LATVIJAS REPUBLIKAS
SATIKSMES MINISTRIJA

drukāt

Aiz cik drošas atslēgas ir Tavi dati?

Mūsdienu cilvēkam ir jāatceras diezgan daudz dažādu paroļu un kodu. Turklāt svarīgi, ka tiešām jāatceras – nevajag šo informāciju pierakstīt uz papīra lapiņas un nēsāt līdz. Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (CERT.LV) eksperti norāda – parolēm jābūt vienkāršam, lai būtu viegli atcerēties, un reizē sarežģītām, lai būtu grūti tās uzminēt.

„Pietiekami daudz ir dzirdēti stāsti par cilvēkiem, kas uzraksta PIN kodu uz bankas kartes vai pielīmē lapiņu ar svarīgām parolēm uz datora ekrāna un „iekrīt". Jūs taču neaizslēdzat mājai durvis un neatstājat vaļā logu?", retoriski jautā CERT.LV Baiba Kaškina.

Kādas paroles nedrīkst izvēlēties?

Protams, viegli uzminamās. Jāņem vērā, ka paroļu uzlaušanai pieejamas daudzas programmas, kuras izstrādājuši pieredzes bagāti un psiholoģiski izglītoti blēži.

Visvieglāk uzminama ir parole ir viens jēgpilns vārds. Tāpēc kāds atsevišķs vārds neder par paroli un turklāt nav tik svarīgi, kādā valodā tas ir. Kādam varbūt zulu vai kečua valodas šķiet ļoti svešas, bet paroļu uzlauzējam var būt šo valodu vārdnīcas un visu šīs valodas vārdu pārbaude aizņems pavisam neilgu laiku. Tāpat paroļu uzlauzējiem ir sagatavoti vārdu krājumi ar saīsinājumiem, pazīstamu personu uzvārdiem, vīriešu, sieviešu un suņu vārdiem, kino varoņiem, ģeogrāfiskiem nosaukumiem u.c. Visi šie vārdi vieni paši par parolēm neder. Daži domā, ka, izvēloties par paroli kādu rupju vārdu, kas nav vārdnīcā, varētu izsaukt paroles uzlauzēja nosarkšanu un ļauno nodomu atmešanu. Pārbaudīs arī šādus vārdus!

Tāpat par parolēm neder šādu vārdu nelielas modifikācijas. Piemēram, ja šiem vārdiem beigās vai sākumā pievienos vienu vai divus burtus vai ciparus („apslacinatqw" vai „rtskaistums"), vai arī uzrakstīs šo vārdu otrādi, sākot no beigām („sjiharbifma" vai „stneirutiba"). Neder arī tāda viltība kā izvēlēties vajadzīgo skaitu burtu no tastatūras pēc kārtas („qwertyu" vai „asdfgh") vai no alfabēta („abcdefgh"). Īsas standartfrāzes arī ir bīstami izvēlēties („kastasir" vai „kurtuesi").

Kādas paroles izvēlēties?

Labai parolei ir jābūt pietiekami garai un izmantoto simbolu kopai pietiekoši plašai. Kā norādījums var kalpot šāda tabula ar laiku, kāds nepieciešams dažāda garuma paroļu atšifrēšanai (no žurnāla „Chip"), izmantojot datoru ar augstas veiktspējas videokarti (ATI Radeon HD 5970).

Simbolu komplekts	Nepieciešamais laiks 6 simbolu paroles uzlaušanai	Nepieciešamais laiks 7 simbolu paroles uzlaušanai
Cipari	9.7 sekundes	97 sekundes
Mazie burti	50 minūtes	22 stundas
Lielie un mazie burti	53 stundas	116 dienas
95 simboli	2 gadi	252 gadi

Parasti dažādas interneta vietnes gan uzreiz pasaka, kāds ir mazākais simbolu skaits parolē, bet, piemēram, lietotāja parole datora operētājsistēmā var būt arī tikai ar vienu burtu. Tas ir par maz. Vajadzētu izvēlēties vismaz sešus simbolus. Labai parolei jāsatur gan lielie, gan mazie burti, gan cipari un vēlams arī kādi pāris papildsimboli, piemēram, tā varētu būt – „r6Su?Q8z%". Lai uzlauztu šādu paroli, vajadzēs krietni daudz laika.

Diemžēl šādu paroli ir grūti atcerēties. Un, ja paroli ir grūti atcerēties, tad ir ļoti liela varbūtība, ka tā tiks uzrakstīta uz papīrīša un tas tiks pielīmēts pie displeja vai nēsāts visur līdzi. Tā darīt nedrīkst! CERT.LV eksperti iesaka dažādas metodes, kā izdomāt pietiekami sarežģītu paroli, kuru varētu atcerēties. Viena no tām ir izmantot dzejoli, kas ir atmiņā, un paņemt pirmos burtus no tā vārdiem. Piemēram, dzejolītis:
Jefiņš kaulu skrubina
Un pie sevis bubina:
Ar tik karstu ēdamo
Izplaucēt var mēdamo.
dos tīri labu paroli: „JksUpsb:Atkelvm." .

Cits piedāvājums: paņemt vārdu no vārdnīcas un pārbīdīt tā burtus pa alfabētu – pirmo uz priekšu otro atpakaļ, trešo uz priekšu utt. Tad vārds „proporcija" dotu „rpposbjib". Šo rezultātu gan vēl vajadzētu padarīt sarežģītāku, piemēram, dažus burtus uzrakstīt kā lielos, teiksim, katru trešo – „rpPosBjiB".

Tīri labi vajadzētu strādāt parolēm „pi-valodā". Kādreiz skolēni diezgan plaši izmantoja šo valodu, lai varētu sazināties tā, lai skolotāji un vecāki nesaprastu. Lai rastos teksts „pi-valodā", pēc katras latviešu valodas zilbes ir jāiesprauž „pi-„,. Piemēram: „Manpi irpi cipigapirepitespi, iepisimpi uzpipīpipētpi". Var, protams, izmantot arī citus burtu savienojumus: „mi-„, „ni-„, „zi-„ utt. .

Vai vienmēr vajadzīgas sarežģītas paroles?

Drīzāk jā, taču patiesībā tomēr ir vietas, kur sarežģīta parole nav vajadzīga un netiek lietota.

Acīmredzamākais piemērs ir bankas kartes personas identifikācijas kods (numurs), kas, protams, arī ir tikai parole – četri cipari un bieži vien divi no šiem cipariem ir vienādi. Pieliekot pūles, dažās dienās šo kodu var atklāt. Taču realitātē jebkura banka pēc trim nesekmīgiem mēģinājumiem karti nobloķē. Ja vien kartes PIN kods nav laipni uzrakstīts kartei otrā pusē, tad ir nepieciešama speciāla iekārta, kas šo kodu nolasa ļoti ātri, tāpēc bankas karte tomēr ir labi jāglabā un uzreiz ir jāziņo par tās nozaudēšanu.

Līdzīgi ir arī ar parolēm internetbankās. Arī tur – daži nesekmīgi mēģinājumi un bankas konts tiek nobloķēts. Tiesa gan, šajā gadījumā tiek prasītas daudz sarežģītākas paroles par četriem cipariem, kaut arī parasti banka nosaka tikai paroles garumu. Tāpat regulāri tiek prasīts nomainīt paroli.

Mūsdienu datoru lietotājam vajag daudz paroļu. Sociālie tīkli, pasta serveri, informācijas vietnes, bankas u.c. Te nu jāsaka, ka ļoti izplatīta nolaidība ir visur lietot vienu un to pašu paroli. Paroles nedrīkst būt vienādas, bet līdzīgas gan tās varētu būt. Piemēram, viena parole veidota ar „pi-valodas" palīdzību, bet cita ar „mu-valodas" palīdzību. CERT.LV eksperti iesaka arī izstrādāt vienu drošu paroli un tad to vienkāršā veidā modificēt, piemēram, pieliekot dažus papildsimbolus.

Kur glabāt paroles?

Visdrošāk tās atcerēties! Bet reālistiski noskaņoti drošības eksperti pieļauj tās vēl arī uzrakstīt uz papīra lapiņas un noglabāt drošā vietā, kur tiek glabāti vissvarīgākie dokumenti (tāda vieta katram cilvēkam kaut kur ir). Nēsāt līdzi šo papīru gan nevajadzētu.

Visi ir pamanījuši, ka daudzi pārlūki un cita programmatūra piedāvājas atcerēties paroli, ar kādu lietotājs slēdzas klāt kādai vietnei. Var arī ļaut to darīt, bet, tā teikt, uz paša atbildību, jo katrs, kas strādā uz šī datora tad varēs pieslēgties šai vietnei.

Paroļu glabāšanai var izmantot arī speciālas programmas – paroļu menedžerus. Viens no daudzajiem ir „KeePass". Šī programma izveido datu bāzi, kurā glabā lietotāja paroles šifrētā veidā un var arī noģenerēt īsti labu paroli. Tā ir brīvi pieejama internetā. Programmu nevajag obligāti instalēt savā datorā, tā var glabāties zibatmiņā kopā ar paroļu datu bāzi, kuru vajadzības gadījumā var iespraust datorā un nolasīt nepieciešamo paroli. Lai varētu piekļūt šim paroļu failam, protams, ir nepieciešama vēl viena ļoti laba parole.

Paroļu izvēle ir nopietns un atbildīgs darbs! To nedrīkst darīt pa roku galam, un tas ir jādara pašam, neaicinot nevienu palīgā.

Baiba Kaškina
CERT.LV vadītāja
Tālrunis: 67085858
E-pasts: *baiba.kaskina@cert.lv*
Mājaslapa: *www.cert.lv*