Ikmēneša informācijas drošības izdevums tev

Pārlūkprogrammas

Pārskats

Pārlūkprogrammas, kā Google Chrome, Microsoft Edge, Apple Safari vai Mozilla Firefox, ir viens no izplatītākajiem veidiem, kā cilvēki mijiedarbojas ar internetu. Tos izmanto, lai lasītu ziņas, apskatītu e-pastu, iepirktos tiešsaistē, skatītos videoklipus un spēlētu spēles. Tāpēc arī pārlūkprogrammas ir kiberuzbrucēju mērķis.
Daudzi uzskata, ka pārlūkošana tiešsaistē ir droša, ja apmeklējat tikai labi zināmas un uzticamas vietnes. Tomēr ir diezgan viegli nejauši noklikšķināt uz nedrošas tīmekļa lapas vai to apmeklēt, dažkārt pat nezinot par to. Turklāt var tikt uzlauztas arī tīmekļa vietnes, kuras zināt un kurām uzticaties, un kiberuzbrucēji tajās var instalēt ļaunprātīgu programmatūru. Visbeidzot, mūsdienu pārlūkprogrammās ir daudz jaunu funkciju, kas bieži var būt mulsinošas un nepareizas konfigurācijas gadījumā var radīt vēl lielākus draudus.

Droša pārlūkprogrammas izmantošana

Lūk, galvenie soļi, kā būt pasargātam:

Atjaunināšana: Vienmēr izmantojiet jaunāko pārlūkprogrammas versiju. Atjauninātajās pārlūkprogrammās ir jaunākie drošības labojumi, un tās ir daudz drošākas. Mūsdienu datoros atjaunināšana ir kļuvusi daudz vienkāršāka, jo iespējams ieslēgt automātisko atjaunināšanu savā sistēmā. Dažās pārlūkprogrammās vienkārši "restartējiet" pārlūkprogrammu, tiklīdz saņemat paziņojumu, ka ir pieejams atjauninājums. Pēc atjaunināšanas pārbaudiet, vai ir pieejamas jaunas drošības funkcijas, kas var jums nākt par labu.

Brīdinājumi: Mūsdienu pārlūkprogrammas bieži spēj atpazīt konkrētas ļaunprātīgas vietnes, kuru mērķis ir nodarīt jums kaitējumu. Ja pārlūkprogramma brīdina, ka tīmekļa vietne, kuru gatavojaties apmeklēt, ir bīstama, aizveriet pārlūkprogrammas cilni un meklējiet nepieciešamo citā tīmekļa vietnē.

Sinhronizēšana: Nekad nesinhronizējiet darba pārlūkprogrammu ar personīgo pārlūkprogrammu vai personīgajiem kontiem. Sinhronizēšana notiek tad, kad dažādās ierīcēs esošajām pārlūkprogrammām tiek dota iespēja savstarpēji apmainīt informāciju un kopīgot pārlūkošanas informāciju, piemēram, pārlūkošanas vēsturi, grāmatzīmes un saglabāto saturu.

Paroles: Daudzās pārlūkprogrammās ir iespēja saglabāt paroles dažādām vietnēm. Tā vietā, lai paroles glabātu pārlūkprogrammā, iesakām izmantot īpašu paroļu pārvaldnieku. Paroļu pārvaldnieki ir atsevišķa drošības programma, kurai ir daudz vairāk drošības funkciju un funkcionalitātes.

Spraudņi: Spraudņi jeb paplašinājumi ir pārlūkprogrammām pievienotas nelielas programmatūras daļas, kas var pievienot papildu funkcijas. Tomēr katrs pievienotais spraudnis var arī palielināt ievainojamību. Darba datorā pievienojiet tikai autorizētus un apstiprinātus spraudņus un, tāpat kā pārlūkprogrammā, regulāri tos atjauniniet. Noņemiet spraudņus, kas jums vairs nav nepieciešami vai kurus vairs neizmantojat.

Privātuma režīms: Lielākā daļa pārlūkprogrammu piedāvā privātuma opciju (sauktu arī par "inkognito režīmu"). Tas nozīmē, ka, atverot pārlūkprogrammas cilni privātuma režīmā, jūs ierobežojat to, kāda informācija par jums tiek apkopota. Piemēram, jūsu pārlūkprogramma neuzkrāj sīkdatnes, neizseko pārlūkošanas vēsturi, kā arī neuzkrāj un neizplata sensitīvu informāciju par jums.

Tiešsaistes tērzēšana: Dažās vietnēs nu ir pieejama tērzēšanas funkcija, lai uzdotu jautājumus. Tiešsaistes tērzēšanā iesaistieties tikai zināmās, uzticamās vietnēs. Turklāt ierobežojiet informāciju, ko sniedzat tiešraides tērzēšanas sesijas laikā, jo jums nav ne jausmas, kas vāc jūsu informāciju, ko ar to dara un kam to var pārdot vai nodot.

Uzmanieties no tālvadības: Krāpnieciskās vietnes var mēģināt uzlauzt jūsu datoru, izsūtot viltus drošības uznirstošo logu ar brīdinājumu pārlūkprogrammā, ka jūsu dators ir inficēts, un aicinot jūs piedalīties tiešsaistes tērzēšanas sesijā, lai salabotu jūsu datoru. Pēc tam ļaundari steidzami lūdz atļaut instalēt attālinātās darbības rīku, lai varētu salabot jūsu datoru. Patiesībā ar datoru viss ir kārtībā. Viņi vienkārši mēģina jūs pierunāt instalēt ļaunprātīgu programmatūru, lai varētu nozagt jūsu paroles un datus, kā arī izsekot visas jūsu darbības tiešsaistē.

Atslēdzieties no kontiem: Kad esat beidzis tīmekļa vietnes apmeklējumu, pirms pārlūkprogrammas aizvēršanas noteikti atslēdzieties no konta, lai dzēstu pieteikumvārdu un paroles informāciju.

Viesredaktors

Dīns Pārsonss (Dean Parsons) ir "ICS Defense Force" izpilddirektors, kuram ir vairāk nekā 20 gadu pieredze IT/ICS kiberaizsardzībā. Viņš ir arī sertificēts "SANS" ICS515 instruktors un ICS418 līdzautors / instruktors, kas māca aktīvu kiberaizsardzību, reaģēšanu uz incidentiem, vadību un riska pārvaldību rūpniecisko vadības sistēmu jomā. www.linkedin.com/in/dean-parsons-cybersecurity.

Resursi

Paroļu pārvaldnieki: https://www.sans.org/newsletters/ouch/password-managers/
Atjaunināšana: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Sociālā inženierija: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Savas "digitālās pēdas" aizsardzība: https://www.sans.org/newsletters/ouch/privacy/

Tulkojums: CERT.LV