Ikmēneša informācijas drošības izdevums tev

Digitālais mantojums

Pārskats

Vai esat kādreiz aizdomājušies par tādiem neērtiem jautājumiem, kā, "kas notiek ar mūsu digitālo es, kad mēs nomirstam vai kļūstam rīcībnespējīgi"? Daudziem no mums ir, vai mēs zinām, ka ir nepieciešams testaments un lietu saraksts, kas mūsu tuviniekiem ir jāzina mūsu aiziešanas gadījumā. Bet kā ar mūsu digitālajiem datiem un tiešsaistes kontiem? Vai mums ir jāapsver kāds digitālais testaments? Vai jāizveido "digitālā mantojuma" plāns?

Padomājiet par sevi digitālajā vidē. Bankas un pensiju konti, nekustamā īpašuma kredīts, ģimenes bildes un video, gudrās mājas konti, e-pasts un sociālie tīkli ir tikai daži piemēri no tā, kas veido mūsu digitālo "es". Jūsu vai kāda tuva ģimenes locekļa nāves gadījumā ģimenei un tuviniekiem varētu būt nepieciešama steidzama piekļuve šiem kontiem vai datiem. Papildus tam, bez saimnieka palikuši tiešsaistes konti un dati ar laiku var ciest no hakeru uzbrukumiem, tādējādi pakļaujot ģimenes locekļus un draugus riskam.

Plāna izveidošana

Vēlams ar kādu uzticamu ģimenes locekli vai draugu pārrunāt jūsu vēlmes, tāpat kā jebkurus citus ar jūsu nāvi saistītus aspektus. Papildus jūsu sarunām, izveidojiet sarakstu un dokumentējiet jūsu digitālās dzīves resursus un tiešsaistes kontus. Ja nenodrošināsiet piekļuvi saviem kontiem pēc savas nāves, jūsu ģimenes locekļiem var būt ļoti sarežģīti piekļūt šiem kontiem vai tos aizvērt. Vai jūs, piemēram, vēlētos, lai jūsu ģimenes locekļiem tiek liegta piekļuve visiem šiem video un fotogrāfiju gadiem, kurus esat apkopojis tiešsaistē?

Viens variants ir dokumentēt savu tiešsaistes dzīvi paroļu pārvaldniekā. Tā ir programma, kas droši uzglabā visus jūsu lietotājvārdus un paroles, maksājumu karšu datus un citu sensitīvu informāciju. Tā ir radīta, lai padarītu paroļu un drošības jautājumu veidošanu, uzglabāšanu un izmantošanu daudz vienkāršāku. Šis ir jaudīgs rīks jūsu digitālās dzīves dokumentēšanai dažādos aspektos. Daudzu paroļu pārvaldnieku gadījumā jūs pat varat izvēlēties iestatījumos, vai atklāt jūsu uzticības personām visas vai tikai noteiktas paroles. Ja jums ar to šķiet par maz, tad dokumentējiet piekļuvi savam paroļu pārvaldniekam un ievietojiet šo dokumentu aizzīmogotā aploksnē; nosakiet, ka šo aploksni atver pēc jūsu nāves testamenta

izpildītājs vai uzticams ģimenes loceklis. Tādējādi viņiem būs piekļuve jūsu paroļu pārvaldniekam, un viņi varēs piekļūt jūsu tiešsaistes kontiem un informācijai, kas tajos uzglabāta.

Dažas vietnes piedāvā iespēju norādīt arī pārņēmēja vai uzticības personas kontaktinformāciju. Piemēram, Facebook sniedz dalībniekiem iespēju jau iepriekš noteikt, vai viņi vēlas savu kontu dzēst vai padarīt par piemiņas vietu. Piemiņas vietas gadījumā tiek izveidota sadaļa, kas redzama tikai esošajiem draugiem, lai varētu dalīties ar atmiņām. Visbeidzot, jūs varat apsvērt iespēju piesaistīt juristu vai īpašumu pārvaldnieku, kas specializējas digitālajā mantojumā.

Digitālo īpašumu mantošana

Jūs varat nonākt situācijā, kurā jums jāatjauno vai jāiegūst piekļuve nesen aizgājuša drauga vai ģimenes locekļa tiešsaistes kontiem. Mēs iesakām jums vispirms sazināties ar juristu un citiem ģimenes locekļiem, pirms uzsākt kādas darbības. Citi ģimenes locekļi var tapt aizvainoti, ja redzēs, ka uzsākat darbības bez viņu ziņas. Tad sāciet ar to, ka identificējiet paroles, kuras varat atrast. Vai ģimenes loceklis tās pierakstīja vai kaut kur uzglabāja? Ja šāda varianta nav, varbūt varat piekļūt datoram vai mobilajai iekārtai, kuru ģimenes loceklis izmantoja un kurā ir joprojām pierakstījies? Ja nē, tad jums visdrīzāk nāksies sazināties ar katru tīmekļa vietni atsevišķi, lai iegūtu piekļuvi mirušā ģimenes locekļa kontam. Tas bieži vien nozīmē miršanas apliecības uzrādīšanu un pierādīšanu, ka esat pirmās pakāpes radinieks. Dažos gadījumos jums nebūs iespējas piekļūt kontam vai tajā uzglabātajiem datiem, bet tikai tos izdzēst. Katra tīmekļa vietne šādas situācijas apstrādā atšķirīgi, kas var izvērsties par laikietilpīgu procesu.

Šodienas digitālajā pasaulē mantojuma gatavošanā mums jāņem vērā ne tikai fiziskie, bet arī digitālie īpašumi.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Viesredaktors

Cheryl Conley *ir pikšķerēšanas un informācijas drošības jautājumu eksperte, kuras pieredze ietver arī atbalsta sniegšanu pikšķerēšanas programmas izveidē un uzturēšanā kompānijā "Lockheed Martin". Šobrīd viņa sniedz atbalstu SANS informācijas drošības komandai un ir saņēmusi SSAP (SANS Security Awareness Professional) sertifikātu.*

Resursi

Paroļu pārvaldnieki: http://www.sans.org/u/Y5Y

Kā padarīt paroles vieglāk iegaumējamas: http://www.sans.org/u/Y63

OUCH! izdod SANS institūts programmas "Security Awareness" ietvaros un tas tiek izplatīts saskaņā ar Creative Commons BY-NC-ND 4.0 licences nosacījumiem. *Jūs varat izplatīt šo biļetenu vai izmantot to savā informācijas tehnoloģiju drošības izglītošanas programmā ar nosacījumu, ka biļetens netiek izmainīts Papildu informācijai vai jautājumiem par tulkošanu izmantojiet* www.sans.org/security-awareness/ouch-newsletter e-pasta adresi.
Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: CERT.LV