OUCH! | 2017.gada oktobris

Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

Palīdzēt citiem būt drošībā

Pārskats

Daudzi no mums jūtas komfortabli, izmantojot tehnoloģijas un darot to droši. Taču citi draugi vai ģimenes locekļi var nebūt tik pārliecināti. Patiesībā tie var būt pat apjukuši vai nobijušies no tehnoloģijām. Tas var padarīt viņus par kibernoziedznieku upuriem. Taču kiberdrošībai nav jābūt biedējošai, patiesībā tā ir diezgan vienkārša, līdzko ir skaidras pamata lietas. Viņiem vienkārši vajag palīdzēt saprast šos pamatus.

Viesredaktors

Randy Marchany (Twitter: **@randymarchany**) ir Virginia Tech CISO (informācijas drošības vadītājs) un sertificēts SANS institūta pasniedzējs.

Pieci soļi

Šeit ir pieci vienkārši soļi, kā jūs varat citiem palīdzēt pārvarēt bailes un pilnvērtīgi izmantot mūsdienu tehnoloģiju iespējas. Ja gribat zināt vairāk par katru no šiem soļiem, skatieties šī izdevuma atsauču sadaļā.

1. **Sociālā inženierija**: Sociālā inženierija ir plaši izplatīts kiberuzbrukumu paņēmiens, kas apmāna cilvēkus, lai tie izdarītu to, ko viņiem nevajadzētu darīt, piemēram, atklātu savas paroles, inficētu datoru vai atklātu sensitīvu informāciju. Tas nav nekas jauns, krāpnieki ir eksistējuši jau tūkstošiem gadu. Vienīgā atšķirība - tagad ļaundari, šos pašus paņēmienus izmanto internetā. Jūs varat palīdzēt citiem, paskaidrojot viņiem visizplatītākās sociālās inženierijas uzbrukuma pazīmes, piemēram, ja kāds rada milzīgu steidzamības sajūtu, kad kaut kas ir pārāk labs, lai būtu patiesība, vai ja kiberuzbrucējs izliekas par kādu, ko jūs zināt, taču īsti neizklausās pēc tā. Pieminiet šādu uzbrukumu piemērus, piemēram, pikšķerēšanas e-pastus vai neīstos Microsoft tehniskā atbalsta tālruņa zvanus. Kā minimums, pārliecinieties, ka ģimenes locekļi saprot, ka nedrīkst nevienam atklāt savu paroli vai sniegt attālinātu piekļuvi savam datoram.
2. **Paroles**: Drošas paroles ir pamats iekārtu un tiešsaistes kontu aizsardzībai. Palīdziet ģimenes locekļiem saprast, kā izveidot drošu paroli. Mēs iesakām paroļu frāzes, jo tās ir vieglāk gan uzrakstīt, gan atcerēties. Paroļu frāzes nav nekas cits kā paroles, kas izveidotas no vairākiem vārdiem. Papildus palīdziet viņiem uzstādīt paroļu pārvaldnieku. Svarīgi ir izveidot unikālu paroli katrai ierīcei un katram kontam. Ja paroļu pārvaldnieks ir par sarežģītu, varbūt

Palīdzēt citiem būt drošībā

iemāciet pierakstīt paroles un saglabāt tās drošā vietā. Visbeidzot, svarīgiem kontiem palīdziet uzstādīt divu pakāpju verifikāciju (bieži sauktu arī par divu faktoru autentifikāciju). Divu pakāpju verifikācija ir viena no efektīvākajām kontu aizsardzības metodēm.

3. **Atjauninājumi**: Sistēmu uzturēšana aktuālā stāvoklī ir svarīgs ierīču aizsardzības pasākums. Tas attiecināms ne tikai uz datoriem un mobilajām ierīcēm, bet arī uz jebko, kas ir pieslēgts internetam, piemēram, spēļu konsoles, termometri vai pat gaismekļi un skaļruņi. Vienkāršākais veids ir pieslēgt automātisku atjauninājumu uzstādīšanu, kad iespējams.
4. **Antivīruss**: Cilvēki pieļauj kļūdas, dažkārt mēs uzklikšķinām vai instalējam kaut ko, ko droši vien nevajadzētu, kas var inficēt mūsu sistēmas. Antivīrusa programmas ir paredzētas, lai aizsargātu mūs no šādām kļūdām. Tās nevar apturēt katru ļaunatūru, taču palīdz aizsargāties pret izplatītākajiem uzbrukumiem. Tādēļ uzstādiet antivīrusu katram mājas datoram un nodrošiniet, ka tas ir aktuāls un aktīvs. Papildus daudzi mūsdienu risinājumi ietver arī citus drošības risinājumus kā ugunssienas vai pārlūka aizsardzību.
5. **Rezerves kopijas**: Kad viss pārējais nav nostrādājis, bieži vienīgais veids, kā atgūties no kļūdām (piemēram, nepareizo failu izdzēšana vai izspiedējvīrusa uzbrukums) ir rezerves kopijas. Pārliecinieties, ka jūsu draugiem un ģimenes locekļiem ir uzstādīts automātisks rezerves kopiju veidošanas risinājums. Bieži vienkāršākie risinājumi ir t.s. mākoņpakalpojumi, kas veido rezerves kopijas katru stundu vai pēc failu izmaiņām. Tādi risinājumi atvieglo ne tikai rezerves kopiju izveidi, bet arī failu atjaunošanu.

Izmantojiet piecus vienkāršus soļus, lai palīdzētu citiem pilnvērtīgi izmantot tehnoloģijas, darot to droši.

Bērnu drošība viesojoties

Ja jūs esat pietiekoši zinoši tehnoloģiju jomā, jūs noteikti aizsargājiet ne tikai sevi, bet arī savus bērnus. Tomēr, kad bērni viesojas pie radiem, kas nav tik zinoši attiecībā uz tehnoloģijām, piemēram, vecvecākiem, šie draugi vai ģimenes locekļi var nezināt, kā aizsargāt bērnus tiešsaistē. Šeit ir daži pasākumi, kas ļauj bērniem būt drošībā, kad tie viesojas pie citiem, īpaši ģimenes locekļiem.

- **Likumi**. Pārliecināties, ka citi zina par likumiem vai to, ko jūs sagaidāt no bērnu tiešsaistes drošības. Piemēram,

Palīdzēt citiem būt drošībā

vai ir skaidri nosacījumi, cik laika bērns var pavadīt tiešsaistē vai kādas spēles var spēlēt, vai ar ko var sazināties. Bērni paši droši vien nevēlēsies šos nosacījumus izskaidrot. Mūsu priekšlikums ir izveidot likumu grāmatu, ko izdalīt visiem, pie kā bērni regulāri ciemojas.

- **Kontrole**: Ja bērns saprot tehnoloģijas labāk nekā viņa pieskatītājs, viņš var to izmantot. Piemēram, var iegūt administratora tiesības vecvecāku datorā un tad darīt visu, ko vien vēlas, piemēram, instalēt spēles, ko jūs nevēlaties, lai viņš spēlētu. Pārliecinieties, ka radi saprot to, ka nedrīkst bērniem dot vairāk tiesību piekļūt datoram, kā iepriekš noteikts.

Visbeidzot, iesakiet cilvēkiem abonēt resursus, kā piemēram OUCH! Izdevumu, kur viņi var izglītoties tālāk. Šis izdevums katru mēnesi tiek izdots vairāk kā 20 valodās. Abonējiet to https://securingthehuman.sans.org/ouch.

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 securingthehuman.sans.org/ouch/archives.

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

Sociālā inženierija:	https://securingthehuman.sans.org/ouch/2017#january2017
Paroļu frāzes:	https://securingthehuman.sans.org/ouch/2017#april2017
Paroļu pārvaldnieks:	https://securingthehuman.sans.org/ouch/2017#september2017
Divu pakāpju verifikācija:	https://securingthehuman.sans.org/ouch/2015#september2015
Rezerves kopijas un atjaunošana:	https://securingthehuman.sans.org/ouch/2017#august2017
Šodienas tiešsaistes bērnu drošība:	https://securingthehuman.sans.org/ouch/2017#may2017

License

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Tulkojums: Edgars Tauriņš