OUCH! 2020. gada

SANS SECURITY AWARENESS

Nodrošinot saikni starp paaudzēm

Pārskats

Cenšanās droši izmantot mūsdienu tehnoloģijas var būt liels izaicinājums gandrīz visiem, bet tas var būt īpaši grūti ģimenes locekļiem, kuri nav pieraduši pie tehnoloģijām vai tās tik labi nepārzina. Tāpēc vēlējāmies dalīties informācijā par dažiem būtiskākajiem jautājumiem, lai palīdzētu aizsargāt ģimenes locekļus, kuriem, iespējams, ir grūti darboties ar tehnoloģijām un kuri nepietiekami novērtē ar to izmantošanu saistītos riskus.

Koncentrējieties uz pamatlietām

Bieži vien labākais veids, kā palīdzēt aizsargāt citus, ir padarīt drošību pēc iespējas vienkāršāku. Koncentrējieties uz mazāku skaitu darbību ar vislielāko ietekmi.

1. **Sociālā inženierija:** Uzbrukumi, izmantojot sociālo inženieriju, ir viens no galvenajiem veidiem, kā mums mēģina piekļūt. Izskaidrojiet, ka krāpnieki un blēži ir darbojušies tūkstošiem gadu un vienīgā atšķirība, ka tagad sliktie apmuļķošanai izmanto internetu. Miniet tādus piemērus kā krāpniecību ar e-pasta vēstulēm, izliekoties par jūsu banku vai sūtījumu piegādātāju, vai krāpniekus, kuri uzdodas par tehnisko dienestu vai valdības pārstāvjiem. Pārliecinieties, ka ģimenes locekļi saprot, ka nekad un nevienam nedrīkst dot savu paroli, kredītkartes, personīgo informāciju vai piekļuvi savam datoram. Atgādiniet viņiem: jo steidzamāka un uzstājīgāka ir ziņa, jo lielāka ir iespējamība, ka tas ir uzbrukums. Daži noziedznieki manipulēs ar mūsu tuviniekiem, kuri ilgojas pēc mīlestības, un izliksies, ka piepildīs viņu sapņus. Pārlieciniet viņus: ja viņiem rodas neērtības sajūta vai jautājumi par e-pastu vai zvanītāju, visdrošāk ir vispirms sazināties ar jums.
2. **Mājas bezvadu (Wi-Fi) tīkls:** Veltiet laiku, lai pārbaudītu, vai jūsu mājas bezvadu tīkls ir aizsargāts ar paroli un vai administratora noklusējuma parole ir nomainīta ar citu. Varat arī apsvērt iespēju konfigurēt bezvadu tīklu tā, lai izmantotu drošu domēna vārdu sistēmu (DNS – Domain Name System), piemēram, bezmaksas https://www.opendns.com. Drošie DNS pakalpojumi ne tikai pasargā no inficētu vietņu apmeklēšanas, bet var arī nodrošināt kontroli pār vietnēm, kurām interneta lietotāji var vai nevar piekļūt, kas var būt īpaši vērtīgi, ja mājās ir bērni.

3. **Atjaunināšana:** Īpaši uzsveriet, ka sistēmu, programmatūras un ierīču atjaunināšana uz jaunāko versiju apgrūtina noziedznieku darbības. Vienkāršākais veids, kā to nodrošināt, ir automātiskas atjaunināšanas iespējošana, kad vien tas ir iespējams. Ja ierīce vai sistēma ir pārāk veca, lai to varētu atjaunināt, ir ieteicams aizstāt to ar jaunu ierīci, kas atbalsta atjaunināšanu.
4. **Paroles:** Stipras un drošas paroles ir galvenais gan ierīces, gan jebkura tiešsaistes konta aizsardzības līdzeklis. Iemāciet saviem ģimenes locekļiem veidot garas paroļu frāzes. Šādas frāžveidīgas paroles viņiem būs vieglāk iegaumēt un lietot. Cita iespēja ir uzstādīt paroļu pārvaldnieku un iemācīt, kā to izmantot. Tādā veidā jūsu mīļie var viegli un droši izmantot internetu: ir tikai jāatceras viena parole, lai atslēgtu paroļu glabātavu. Atkarībā no risinājuma, iespējams, pat spējat to pārraudzīt attālināti. Ja tas neizdodas, varat lūgt viņiem pierakstīt savas paroles piezīmju grāmatiņā un pēc tam glabāt to ērtā un drošā vietā. Vissvarīgākajiem tiešsaistes kontiem, piemēram, finanšu kontiem, iespējams, vēlēsieties iestatīt divpakāpju pārbaudi (verifikāciju). Noteikti izveidojiet mantošanas plānu visiem tiešsaistes kontiem tādā pašā veidā, kā gatavojat testamentu fiziskajiem īpašumiem.
5. **Rezerves kopijas:** Kad nekas cits vairs nepalīdz, glābiņš būs rezerves kopijas. Parūpējieties, lai ģimenes locekļiem būtu vienkāršs, uzticams rezerves kopiju veidošanas risinājums. Daudziem lietotājiem datu glabāšana virtuālajā mākonī būs visvienkāršākais risinājums.

Ja jūsu ģimenes locekļiem tas viss šķiet pārāk sarežģīti un nomācoši, palīdziet viņiem, koncentrējoties uz pamatlietām, tādējādi padarot drošību pēc iespējas vienkāršāku. Esiet pacietīgs, veltiet laiku izskaidrošanai, ļaujiet tuviniekiem kļūdīties un palīdziet viņiem neatkārtot pieļautās kļūdas. Visbeidzot, apdomājiet, vai viņiem nevajadzētu abonēt OUCH! informatīvo izdevumu.

Viesredaktors

Kriss Deils (Chris Dale) (Twitter @chrisadale) ir Eiropas drošības konsultāciju uzņēmuma River Security galvenais konsultants un sertificēts SANS instruktors (https://www.sans.org/profiles/chris-dale/).
Atrodiet Krisu vietnē LinkedIn: https://www.linkedin.com/in/chrisad/

Resursi

Sociālā inženierija: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Paroļu pārvaldnieki: https://www.sans.org/security-awareness-training/resources/password-managers-0
Atjaunināšana: https://www.sans.org/security-awareness-training/resources/power-updating
Rezerves kopijas: https://www.sans.org/security-awareness-training/resources/got-backups
Digitālais mantojums: https://www.sans.org/security-awareness-training/resources/digital-inheritance

Tulkojums: CERT.LV