Kā saglabāt drošību virtuālajā vidē?

Ik dienas interneta vidē tiek pastrādāti neskaitāmi drošības pārkāpumi, zādzības un krāpšanas gadījumi. Kā iespējams sevi no tiem pasargāt?

Nesen Latvijā atkal nācās saskarties ar drošības pārkāpumu, kad kāds vidusskolas skolēns bija piekļuvis skolotājas kontam izglītības sistēmā E-klase.

Skolēns bija labojis savas un savu klasesbiedru atzīmes. Par pārkāpumu ticis ziņots un incidents novērsts, taču tas izgaismo plašāku problēmu – vai ikdienā pietiekami rūpīgi sargājam savus datus, lai nepiederošas personas tiem nevarētu piekļūt?

Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas Cert.lv IT drošības speciālists Gints Mālkalnietis uzskata, ka kopumā situācija Latvijā uzlabojas, taču aizvien cilvēki pieļauj pavisam elementāras kļūdas, kuru izskaušana varētu novērst arī visai nopietnus starpgadījumus.

Kādēļ notika starpgadījums ar ielaušanos skolotājas E-klases kontā?

Viens no galvenajiem priekšnosacījumiem personas datu drošības nodrošināšanai internetā ir piemērota parole. Skolotāju vadītie dati, atzīmes nav viņu personīgā informācija, tie ietekmē plašu cilvēku loku, tādēļ tie ir īpaši sargājami, informē Gints Mālkalnietis. Tieši drošības noteikumu neievērošana attiecībā uz paroles glabāšanu izraisīja attiecīgo incidentu ar skolotājas paroles izmantošanu, lai skolēns varētu nelikumīgi mainīt atzīmes.

Jaunietis izmantoja situāciju, kad pirms pāris gadiem no korporatīvo kontaktu sociālā tīkla “LinkedIn” tikuši nozagti vairāk nekā 100 miljoni paroļu datu, kas vēlāk bijuši pieejami internetā.

“Nelaime ir tā, ka cilvēki nereaģē uz brīdinājumiem no dažādiem portāliem, pakalpojumu sniedzējiem, kas informē, ka ir nepieciešams mainīt paroli. Ja nemaldos, no “LinkedIn” puses brīdinājums tika sūtīts vismaz divas reizes, taču parole netika nomainīta. Ja cilvēki nereaģē, tad piekļuves datus iespējams visai viegli sameklēt. Šajā gadījumā tas gāja kopā ar citu sliktu praksi – vienas paroles lietošanu vairākās vietnēs,” stāsta G.Mālkalnietis.

Lai ikdienā būtu vieglāk strādāt ar dažādām interneta vietnēm, izmantojot katrai savu unikālo paroli, Cert.lv iesaka izmantot t.s. paroļu pārvaldītājus. Internetā ir iespējams atrast dažādas versijas (gan maksas, gan bezmaksas), ko var izmantot gan datoros, gan telefonos un citās viedierīcēs. Attiecīgajā programmā tiek izveidots konts, kuru aizsargā viena gara parole, ar kuru tiek saglabātas daudzu kontu paroles. “Teorētiski Jūs riskējat, ja kāds no šī Jūsu paroļu faila uzzina garo paroli, bet tieši tāpēc ir nepieciešams izvēlēties ļoti garu paroli - jūtami virs 16 simboliem. Nevajag obligāti izveidot nesakarīgu paroli, galvenais - pietiekoši garu, ar dažādiem simboliem. Tā, katru reizi autorizējoties savā kontā, mēs to iekopējam no pārvaldnieka. Praksē nākas redzēt, ka portālu īpašnieki izvēlas aizliegt iespēju kopēt paroles, kas, manuprāt, ir nepareizi, jo tas spiež cilvēkus izvēlēties īsas un vienkārši uzlaužamas paroles. Šāda prakse ik pa laikam kaut kur parādās, bet īpašu drošību tā nedod,” skaidro G.Mālkalnietis. Visbiežāk cilvēki kļūdās tieši ar īso un vienkāršo paroļu izvēli, jo viņiem ir slinkums ar roku rakstīt garākas. Jāņem vērā, ka dažādām interneta vietnēm nevajadzētu izdomāt vienu universālu paroles sākumu un pēc tam tikai mainīt pēdējos divus vai trīs simbolus. Arī tas padarīs paroli diezgan nedrošu. Līdzīga kļūda ir pamainīt vien dažus burtus saskaņā ar izvēlēto pakalpojumu vai interneta vietni. Ja kaut kur parādās loģika, uzbrucējs to var viegli uzminēt un izdomāt arī visas pārējās pieejas.

Izmantot citas personas paroli – tie nav nevainīgi joki

E-klase un Cert.lv vēlas atgādināt, ka svešu paroļu izmantošana ir sodāma rīcība - nelikumīgas darbības ar fiziskās personas datiem ir administratīvi vai krimināli sodāmas.

Attīstoties tehnoloģijām, virtuālajā vidē tiek piedāvāts arvien plašāks pakalpojumu klāsts. Tieši tāpat parādās arvien jauni riski un pieaug cilvēku skaits, kuri virtuālajā vidē mēģina rīkoties negodprātīgi. Kā stāsta G.Mālkalnietis, mūsdienās skolēni bieži vien it kā ir izglītotāki par saviem vecākiem jaunajās tehnoloģijās, taču viņi ir arī drosmīgāki, savukārt drosmīgums ne vienmēr ir proporcionāls viņu reālajām zināšanām: “Skolēni ļoti bieži pārvērtē savas spējas vai arī nenovērtē citu zināšanas – gribēšana un varēšana eksperimentēt ir, bet saprašanas par sekām – nav. Tāpēc viņi mēdz eksperimentēt, piemēram, ar datorvīrusu rakstīšanu, kas nav legāli. Kamēr visi eksperimenti paliek joku līmenī, tas ir nekaitīgi, bet, ja kāds mēģina iegūt citas personas datus, zagt naudu un līdzīgi, tad jau var beigties ļoti bēdīgi.”

Būtu jāņem vērā, ka par darbībām, kas skar “Korespondences un pa elektronisko sakaru tīkliem pārraidāmās informācijas noslēpuma pārkāpšanu” un “Nelikumīgas darbības ar fiziskās personas datiem” var draudēt sods ar brīvības atņemšanu uz laiku līdz pat pieciem gadiem, piespiedu darbs vai naudas sods.

Atbilstoši krimināllikumam, situācijā, kad skolēns izmainīja atzīmes, krimināla atbildība tiktu piemērota, ja nodarījums būtu radījis būtisku kaitējumu. Būtiskais kaitējums šajā gadījumā tomēr neesot sasniegts, nav ticis pierādīts kaitniecīgs nodoms un nav konstatēts arī materiālais kaitējums. Taču, ja šī atzīmju labošana būtu radījusi iespēju, piemēram, kādam saņemt palielinātu stipendiju ilgstošākā laika periodā, iespējams, šī finansiālā kaitējuma robeža tiktu sasniegta. Gadījumā, ja skolēna nodoms būtu izlasīt skolotājas vēstules, tad nebūtu svarīgs pat būtiskais kaitējums. Ja kāds ielaužas svešā e-pastā, lasa svešas sarakstes, tad jau tiek pārkāpts korespondences noslēpums, skaidro G.Mālkalnietis.

Katrs pārkāpums tiek izvērtēts individuāli, sekas un sods ir atkarīgs gan no nodarījuma kaitējuma, gan arī personas nodoma. Piemēram, par nelikumīgām darbībām ar fiziskās personas datiem, ja ar to radīts būtisks kaitējums, soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu.

Zināšanai

Izvērstāka informācija par līdzīgām un krimināli sodāmām darbībām, kā arī iespējamām sekām par noteikumu pārkāpšanu un nelikumīgu rīcību lasāma Krimināllikumā:

144.pants. Korespondences un pa elektronisko sakaru tīkliem pārraidāmās informācijas noslēpuma pārkāpšana

145.pants. Nelikumīgas darbības ar fiziskās personas datiem

241.pants. Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai

243.pants. Automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju

244.pants. Nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm

244.1 pants. Datu, programmatūras un iekārtu iegūšana, izgatavošana, izmainīšana, glabāšana un izplatīšana nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām

245.pants. Informācijas sistēmas drošības noteikumu pārkāpšana

Fizisko personu datu aizsardzības likums

Jāņem vērā, ka personas dati ir jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisku personu. Privātuma apdraudējums ir nelikumīga personas datu apstrāde, bet par šo pārkāpumu atbildība norādīta Krimināllikuma 145.pantā.

Ar skolu programmu bērniem māca drošību virtuālajā vidē

Lai jaunākā paaudze būtu izglītota ne tikai viedierīču lietošanā, bet arī prastu droši izmantot tehnoloģijas, Cert.lv nodrošina speciālu skolu programmu. Ja skolā ir interese par bērnu un jauniešu izglītošanu, tad mācību pārstāvis var sazināties ar institūciju, lai tās speciālisti uzstātos ar izglītojošām prezentācijām, kas piemērotas trīs dažādām skolēnu vecuma grupām.

Ar prezentācijām valsts un pašvaldību iestādēm iespējams iepazīties interneta vietnē Cert.lv.

Par drošības pasākumiem virtuālajā vidē gan būtu jāinformē ne tikai skolas solā, bet arī mājās. Cert.lv iesaka katram ģimenes loceklim, kurš izmanto datoru, izveidot savu personīgo piekļuves kontu. Lai mazinātu iespēju bērnam lejuplādēt kaitniecīgas spēles un ļaundari nevarētu datorā uzstādīt pārtveršanas programmas, datora kontiem iespējams aizliegt instalēšanas tiesības. Ja ir iespējams, varbūt vecāki bērnam var piešķirt atsevišķu datoru, kurā nevajadzētu lietot neko, kas ir saistīts ar banku, naudu, kredītkaršu datiem, iepirkumiem internetā, jo grūti izkontrolēt, kas datorā ir parādījies, lejuplādējot dažādas spēles un programmas.

Tāpat bērnam vajadzētu mācīt izmantot pašam savu paroli – arī uz mājas datora. Sākumā tā var būt arī vienkāršāka, īsāka. Lai bērns pierod un saprot, ka arī virtuālajā vidē viņam ir sava privātā telpa, kas nav tā pati, kas ir vecākiem, brāļiem un māsām, un pret kuru jāmācās pienācīgi izturēties.

Ko darīt, ja māc šaubas par nelegālu saturu?

Ja ir aizdomas, ka, piemēram, saņemta vīrusu saturoša e-pasta vēstule un māc šaubas, vai vēstuli vajadzētu atvērt, ikviens var lūgt padomu Cert.lv speciālistiem izvērtēt saņemto saturu. “Mums bieži sūta informāciju, ja ir aizdomas par krāpniecību, par **pikščerēšanas** uzbrukumiem (**pikšķerēšana** jeb t.s. **fišings** (angļu: **phishing**) datorzinātnē ir nelikumīgs veids, kad ar viltu no interneta lietotāja mēģina iegūt slepenu informāciju, piemēram, lietotāju vārdus, paroles, kredītkaršu numurus), lūdz izvērtēt aizdomīgas vēstules vai citas lietas, kas cilvēkiem internetā šķitušas jocīgas. Un pietiekoši bieži, jā, tā ir taisnība, ka tiešām šāds e-pasts satur kādus kaitīgus pielikumus. Cilvēki sāk pievērst lielāku uzmanību kaitīgiem e-pastu pielikumiem, pateicoties jau notikušiem incidentiem,” stāsta G.Mālkalnieks.

Ja skolēns saskaras ar nelegālu interneta saturu, par to būtu vēlams ziņot vecākiem vai zvanīt pa uzticības tālruņa numuru 116111. Tā vienmēr iespējams saņemt atbalstu problēmsituācijās un ziņot par pārkāpumiem interneta vidē. Vecākiem ieteicama arī elektroniskā ziņošanas līnija **Drossinternets.lv**.