datoru darbam.
- Izmanto tikai oficiālos veikalus (*Google Play*, *App Store*) – neinstalē programmas no nezināmiem avotiem.
- Nelieto novecojušu programmatūru (piemēram, *Windows 7* vai vecas *MS Office* versijas).
- Restartē ierīci pēc lielajiem atjauninājumiem – tie bieži stājas spēkā tikai pēc restarta.
- Pievērs uzmanību pārlūka brīdinājumiem (piemēram, "Šī lapa nav droša") – tie parādās bieži tieši novecojušās versijās.
- Iemāci skolēniem: atjauninājumi nav traucēklis, bet digitālās drošības pamats.

Papildu drošības padomi

- Izmanto antivīrusu datora drošībai.
- Izmanto bezmaksas rīku individuālu lietotāju un organizāciju pasargāšanai no kiber-apdraudējumiem (piemēram, DNS ugunsmūris).
- Regulāri dublē svarīgos failus (vērtējumus, dokumentus) mākonī vai ārējā diskā.
- Atinstalē lietotnes no ierīcēm, kuras vairs nelieto (vecais telefons, dators u. c.).
- Atvieno publiskos Wi-Fi tīklus no ierīces, kad tie nav nepieciešami.

Datu aizsardzība un privātums

Skolotāji ikdienā strādā ar sensitīviem datiem – skolēnu sasniegumiem, veselības informāciju, atzīmēm, vecāku kontaktinformāciju. Tāpēc ir īpaši svarīgi ievērot personas datu aizsardzības (GDPR) principus.

Galvenie drošas datu apstrādes pamatprincipi

- Minimālisms – tikai nepieciešamie dati konkrētam mērķim.
- Droša glabāšana – dati tiek glabāti tikai autorizētās platformās.
- Piekļuves ierobežošana – tikai tiem, kam tas nepieciešams.
- Regulāra pārskatīšana – nevajadzīgie dati tiek dzēsti.

Praktisks piemērs: Skolotāja Ilze vēlas nosūtīt vecākiem informāciju par konsultācijām. Viņa izmanto savu personīgo *Gmail* e-pastu un sūta ziņu, kurā visiem adresātiem redzami citu vecāku e-pasta kontakti, kas ir personas datu aizsardzības pārkāpums.

Pareizais risinājums: izmantot skolas oficiālo e-pasta adresi un nosūtīt e-pasta vēstuli, izmantojot funkciju "Bcc" (*Blind Carbon Copy*), lai adresāti neredzētu cits cita kontaktinformāciju.

Kur un kā drīkst glabāt skolēnu datus?

Platforma	Vai drīkst glabāt?	Piezīmes
E-klase, *Mykoob*, *Tamo*	Jā	Sertificētas izglītības sistēmas ar atbilstošiem drošības un šifrēšanas protokoliem.
Google Workspace for Edu	Jā	Ja izmanto oficiālu skolas domēnu un ievēro drošības iestatījumu vadlīnijas.
Personīgais *USB* datu nesējs vai dators	Nav ieteicams	Pastāv datu zuduma vai ļaunatūras inficēšanas risks.
Personīgais e-pasts (piemēram, *inbox* vai *Gmail*)	Nav ieteicams	Neatbilst personas datu aizsardzības (GDPR) prasībām un nav pietiekamas drošības garantijas.

Ieteikumi skolotājiem:

- neglabājiet skolēnu sarakstus vai vērtējumus uz darba virsmas vai ārpus autorizētām sistēmām;
- iestatiet piekļuves tiesības *Google* dokumentiem, tabulām vai mapēm (*View only, Edit, Comment*);
- ja dati jāpārsūta kolēģiem, izmantojiet šifrētas saites vai failus, kas aizsargāti ar paroli.

Sociālā inženierija

Sociālā inženierija ir manipulācijas metode, kurā uzbrucēji izmanto cilvēku uzticēšanos un emocijas, lai iegūtu piekļuvi informācijai vai sistēmām. Atšķirībā no tehniskiem uzbrukumiem šādi mēģinājumi balstās uz pārliecināšanu, steidzamības radīšanu vai bailēm,– piemēram, viltoti e-pasti, kas "it kā" sūtīti no kolēģiem vai skolas vadības ar aicinājumu rīkoties nekavējoties.

Izplatītākās metodes:

Skolotāji bieži ir mērķauditorija dažādiem digitālajiem krāpniekiem, kuri cenšas iegūt piekļuvi skolas sistēmām vai personīgajiem datiem. Šeit ir daži izplatītākie scenāriji, kam jāpievērš uzmanība.

1. "Tehniskais atbalsts" zvana vai raksta:

Persona izliekas par IT speciālistu un piedāvā palīdzību ar datoru, e-klasi vai citu sistēmu, vienlaikus lūdzot piekļuvi tavam datoram, kontam vai parolēm.

Piemērs: "Labdien, mēs no IT nodaļas redzam kļūdu jūsu profilā. Lūdzu, lejupielādējiet šo rīku (*AnyDesk/TeamViewer)*, lai to salabotu."

Kā izvairīties: IT speciālisti nekad neprasa paroles. Attālinātu piekļuvi dod tikai ar iepriekšēju saskaņošanu un tikai skolas apstiprinātos rīkos. Ja rodas šaubas – labāk piezvani un pārliecinies pats.

2. "Vadītāja" e-pasti:

Krāpnieki izmanto steidzamību un adreses, kurās burti vai simboli izskatās līdzīgi (piemēram, "0" vietā "o"), lai maldinātu e-pasta saņēmējus.

Piemērs: "Steidzami līdz plkst. 14.00 atsūti 9.b klases vērtējumu izrakstus šeit (saite)" vai "Nosūti dokumentus tagad uz direktore@sk0la.lv".

Kā izvairīties: Pārbaudi sūtītāja adresi (salīdzini ar iepriekšējām īstajām sarakstēm) un noskaidro pieprasījuma mērķi, izmantojot citu saziņas formu (piemēram, piezvanot).

3. "Skolēna vecāks" saziņas platformā *WhatsApp* vai e-pastā:

Krāpnieks izliekas par skolēna vecāku, kurš "it kā" steidzami vēlas informāciju par bērnu vai vērtējumiem.

Piemērs: "Lūdzu, atsūtiet Jāņa pēdējos vērtējumus PDF failā."

Kā izvairīties: nekad neizpaud skolēnu personas datus ārpus oficiālajām sistēmām. Skolēnu personas dati tikai oficiālajās sistēmās (piemēram, E-klase).

4. Balss ziņas ar viltotu identitāti

Krāpnieki var sūtīt balss ziņas vai ierakstus, izlikdamies par kolēģiem vai skolas vadību, lai iegūtu informāciju vai konkrētu rīcību.

Piemērs: Saziņas platformā *WhatsApp* ir atsūtīta balss ziņa no nepazīstama numura, "it kā no direktores" ar lūgumu atsūtīt skolēnu kontaktinformāciju.

Kā izvairīties: neapstiprini pieprasījumus balss ziņās un pārzvani uz sev zināmu numuru.

5. Nezināms USB datu nesējs

Nezināmi datu nesēji var saturēt ļaunprogrammatūru, kas inficē datoru uzreiz, kad tie tiek pievienoti.

Piemērs: skolas gaitenī atrasts USB datu nesējs ar nosaukumu "9.c pārbaudes darbi".

Kā izvairīties: nepievieno nezināmus USB datu nesējus savam datoram un nodod IT speciālistam tos pārbaudei.

Kā sevi pasargāt?

1) Pārbaudi sūtītāja identitāti, – pat ja ziņa šķiet no kolēģa, vadības vai vecāka.

Krāpnieki izmanto līdzīgus vārdus, kļūdaini pierakstītas e-pasta adreses vai viltotas profila bildes. Skaties domēna vārdu pēc "@", toni un steidzamību. Ja rodas šaubas, sazinies citā kanālā (piezvani vai raksti e-klasē).

2) Nekad neievadi paroles vai piekļuves kodus, ja pieprasījumu saņem e-pastā, čatā vai telefonsarunas laikā.

Saites var novirzīt uz viltotām lapām, kas izskatās kā īstās (E-klase, *Google, Microsoft* u. c.). Atver vietni manuāli, ierakstot adresi.

3) Nesniedz attālinātu piekļuvi savam datoram vai sistēmām nevienam, kam neesi pilnībā pārbaudījis identitāti un nepieciešamību.

Krāpnieki bieži lūdz uzstādīt *AnyDesk/TeamViewer* u. c. Attālinātu piekļuvi piešķir tikai autorizētam skolas IT speciālistam, apstiprinātā rīkā un pēc iepriekšējas vienošanās.

4) Ja rodas pat vismazākās šaubas – apstājies un pārbaudi.

Steiga ir krāpnieka sabiedrotais. Pirms izpildi lūgumus, klikšķini uz saitēm, atver pielikumus vai sūti datus, konsultējies ar kolēģi, IT atbalsta dienestu vai vadību.

Ko darīt, ja tomēr noklikšķināji uz saites vai ievadīji datus?

- Nekavējoties nomaini paroli (arī citās vietnēs, kur tika izmantota tā pati parole).
- Ja iespējams, atsauc piekļuvi.
- Informē IT atbalsta dienestu un vadību, pabrīdini kolēģus par iespējamu krāpšanu.
- Ja atvērts aizdomīgs pielikums, – atvieno datoru no interneta tīkla un informē IT speciālistu.

Droša uzvedība tiešsaistē

Internets ir kā publisks laukums – viss, ko mēs tur darām, atstāj pēdas. Šīs pēdas sauc par digitālo nospiedumu, un tās var ietekmēt gan skolēnu, gan skolotāju reputāciju, drošību un pat nākotnes iespējas.

Kas veido digitālo nospiedumu?

Pat šķietami nenozīmīga aktivitāte internetā var saglabāties ilgstoši un kļūt publiski pieejama – arī pēc vairākiem gadiem.

- Sociālo tīklu ieraksti, komentāri, attēli.
- Atrašanās vietas atzīmes un lietotņu lietošanas paradumi.
- Profili dažādās platformās (piemēram, *YouTube, Instagram, TikTok*).
- Komentāri forumos, čatos, spēļu platformās.

Ko skolotāji var mācīt skolēniem (un ievērot paši)

- Padomā, pirms publicē. Pirms ievieto foto vai komentāru, pajautā sev: vai būtu pieņemami, ja šo redzētu direktors, kolēģi vai vecāki?
- Pārvaldi privātuma iestatījumus. Regulāri pārbaudi, ko redz citi – vai profils ir publisks, vai foto un ieraksti redzami visiem?
- Komunicē cieņpilni. Tiešsaistes vide neatbrīvo no atbildības – izvairies no negatīviem komentāriem, baumām vai sarkastiskiem ierakstiem.

Uzmanies no aizdomīgām saitēm – sociālajos tīklos bieži izplatās krāpnieciskas saites, kas var nozagt lietotāja datus vai inficēt ierīci.

Ieteikumi skolotājiem

- **Saglabā profesionālās robežas.** Nepievieno skolēnus savos personīgajos profilos (piemēram, *Facebook, Instagram*). Saziņai izmanto oficiālos kanālus – e-klasi vai skolas e-pastu.
- **Veido pārdomātu publisko tēlu.** Skolotāja profils ir daļa no viņa profesionālās identitātes – arī ārpus darba laika. Izvairies no ierakstiem vai attēliem, kas var radīt pārpratumus un negatīvi ietekmēt skolas vai tavu reputāciju.
- **Aizsargā skolēnu privātumu.** Neievieto skolēnu foto, vārdus vai citus datus bez vecāku un skolas atļaujas.
- **Esi paraugs digitālajai kultūrai.** Demonstrē skolēniem, ka droša, cieņpilna un atbildīga uzvedība internetā ir tikpat svarīga kā klātienē.

Darbā ar skolēniem izmanto **Drossinternets.lv** izstrādātos metodiskos mācību materiālus:

- Interaktīvu materiālu kopa **"Make it clear"** darbam ar 11-17 g.v. skolēniem, kas ietver situāciju izspēli, uzdevumus terminu skaidrojumiem un testu zināšanu pārbaudei par tēmām: digitālā drošība; privātums; kritiskā domāšana; fakti un viedokļi; naida runa u.c.

  Programmas materiāli →

- **"Esi interneta izcilnieks!"** programmas materiālus (rokasgrāmata, uzdevumi, prezentācijas spēle) skolēnu izglītošanai par 5 svarīgākajām prasmēm būt gudriem, piesardzīgiem, laipniem, drosmīgiem un rūpēties par savu drošību.

  Programmas materiāli →

- **Digitālās pilsonības rokasgrāmatu** darbam ar 13-17 g.v. jauniešiem, kurā ietvertas 30 ar digitālo pratību, medijpratību un digitālajām tehnoloģijām saistītas atgādnes skolēniem, kā arī idejas pedagogiem skolēnu tekstpratības pilnveidei un diskusiju organizēšanai klasē. Rokasgrāmatā ietverti 4 tēmu bloki: Mēs tīmeklī; Lieto internetu gudri; Apzinies riskus; Digitālā pasaule.

  Programmas materiāli →

Kiberhigiēna ikdienā

Tāpat kā personīgā higiēna rūpējas par mūsu veselību, kiberhigiēna palīdz uzturēt digitālo vidi tīru un drošu. Tā sastāv no maziem, bet ļoti nozīmīgiem paradumiem, kas aizsargā personīgos un darba datus, samazina kiberrisku iespēju un veido atbildīgas digitālās uzvedības kultūru skolā — gan skolotājiem, gan skolēniem.

Ikdienas drošības paradumi skolotājiem

- Vienmēr izraksties no platformām pēc to lietošanas. Pārliecinies, ka esi izgājis no profila — īpaši, ja dators tiek koplietots (piemēram, E-klase, *Google* konts, *Zoom*).
- Bloķē datoru vai planšeti, aizejot no darba vietas. Īpaši svarīgi koplietojamās telpās – skolotāju istabās vai kabinetos, kur datoru izmanto vairāki cilvēki.
- Neizmanto publiskus Wi-Fi tīklus bez VPN. Atvērtie tīkli (piemēram, kafejnīcās, konferencēs vai pasākumos) ir neaizsargāti pret datu pārtveršanu. Ja nepieciešams strādāt ārpus skolas, izmanto mobilo internetu vai drošu VPN savienojumu.
- Neuzglabā failus uz datora darba virsmas vai "Lejupielāžu" mapē. Saglabā dokumentus drošā vietā – skolas mākonī, *OneDrive* vai šifrētā mapē.
- Nepieļauj, ka skolēni izmanto skolotāja datoru, pat uz īsu brīdi. Pat ar labiem nodomiem skolēni var netīšām atvērt sensitīvus failus vai izmainīt iestatījumus.

Ko vēl iekļaut savā ikdienas kiberhigiēnā?

- **Regulāri veic antivīrusu skenēšanu** (piemēram, reizi nedēļā vai automātiski).
- **Dzēs sīkfailus (*cookies*) un atmiņu pārlūkprogrammā**, lai aizsargātu privātumu un uzlabotu ierīces veiktspēju.
- **Pārbaudi drošības iestatījumus savos kontos**, piemēram, izmantojot *Google Privacy Checkup* vai *Microsoft Security Panel*.
- **Iestati automātisku ekrāna bloķēšanos** pēc īsa neaktivitātes brīža (piemēram, 5 minūtēm).
- **Regulāri atjauno programmatūru** – gan datoram, gan pārlūkprogrammai, gan mācību lietotnēm.
- **Neizmanto vienas un tās pašas paroles** dažādos kontos – izmanto paroļu pārvaldnieku vai divfaktoru autentifikāciju (2FA).

Datu rezerves kopiju glabāšana (*Backup*)

Pat vislabāk aizsargātās sistēmas nav pasargātas no neparedzētiem gadījumiem – tehniskām kļūmēm, ļaunprogrammatūras vai vienkāršas cilvēciskas kļūdas.

Regulāra datu rezerves kopiju veidošana ir ļoti būtiska aizsardzības līnija, kas ļauj atjaunot datus un turpināt darbu bez lieliem zaudējumiem.

Kāpēc veidot rezerves kopijas?

- **Aizsardzība pret ļaunprogrammatūru un "ransomware" uzbrukumiem.**
  Šāda programmatūra var bloķēt piekļuvi failiem un pat pieprasīt izpirkuma maksu. Ja ir rezerves kopija, dati paliek drošībā.
- **Datu atjaunošana pēc kļūdainas dzēšanas vai ierīces bojājuma.**
  Piemēram, ja pazūd vērtējumu tabula, prezentācija vai skolēnu darbi, – tos iespējams ātri atjaunot no rezerves kopijas.
- **Droša uzglabāšana mācību materiāliem un dokumentiem.**
  Projekti, pārbaudes darbi, E-klases eksporta faili vai sertifikāti – tie ir vērtīgi resursi, kurus vērts saglabāt ilgtermiņā.

Ieteicamās datu glabāšanas metodes

Metode	Piemēri	Priekšrocības	Riski
Mākoņ-pakalpojums	*Google Drive, OneDrive, Dropbox, iCloud*	Pieejams no jebkuras vietas. Automātiski sinhronizējas un saglabā versijas. Nav nepieciešams fizisks datu nesējs.	Nepieciešama droša parole un divfaktoru autentifikācija (2FA). Dati tiek glabāti ārpus skolas servera – jāievēro privātuma prasības.
Ārējais disks (HDD/SSD)	Fizisks disks	Nav piesaistīts internetam – drošāks pret kiberuzbrukumiem. Piemērots lieliem datu apjomiem.	Var tikt pazaudēts, nozagts, bojāts. Nepieciešama manuāla kopiju atjaunošana.
USB zibatmiņa	Portatīvs risinājums nelieliem failiem	Ērti lietojams un viegli pārnēsājams.	Viegli pazaudējams, zems drošības līmenis, parasti dati nav šifrēti

Ieteikumi drošai datu dublēšanai skolotājiem:

- Izmanto uzticamus mākoņpakalpojumus (piemēram, *Google Drive, OneDrive, iCloud* vai skolas serveri).
- Regulāri pārkopē svarīgākos failus ārējā datu nesējā (USB, ārējā diskā) vai drošā tīkla mapē.
- Neturi visas kopijas vienā vietā. Ideālā gadījumā – viena kopija mākonī, otra ārējā datu nesējā.
- Atjaunošanas pārbaude. Laiku pa laikam pārliecinies, ka failus tiešām vari atvērt un atjaunot.
- Sargā datu nesējus. Ja izmanto USB vai ārējo disku, glabā to drošā vietā, kas nav pieejama skolēniem.

DNS ugunsmūris

DNS ugunsmūris (*Firewall*)ir aktīvās aizsardzības bezmaksas rīks individuālu lietotāju un organizāciju pasargāšanai no aktuālajiem kiberapdraudējumiem Latvijas kibertelpā, piemēram, viltus banku lapām, krāpnieciskām tirdzniecības platformām, vīrusus izplatošām vietnēm u. c.

Kā ugunsmūris darbojas?

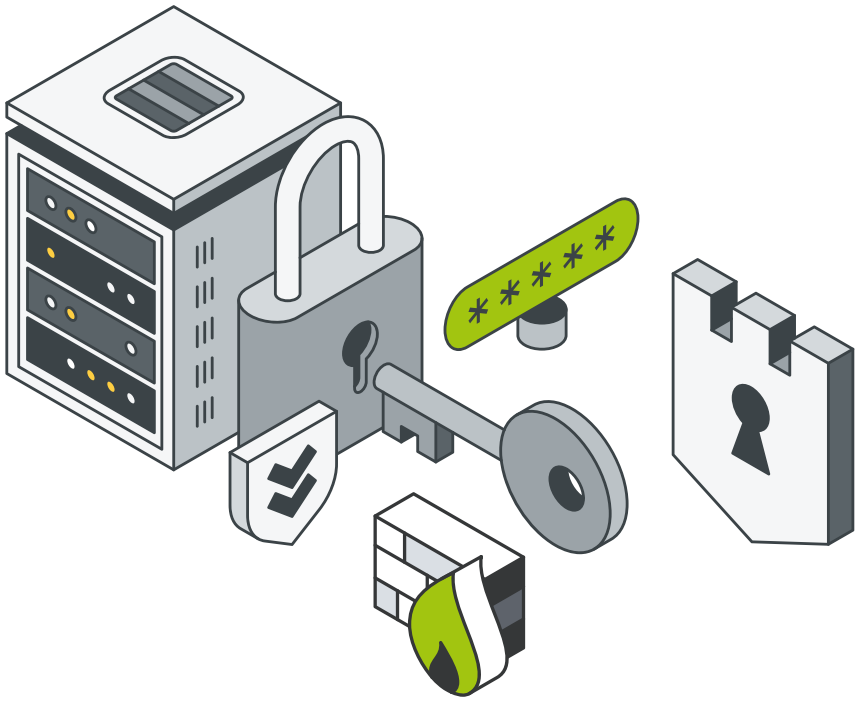
Ugunsmūris ir kā sargs, kas pārbauda katru tīmekļa adresi, ko lietotājs mēģina atvērt, un bloķē piekļuvi kaitīgām vai krāpnieciskām lapām, pirms tās tiek ielādētas. Tā ierīces automātiski tiek pasargātas no vīrusiem, pikšķerēšanas un citiem kiberdraudiem.

Kāpēc tas ir noderīgi?

Ugunsmūris pasargā datoru, telefonu un citas ierīces, nodrošinot drošu interneta pārlūkošanu. Tas nepārtraukti darbojas fonā, neradot traucējumus interneta lietošanā, bet nodrošinot, ka ierīces un dati ir pasargāti.

Padoms:

Pieslēdziet ugunsmūrī un informējiet par šādu iespēju arī skolēnu vecākus. Kiberincidentu novēršanas institūcija CERT.LV sadarbībā ar NIC ir izveidojusi rīku "DNS ugunsmūris" – bezmaksas lietotni, kas atpazīst bīstamās vietnes un bloķē tās. Lietotni iespējams lejupielādēt *App Store* vai *Google Play* veikalā un izmantot bez maksas. DNS ugunsmūri iespējams uzstādīt arī datorā. Instrukcijas atrodamas dnsmuris.lv



Svarīgākais pamatskolas skolotājiem

Pamatskolas skolotājiem digitālās drošības jomā ir divējāda loma:

viņi ne tikai ievēro drošas digitālās uzvedības principus paši, bet arī veido skolēnu pirmo izpratni par drošu un atbildīgu rīcību internetā. Šajā vecumposmā bērni sāk patstāvīgi lietot internetu – spēlē spēles, skatās video, izmanto mācību platformas un sazinās ar citiem tiešsaistē, tāpēc skolotāja piemērs un skaidrojums ir īpaši nozīmīgs.

Galvenie uzdevumi un ieteikumi

- **Aizsargā savus darba kontus.**

  Aizsargā visus savus darba kontus (E-klase, *Google*, e-pasts u. c.) ar unikālām parolēm un divfaktoru autentifikāciju (2FA). Tas palīdz novērst neatļautu piekļuvi skolēnu datiem un mācību materiāliem.

- **Skaidro skolēniem drošības jautājumus saprotamā, vecumam atbilstošā valodā.**

  Piemēram: "Neatver ziņu no cilvēka, kuru nepazīsti" vai "Ja kaut kas liekas aizdomīgs – pastāsti pieaugušajam".

- **Runā par paroļu nozīmi radošā un pozitīvā veidā.**

  Piemēram, kopā ar klasi izveido "supervaroņu paroles" – frāzes ar cipariem un simboliem, kuras ir drošas, bet viegli iegaumējamas. Bet svarīgi lai visa klase pēc tam neizmanto vienas un tās pašas paroles

- **Analizējiet reālas situācijas un rīcības piemērus.**

  Diskutējiet par to, kā rīkoties, ja:

  – tiek saņemta aizdomīga ziņa,

  – redzams aizvainojošs komentārs,

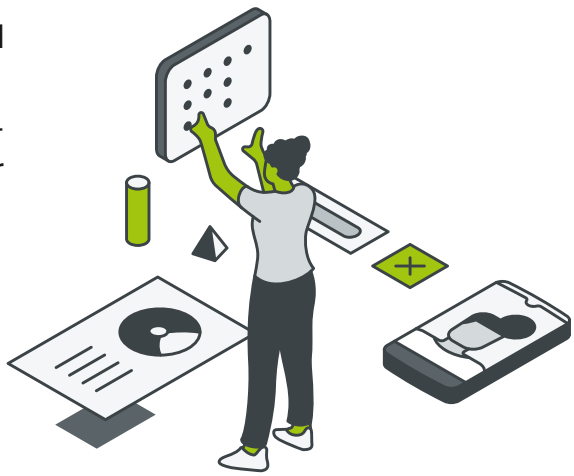
  – kāds lūdz kopīgot privātu informāciju vai foto.

- **Pārrunā ar skolēniem, kā lietot sociālos tīklus.**

  Ne tikai par drošību, bet arī par cieņpilnu un atbildīgu uzvedību tiešsaistē – ko drīkst un ko nedrīkst publicēt, kā atšķirt joku no aizvainojuma un kā cienīt citu privātumu.

- **Padoms skolotājiem: pamatskola ir brīdis, kad bērni veido pirmos digitālos ieradumus.**

  Skolotājs var palīdzēt viņiem iemācīties – internets nav tikai izklaide, bet arī vide, kur jāievēro cieņa, drošība un atbildība.



Svarīgākais vidusskolas skolotājiem

Vidusskolēni ir digitāli aktīvi, pašpārliecināti un informācijas ziņā pieredzējuši lietotāji, taču bieži nenovērtē digitālās uzvedības riskus un savas rīcības iespējamās sekas.

Šajā posmā skolotāja loma ir palīdzēt jauniešiem attīstīt kritisko domāšanu, izprast digitālo reputāciju un lietot tehnoloģijas atbildīgi – gan mācībās, gan ārpus tām.

Prioritātes un ieteicamā rīcība:

- **Diskusijas par digitālo identitāti un reputāciju.**

  Runā ar skolēniem par to, kā viņu darbības internetā veido personīgo tēlu.

  (***Ko par mani var atrast Google meklētājā? Kādu iespaidu radīšu darba devējam vai augstskolai?***) Iedrošini skolēnus pārdomāt, ko viņi publicē un kā tas var ietekmēt viņu nākotni.
- **Kritiskā domāšana un dezinformācijas atpazīšana.**

  Analizējiet kopā ziņu rakstus, sociālo tīklu ierakstus un video. Māci skolēniem pārbaudīt avotus, salīdzināt informāciju un domāt: kas ir šīs ziņas autors, kāds varētu būt viņa mērķis?
- **Autortiesību un akadēmiskā godīguma ievērošana.**

  Skolēniem jāzina, kā pareizi izmantot citu radītos materiālus – attēlus, mūziku, tekstus.

  Praktiski piemēri: norādīt atsauces, citēt korekti. Tas veicina cieņu pret autoru darbu un godīgumu mācību procesā.
- **Kibermobings un droša komunikācija.**

  Veido atklātas sarunas par tiešsaistes uzvedību, cieņu un empātiju. Skolotājam svarīgi pamanīt signālus – sliktu noskaņojumu, konfliktus sociālajos tīklos – un piedāvāt atbalstu vai palīdzību.

  Iesaisti arī skolas psihologu, sociālo pedagogu vai vecākus, ja situācija kļūst nopietna.
- **Datu drošība koplietošanas projektos.**

  Grupas darbos izmanto tikai drošas platformas ar ierobežotu piekļuvi (piemēram, *Google Drive, Microsoft 365*). Iemāci skolēniem piešķirt piekļuvi tikai nepieciešamajiem cilvēkiem un aizsargāt failus ar drošām parolēm.

Padoms skolotājiem!

Neignorē jauniešu tiešsaistes vidi – tā ir būtiska viņu ikdienas daļa. Esi atvērts sarunai par to, kas notiek ārpus klases sienām – arī internetā. Ja konflikti "pārceļas" no sociālajiem tīkliem uz klasi, rīkojies savlaicīgi: iesaisti skolas psihologu, klases audzinātāju vai vecākus un kopīgi meklējiet risinājumu.

Darbā ar skolēniem izmanto Drossinternets.lv izstrādātos metodiskos mācību materiālus:

- Interaktīvu materiālu kopu "Make it clear", kas ietver situāciju izspēli, uzdevumus terminu skaidrojumiem un testu zināšanu pārbaudei par tēmām: digitālā drošība; privātums; kritiskā domāšana; fakti un viedokļi; naida runa u. c.

  Metodiskais mācību materiāls →

- Digitālās drošības rokasgrāmatu darbam ar 13-17 g. v. jauniešiem, kurā ietvertas 30 ar digitālo pratību, medijpratību un digitālajām tehnoloģijām saistītas atgādnes skolēniem, kā arī idejas pedagogiem skolēnu tekstpratības pilnveidei un diskusiju organizēšanai klasē. Rokasgrāmatā ietverti četri tēmu bloki: "Mēs tīmeklī"; "Lieto internetu gudri"; "Apzinies riskus"; "Digitālā pasaule".

  Metodiskais mācību materiāls →

Svarīgākais datorikas skolotājiem

Datorikas skolotājam ir unikāla un ietekmīga loma digitālās drošības izglītībā. Viņš ne tikai māca teoriju par kiberdrošību, bet arī praktiski demonstrē drošas rīcības principus, palīdzot skolēniem attīstīt prasmes, kas būs noderīgas gan augstskolā, gan darba vidē. Kiberdrošības jautājumi datorikas stundās ļauj skolēniem saprast, kā aizsargāt datus, izstrādāt drošas sistēmas un domāt atbildīgi digitālajā pasaulē.

Datorikas mācību stundās iemāci svarīgāko:

- **Tīkla drošība.**

  Skaidro un demonstrē, kā darbojas ugunsmūris, porti, IP adreses un piekļuves kontrole.

  Skolēni var praktiski modelēt vienkāršu tīklu vai pārbaudīt, kā datu plūsma tiek aizsargāta.
- **Šifrēšana un autentifikācija.**

  Parādi, kā informāciju var aizsargāt, izmantojot paroles, divfaktoru autentifikāciju (2FA) un failu šifrēšanu.

  Praktisks uzdevums, ko iekļaut: skolēni izveido šifrētu arhīvu vai failu ar paroli un pārbauda, kā dati tiek aizsargāti.
- **Droša programmēšana.**

  Īpaši aktuāli web izstrādes vai datubāzu nodarbībās.

  Iekļauj tēmas par ievades validāciju, SQL injekciju novēršanu, drošu paroļu glabāšanu un datu aizsardzību kodā. Uzsver, ka drošība ir neatņemama programmatūras kvalitātes daļa.
- **Kiberdrošības karjeras iespējas.**

  Iepazīstini skolēnus ar reālām profesijām: ētiskais hakeris, drošības analītiķis, datu aizsardzības speciālists u. c.

  Var izmantot videointervijas vai uzaicināt vieslektoru no IT nozares.
- **Pikšķerēšanas (*phishing*) simulācijas.**

  Izmantojot drošus un bezmaksas izglītojošus rīkus (piemēram, *PhishLabs, Google Phishing Quiz* vai *KnowBe4 Demo*), skolēni var praktiski redzēt, cik viegli var tikt apmānīti, un analizēt kļūdas drošā vidē.
- **Datu aizsardzības principi.**

  Māci skolēniem izprast personas datu nozīmi, piemēram, kā un kāpēc tos nedrīkst publicēt vai kopīgot bez atļaujas. Var analizēt īstus piemērus (piemēram, kā uzņēmums zaudēja klientu datus vai kā tika uzlauzts profils).
- **Privātuma un drošības iestatījumi un kur ziņot par pārkāpumiem.**

  Informē skolēnus par iestatījumiem un ziņošanas iespējām. Kopā izpētiet Drossinternets.lv izstrādāto Sociālo tīklu drošības ceļvedi, kurā saišu veidā apkopoti iestatījumi, palīdzības rīki un ziņošanas iespējas populārākajos e-pasta servisos, sociālo mediju platformās un spēļu platformās.

Papildu resursi un iniciatīvas, kur var iesaistīties:

- **Kiberkonkursi un izaicinājumi.**

Iesaisti skolēnus aktivitātēs, piemēram:

- Nacionālais kiberdrošības izaicinājums (https://kibiz.lv/)
- European Cyber Security Challenge (https://ecsc.eu/)
- Sacensības Kiberplēsis https://kiberplesis.lv/

Šie pasākumi attīsta gan tehniskās prasmes, gan komandas darbu un problēmu risināšanu.

- **Pašpilnveide skolotājam.**

Sekot līdzi brīvpieejamām apmācībām un jaunumiem kiberdrošībā, lai regulāri stiprinātu savas digitālās drošības prasmes:

- Aizsardzības ministrijas, t .sk. Nacionālā Kiberdrošības centra mājaslapā (https://cyber.gov.lv/),
- Latvijas Drošāka interneta centra tīmekļa vietnē (https://drossinternets.lv/).
- Kiberincidentu novēršanas institūcijas CERT.LV tīmekļa vietnē (https://esidross.lv/).

Svarīgākais izglītības pārvalžu darbiniekiem un skolu vadībai

Skolu vadība un izglītības pārvaldes veido pamatu drošības kultūrai izglītības iestādēs.

Tieši viņu lēmumi nosaka, cik droši tiek aizsargāti dati, cik sagatavots ir personāls un cik efektīvi iestāde spēj reaģēt uz drošības incidentiem. Kiberdrošība šajā līmenī nav tikai tehnisks jautājums – tā ir vadības atbildība, organizācijas kultūras un reputācijas daļa.

Galvenās prioritātes:

- **Kiberdrošības politikas izstrāde un ieviešana.**

  Jābūt skaidriem noteikumiem, kas attiecas uz visiem – skolotājiem, skolēniem, IT personālu un vadību.

  Tajā jāietver datu aizsardzības principi, piekļuves tiesības, informācijas apmaiņas kārtība, paroles un ierīču lietošana.

- **Lomu un atbildību noteikšana.**

  Skaidri jādefinē, kurš atbild par datu drošību un kā rīkojas drošības incidentu gadījumā.

  Kurš ziņo par incidentu? Kurš analizē cēloņus? Kurš informē sabiedrību vai citu augstākstāvošu institūciju? Caurskatāma darbību secība palīdz ātri reaģēt un samazina risku kļūdīties krīzes situācijā.

- **Regulāras personāla apmācības.**

  Kiberprasmes ir mainīgas – tās ir jāuztur un jāpilnveido.

  Organizējiet mērķtiecīgus semināru un praktiskas mācības par paroļu drošību, divfaktoru autentifikācijas lietošanu, pikšķerēšanas atpazīšanu un datu aizsardzības prasībām (GDPR).

  Ieteikums: iekļaut kiberdrošības tēmas arī jauno darbinieku apmācībā (ievadīšanā darbā).

- **Incidentu reaģēšanas plāns.**

  Katram darbiniekam jāzina, ko darīt datu noplūdes, vīrusu uzbrukuma vai sistēmas kļūmes gadījumā.

  Plānā jāietver paziņošanas soļi, atbildīgās personas, IT atbalsta un komunikācijas kanāli.

  Regulāra mācību simulācija (piemēram, "Kas notiek, ja E-klase uz brīdi nestrādā?"). Plāns palīdz būt gataviem negaidītām situācijām.

- **IT auditi un infrastruktūras drošības pārbaudes.**

  Veiciet regulāras pārbaudes, lai pārliecinātos, ka:

  – serveri ir šifrēti un atjaunināti;

  – rezerves kopijas tiek veidotas automātiski un pārbaudītas;

  – iekārtas (datori, planšetes) tiek izmantotas saskaņā ar drošības politiku;

  – tiek ieviesti e-pasta drošības standarti (SPF, DKIM, DMARC).

Praktisks piemērs

Pēc pikšķerēšanas incidenta kādā skolā izglītības pārvalde veic visaptverošu drošības auditu, ievieš e-pasta autentifikācijas aizsardzību (SPF/DKIM/DMARC) un nosaka, ka visiem darbiniekiem jāaktivizē divfaktoru autentifikācija (2FA). Pēc sešiem mēnešiem seko atkārtota pārbaude un mācības, lai pārliecinātos, ka drošības principi tiek ievēroti praksē.

Padoms vadībai:

- **Kiberdrošība kā stratēģisks jautājums.**

  Iekļaujiet to skolas un pārvaldes attīstības plānos, budžetā un darba kārtībā.

  Drošība nav izmaksu pozīcija, bet ieguldījums stabilitātē un darbības nepārtrauktībā.
- **Veido sadarbību ar IT speciālistiem un valsts iestādēm.**

  Uzturiet kontaktus ar kiberincindentu novēršanas institūciju CERT.LV un Datu valsts inspekciju, Latvijas Drošāka interneta centru un citām organizācijām, kas sniedz konsultācijas un apmācības par kiberdrošību.
- **Atbalstiet skolu drošības vēstniekus.**

  Iedrošiniet skolotājus, kas interesējas par digitālo drošību, kļūt par drošības vēstniekiem skolā – cilvēkiem, kuri palīdz kolēģiem un skolēniem ievērot labās prakses. Aiciniet savu skolu pedagogus pieteikties Drošāka interneta vēstnešu tīklam, ko koordinē Latvijas Drošāka interneta centrs.
- **Skolotāju digitālās un kiberdrošības prasmes nedrīkst uzskatīt par pašsaprotamām.**

  Tās jāattīsta mērķtiecīgi, regulāri un praktiski – tikai tad drošība kļūst par ikdienas kultūras sastāvdaļu, nevis par vienreizēju projektu.
- **Noteikumi mākslīgā intelekta (MI) rīku izmantošanai.** Skolas iekšējās kārtības noteikumos iekļaujiet arī noteikumus par mākslīgā intelekta rīku izmantošanu mācību procesā. Iedvesmai varat izmantot Vadlīnijas mākslīgā intelekta izmantošanai pamatizglītībā un vispārējā vidējā izglītībā.

Kur vērsties, ja noticis kiberuzbrukums

1. KRĀPNIEKU E-PASTS VAI SMS

- Ja saņēmi krāpniecisku e-pastu vai SMS (pikšķerēšana, viltus saites).
- ja redzi viltotu tīmekļvietni, kas izliekas par banku, e-parakstu u. c.
- Ja tava ierīce uzvedas aizdomīgi vai, iespējams, ir inficēta ar vīrusu.

Ziņo savam IT atbalsta dienestam un CERT.LV:

- rakstot uz e-pastu cert@cert.lv
- zvanot pa tālruni 67085888 (24/7)
- krāpniecisku SMS un telefona numuru pārsūtīšanai: +371 23230444 (telefona zvani netiek apstrādāti)

2. IZSPIEŠANA, ŠANTĀŽA

- Ja ir nozagti vai ļaunprātīgi izmantoti tavi personas dati vai identitāte.
- ja uzbrucējs draud, izspiež vai publicē tavu personīgo informāciju.

Ziņo Valsts policijai:

- pa tālr. 110
- rakstot e-adresē, sūtot elektroniski parakstītu e-pastu https://www.vp.gov.lv/lv/ka-zinot-policijai

3. DRAUDI BĒRNAM

- Ja apdraudēts bērns internetā (mobings, seksuāla rakstura sarakstes u. c.).
- Ja nepieciešams atbalsts un padomi, kā runāt ar bērnu par drošību internetā.

Sazinies ar Drošāka interneta centru:

- konsultatīvais tālrunis: 116111 (bērnu un jauniešu uzticības tālrunis, nodrošina Bērnu aizsardzības centrs)
- ziņot par saturu: uz e-pastu zinojumi@drossinternets.lv vai Drossinternets.lv vietnē, aizpildot "Ziņot" formu

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:
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, rakstot uz e-pastu 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, rakstot uz e-pastu 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 tu vēlies, lai kāds izdzēš 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.

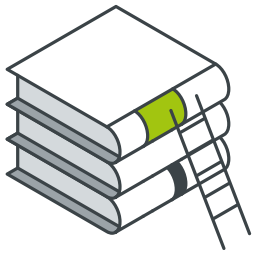
Ziņo "Melns uz balta", aizpildot anketu lietotnē
https://melnsuzbalta.lv/zino-par-dezinformaciju/

9. FINANSIĀLA KRĀPNIECĪBA

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

Sazinies ar savu banku un ziņo Valsts policijai pa tālr. 110.

Kiberdrošības vārdnīca



- **Autentifikācija:** procesa daļa, kur lietotājs apliecina savu identitāti (piemēram, ar paroli vai kodu).
- **Divfaktoru autentifikācija (2FA):** papildu drošības solis pēc paroles – piemēram, apstiprinājuma kods telefonā vai lietotnē.
- **Pikšķerēšana (*Phishing*):** krāpnieciska darbība, kad viltojuma e-pasts vai ziņa aicina ievadīt paroles vai datus.
- **Smikšķerēšana (*Smishing*):** pikšķerēšanas veids, kas notiek ar SMS vai ziņapmaiņas lietotnēm (piemēram, *WhatsApp*).
- **Vikšķerēšana (*Vishing*):** krāpniecība pa telefonu – persona izliekas par bankas vai IT darbinieku, lai iegūtu datus.
- **Ļaunprogrammatūra (*Malware*):** vispārīgs termins visām kaitīgām programmām – vīrusiem, spiegprogrammatūrai, izspiedējvīrusiem utt.
- **Izspiedējvīruss (*Ransomware*):** vīruss, kas bloķē failus un prasa samaksu par to atbloķēšanu.
- **Ugunsmūris (*Firewall*):** programmatūra vai ierīce, kas kontrolē datu plūsmu starp datoru un internetu, bloķējot aizdomīgus savienojumus.
- **Antivīrusu programma:** programma, kas atpazīst un dzēš ļaunprogrammatūru.
- **Paroļu pārvaldnieks (*Password Manager*):** droša programma paroļu glabāšanai un automātiskai ievadei.
- **Datu noplūde (*Data breach*):** situācija, kad personas dati tiek nozagti, publicēti vai nonāk pie nepiederošām personām.
- **Sociālā inženierija:** manipulācijas veids, kur uzbrucējs izmanto cilvēku uzticību vai bailes, lai iegūtu informāciju.
- **Kibermobings:** aizskaršana, pazemošana vai draudi internetā vai sociālajos tīklos.
- **VPN (*Virtual Private Network*):** tehnoloģija, kas šifrē interneta savienojumu un pasargā lietotāju no datu pārtveršanas.
- **Šifrēšana (*Encryption*):** procesa veids, kur dati tiek pārveidoti nesalasāmā formā, lai tos varētu nolasīt tikai ar atļauju.
- **Rezerves kopija (*Backup*):** datu dublēšana drošā vietā, lai tos varētu atjaunot, ja notiek bojājums vai uzbrukums.
- **Digitālais nospiedums:** visas pēdas, ko atstāj tiešsaistē – komentāri, bildes, meklējumi, profili u. c.
- **Kiberhigiēna:** ikdienas paradumi, kas palīdz saglabāt drošību digitālajā vidē.
- **Mākoņpakalpojums (*Cloud service*):** tiešsaistes vieta datu glabāšanai un koplietošanai (piemēram, *Google Drive, OneDrive*).
- **CERT.LV:** kiberincidentu novēršanas institūcija – palīdz un sniedz atbalstu kiberdrošības jautājumos.

Uzdevumu piemēri mācību stundām

PAROLES

Tēma: paroļu drošība un stiprums.

Mērķis: izprast, kas padara paroli stipru un kāpēc vājas paroles ir bīstamas.

Norise:

Skolotājs sadala skolēnus pāros vai nelielās grupās.

Katra grupa izveido trīs paroles – ļoti vāju, vidēji stipru un drošu – vai sašķiro jau iepriekš sagatavotas paroles pēc to drošības pakāpes.

Skolotājs izmanto bezmaksas tiešsaistes rīku, piemēram, https://howsecureismypassword.net, lai pārbaudītu, cik ilgs laiks būtu nepieciešams šo paroļu uzlaušanai.

Diskusijas jautājumi:

Kādas iezīmes padara paroli drošu (garums, dažādi simboli, unikāls saturs)?

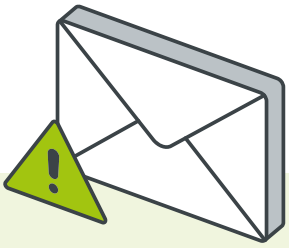
Kā izveidot drošu paroli, ko viegli atcerēties? Iekļaut informāciju par paroļu pārvaldnieku.

Papildus:

Noskatīties CERT.LV video par drošām parolēm:

Video par drošām parolēm →

Nepieciešams:
sagatavoti paroļu piemēri, dators ar interneta pieslēgumu.



KRĀPNIECISKAS ZIŅAS

Tēma: pikšķerēšanas atpazīšana

Mērķis: iemācīties pamanīt krāpnieciskas e-pasta ziņas pazīmes.

Norise:

Skolotājs sagatavo 3-4 e-pasta ziņu piemērus – vienu īstu (drošu), pārējos ar krāpnieciskas ziņas pazīmēm.

E-pasta ziņas var tikt parādītas uz ekrāna vai izdrukātas.

Skolēnu uzdevums: atzīmēt aizdomīgos elementus (dīvaina sūtītāja adrese, steidzamības radīšana, kļūdas tekstā, aizdomīga saite).

Skolotājs kopā ar klasi analizē katru e-pastu un pārrunā, kāpēc tas varētu būt drošs vai bīstams.

Diskusijas jautājumi:

Kādas ir visbiežāk sastopamās pikšķerēšanas pazīmes?

Kā rīkoties, ja saņem šādu e-pastu?

Nepieciešams:

sagatavoti e-pastu piemēri (drukāti vai digitāli).

Materiāls izstrādāts 2025.gada novembrī. Saturs tapis sadarbībā ar Aizsardzības ministriju, kiberincidentu novēršanas institūciju CERT.LV, Latvijas Drošāka interneta centru.