OUCH! | 2016.gada janvāris

Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …


- Planšetdatora drošības pamati
- Drošība ikdienā


# Jūsu jaunā planšetdatora drošība

## Pārskats

Apsveicam Jūs ar jauno planšetdatoru! Tas ir ērts un jaudīgs veids lai sazinātos ar citiem, iepirktos tiešsaistē, skatītos filmas, spēlētu spēles un pievērstos vēl daudz un dažādām aktivitātēm. Planšetdators visdrīzāk kļūs par svarīgu Jūsu dzīves daļu, iespējams, pat aizstājot datoru. Šeit ir daži ieteikumi, ko Jums būtu jāņem vērā, ja vēlaties saglabāt savu planšetdatoru un tajā esošo informāciju drošībā.

## Viesredaktors

Lori Rosenberg ir plaša pieredze, sagatavojot Informācijas drošības izglītības materiālus un apmācības darbiniekiem un klientiem, un viņa vienmēr meklē jaunas un iesaistošas metodes šo zināšanu izplatīšanai. Jūs varat atrast viņu Twitter kā **@InfoSecLori**.

## Planšetdatora drošības pamati

Varbūt Jūs būsiet pārsteigts, bet lielākais risks Jūsu planšetdatoram nav hakeri, tas visdrīzāk esat Jūs pats. Daudz lielāka iespējamība ir ka Jūs pazaudēsiet vai Jums to nozags, nekā kāds to uzlauzīs. Pirmā lieta ir aizsargāt savu planšetdatoru ar automātisku ekrāna bloķēšanu. Tas nozīmē - katru reizi, kad Jūs vēlaties lietot planšetdatoru, Jums tas jāatbloķē ar stipru paroli, švīkošanas rakstu vai pirkstu nospiedumu. Tas nodrošina, ka ja Jūsu planšetdators tiek pazaudēts vai nozagts, piekļūšana tam ir apgrūtināta un Jūsu personiskā informācija, mobilās aplikācijas un visa cita veida informācija planšetdatorā ir aizsargāta. Pēc tam kad esat ieslēdzis automātisku bloķēšanu, vēl dažas papildus lietas planšetdatora aizsardzībai:

1. Uzstādiet programmatūru, kas var attālināti izsekot planšetdatoru, izmantojot Internetu. Pazaudēšanas vai zādzības gadījumā Jums būs iespēja pieslēgties planšetdatoram un noteikt tā atrašanās vietu, vai sliktākajā gadījumā, vismaz attālināti izdzēst visu tajā esošo informāciju.
2. Atjauniniet savu planšetdatoru un uzstādiet automātisku atjauninājumu instalēšanu, lai tam vienmēr būtu jaunākā operētājsistēmas versija. Uzbrucēji vienmēr meklē jaunas programmatūras ievainojamības un ražotāji attiecīgi izlaiž jaunus atjauninājumus un labojumus, lai novērstu šīs ievainojamības. Ja Jums ir jaunākā operētājsistēmas versija un atjauninātas aplikācijas, Jūsu planšetdatoru uzlauzt ir daudz sarežģītāk.

## Jūsu jaunā planšetdatora drošība

3. Sākumā konfigurējot planšetdatoru, īpašu uzmanību pievērsiet privātuma iestatījumiem. Viena no lielākām privātuma problēmām ir tā, ka Jūsu planšetdators dod iespēju citiem uzzināt Jūsu atrašanās vietu. Iesakām sākumā atslēgt atrašanās vietas sekošanas iestatījumu visam, tad atļaut tikai tām aplikācijām, kam tas Jūsuprāt noteikti nepieciešams, piemēram, karšu programmatūrai, vai lai atrastu tuvāko restorānu, bet vairumam Jūsu aplikāciju nav nepieciešama realā laika atrašanās vietas informācija.
4. Vairums planšetdatoru un aplikāciju saglabā Jūsu informāciju mākonī. Jums vajadzētu saprast, kur Jūsu dati atrodas un kā tie ir aizsargāti. Piemēram, Jūs visdrīzāk nevēlaties savu privāto fotoattēlu publicēšanu internetā, kur tos var apskatīt visa pasaule, kopā ar tajos iekļautu atrašanās vietas informāciju. Sākumā atslēdzat jebkādas informācijas augšupielādēšanu mākonī, tad iespējojat to tikai tad ja tiešām vēlaties publiskot kaut ko specifisku.

*labākais veids kā padarīt Jūsu planšetdatoru drošāku ir ieslēgt ekrāna bloķēšanu, pārskatīt privātuma iestatījumus un regulāri atjaunināt planšetdatora programmatūru.*

5. Planšetdatori sinhronizē Jūsu aplikācijas ar citām iekārtām - portatīvajiem datoriem, viedtālruņiem. Sinhronizācija var būt ļoti noderīga, taču esat piesardzīgi atļaujot sinhronizāciju dažādām aplikācijām. Ja sinhronizācija ir ieslēgta, neesat pārsteigts, ja mājas lapas ko Jūs apmeklējāt Jūsu planšetdatorā, pēkšņi parādās Jūsu darba datora interneta pārlūkā.

## Drošība ikdienā

Kad Jūs esat padarījis savu planšetdatoru drošāku, Jūs noteikti gribēsiet arī lai tas tāds paliek. Šeit ir daži ieteikumi planšetdatora ilgstošas drošības nodrošināšanai:

- Nekad nemēģiniet to uzlauzt. Tas apiet un padara par nelietojamām daudzas drošības kontroles un padara Jūsu planšetdatoru daudz ievainojamāku.
- Lejupielādējat aplikācijas tikai tad, ja tās Jums tiešām nepieciešamas un tikai no uzticamiem avotiem. IPad - izmatojat tikai iTunes veikalu. Šajā veikalā atrodamās aplikācijas Apple pārbauda, pirms tās tiek publicētas. Google programmnodrošinājumam iesakām izmantot Google Play veikalu un Amazon planšetdatoriem Amazon App Store. Jūs varat lejupielādēt aplikācijas arī no citām vietnēm, tomēr tās visbiežāk nav pārbaudītas un var būt

## Jūsu jaunā planšetdatora drošība

inficētas. Visbeidzot, neatkarīgi no tā, kur aplikācija iegūta, ja tā Jums vairs nav vajadzīga vai Jūs to aktīvi nelietojat - izdzēsiet to no planšetdatora.

- Instalējot jaunu aplikāciju, pārskatiet un uzstādiet privātuma nosacījumus, tieši tāpat kā Jūs to darījāt sākotnēji konfigurējot planšetdatoru. Esat piesardzīgi, atļaujot aplikācijām piekļuvi. Piemēram, vai tiešām aplikācijai ko Jūs tik tikko lejupielādējat ir nepieciešama piekļuve visiem Jūsu draugiem un kontaktinformācijai. Ja aplikācijas pieprasītās atļaujas Jums nav pieejamas atrodiet citu, kas atbilst Jūsu prasībām. Papildus regulāri pārbaudiet atļaujas, lai pārliecinātos vai nav notikušas izmaiņas.

Jūsu planšetdators ir jaudīgs instruments, ko Jūs vēlaties izmantot bez problēmām. Atceroties šos vienkāršos principus Jūs varat padarīt sevi un savu jauno planšetdatoru daudz drošāku.

## UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni http://www.securingthehuman.org.

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.

## Resursi

| | |
|---|---|
| Mobilo aplikāciju droša izmantošana: | https://www.securingthehuman.org/ouch/2015#january2015 |
| Paroles: | https://www.securingthehuman.org/ouch/2015#april2015 |
| Mākoņa droša izmantošana: | https://www.securingthehuman.org/ouch/2014#september2014 |
| Atbrīvošanās no Jūsu mobilās iekārtas: | https://www.securingthehuman.org/ouch/2014#june2014 |
| SANS dienas drošības ieteikums: | https://www.sans.org/tip_of_the_day.php |

## License



Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Tulkojums: Edgars Tauriņš