Publicația dumneavoastră lunară de sensibilizare asupra securității informatice

Patru pași simpli pentru a rămâne în siguranță

Prezentare generală

A profita cât se poate de tehnologie în condiții de siguranță poate părea copleșitor și confuz. Cu toate acestea, indiferent de ce tehnologie folosiți sau modul cum o folosiți, veți găsi mai jos patru pași simpli, care vă vor ajuta să rămâneți în siguranță.

1. Dumneavoastră: În primul rând, tehnologia singură nu vă poate proteja pe deplin, dvs. sunteți cea mai bună apărare. Atacatorii au învățat că cel mai simplu mod de a obține ceea ce doresc este să vă țintească pe dvs., mai degrabă decât computerul sau alte dispozitive. În cazul în care vă doresc parola, cardul de credit sau să vă controleze computerul, ei vor încerca să vă păcălească să le dați, de cele mai multe ori prin crearea unei iluzii de urgență. De exemplu, vă pot contacta pretinzând a fi reprezentanți tehnici de la Microsoft și spunând că aveti computerul infectat, când de fapt sunt criminali cibernetici care vor accesul la computer. Sau vă trimit un e-mail informându-vă că un anumit pachet nu a putut fi livrat și indicându-vă să faceți clic pe un link pentru confirmarea adresei, când, în realitate, vă trimit la un site web dăunator care vă va infecta computerul. În concluzie, cea mai buna apărare împotriva atacatorilor sunteți dvs. Cu puțină prudență puteți detecta și opri multe atacuri.

2. Frazele de acces: Vitezele moderne de calcul au făcut vechea parolă de 8 caractere învechită și vulnerabilă. Când un site vă solicită să creați o parolă, creați mai degraba o frază de acces puternică și unică. O frază de acces este un tip de parolă care utilizează o serie de cuvinte ușor de amintit, cum ar fi „albina miere cognac ploaie”. Cu cât este mai lungă fraza de acces, cu atât este mai puternică. O frază de acces unică înseamnă utilizarea uneia diferite pentru fiecare dispozitiv sau cont online. În acest fel, dacă o frază de acces este compromisă, toate celelalte conturi și dispozitive rămân în continuare protejate. Nu vă puteți aminti toate aceste fraze de acces? Utilizați un manager de parole, care este un program specializat ce stochează în siguranță toate frazele într-un format criptat (plus o mulțime de alte caracteristici).

În cele din urmă, activați verificarea în doi pași (denumită și autentificare cu doi factori sau multi-factor). Aceasta utilizează o parolă, dar adaugă și un al doilea pas, cum ar fi un cod trimis pe telefon sau o aplicație care

generează codul pentru dvs. Verificarea în doi pași este probabil cel mai important pas pe care îl puteți face pentru a vă proteja conturile online și este mult mai ușor decât ați putea crede.

3. Actualizarea: Asigurați-vă că fiecare dintre computerele, dispozitivele mobile, programele și aplicațiile dvs. rulează cea mai recentă versiune de software. Atacatorii cibernetici caută în mod constant noi vulnerabilități în software-uri. Atunci când le descoperă, folosesc programe speciale pentru a le exploata și a va pirata dispozitivele. Între timp, companiile care au creat software-urile muncesc din greu pentru a le repara, lansând noi actualizări. Piratarea dispozitivelor dvs. devine mult mai grea dacă vă instalați prompt aceste actualizari de software. Pentru a fi mereu la curent, activați actualizarea automată oricând este posibil. Această regulă se aplică aproape oricărei tehnologii conectate la o rețea, inclusiv TV conectat la internet, monitoare pentru copii, camere de securitate, rutere de domiciliu, console de jocuri sau chiar mașină.

4. Backupurile si Recuperarea: Uneori, indiferent cât de atent sunteți, puteți fi atacat. În astfel de cazuri, deseori singura modalitate de a vă restabili toate informațiile personale sunt copiile de rezervă (backup-urile). Efectuați în mod regulat, copii de rezervă ale informațiilor importante și verificați dacă aveți posibilitatea să restaurați datele pornind de la aceste copii. Majoritatea sistemelor de operare și dispozitivelor mobile oferă opțiunea de backup automat, fie pe hard-discuri externe, fie in cloud.

Versiunea în limba română

Ubisoft este o companie de jocuri. Un creator de lumi, dedicat îmbogățirii vieților jucătorilor cu experiențe de joc originale și memorabile. Aflați mai multe la: https://www.ubisoft.com/en-us/.

Editor invitat

***Steve Anson**, instructor certificat SANS, oferă consultantă pentru echipe de securitate IT și guverne din întreaga lume și le ajută să-și îmbunătățească postura de securitate. Steve este autorul cărții "Applied Incident Response" și oferă resurse gratuite pentru cei care lucrează în securitatea cibernetică la www.AppliedIncidentResponse.com.*

Resurse

Ingineria socială:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_ro.pdf
Escrocherii personalizate:	https://www.sans.org/sites/default/files/2019-02/201902-OUCH-February-Romanian.pdf
Simplificarea parolelor:	https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Romanian_0.pdf
Aveți backup:	https://www.sans.org/sites/default/files/2019-08/201908-OUCH-August-Romanian.pdf