Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Böngészők

Áttekintés

Az Internettel leggyakrabban a webböngészők – mint például a Google Chrome, a Microsoft Edge, az Apple Safari vagy a Mozilla Firefox – által lépünk kapcsolatba. Ezeket hírek, e-mailek olvasására, online vásárlásra, videók nézegetésére és játékra is használjuk. Éppen emiatt a böngészők is a kibertámadók célpontjává válhatnak.
Sokan azt feltételezik, hogy az online böngészés biztonságos, ha csak jól ismert, megbízható webhelyeket keresünk fel. Azonban nagyon könnyű nem biztonságos weboldalra tévedni. Továbbá az általunk jól ismert és megbízható weboldalak is feltörhetőek, és a kibertámadók ezekre is telepíthetnek rosszindulatú szoftvereket. Végezetül, a mai böngészők számos olyan új funkcióval rendelkeznek, amelyek akár zavaróak is lehetnek, és ha rosszul vannak konfigurálva, az még több veszélyt jelenthet számunkra.

Így használjuk biztonságosan a böngészőnket

Íme a legfontosabb lépések, amelyeket megtehetünk saját védelmünk érdekében:

Frissítés: Használjuk mindig a böngésző legfrissebb verzióját! A naprakész böngészők rendelkeznek a legújabb biztonsági javításokkal, ezáltal sokkal biztonságosabbak. A mai számítógépekkel ez már gyerekjáték, egyszerűen engedélyezzük az automatikus frissítést! Egyes böngészők esetében csupán annyi a dolgunk, hogy újraindítjuk a programot, amikor az jelzi, hogy új frissítés áll rendelkezésre. A frissítés után mindig ellenőrizzük, hogy érkezett-e új biztonsági funkció, ami hasznos lehet számunkra.

Figyelmeztetések: Ma már a böngészők gyakran felismerik az olyan rosszindulatú weboldalakat, amelyek árthatnak nekünk. Ha böngészőnk arra figyelmeztet, hogy a meglátogatni kívánt webhely veszélyes, zárjuk be a lapot, és folytassuk másik oldalon a keresést!

Szinkronizálás: Soha ne szinkronizáljuk a munkahelyi böngészőnket a személyes böngészőnkkel vagy bármelyik személyes fiókunkkal! A szinkronizálás alatt azt értjük, amikor a különböző eszközeinken lévő böngészőknek engedélyezzük, hogy kommunikáljanak egymással, és megosszák böngészési adatainkat, például az előzményeket, a könyvjelzőket és a lementett tartalmainkat.

Jelszavak: Sok böngésző támogatja a különböző weboldalakhoz tartozó jelszavak mentését. Ahelyett, hogy a böngészőben tárolnánk a jelszavainkat, használjunk inkább egy kifejezetten erre a célra szánt jelszókezelőt! A jelszókezelő egy olyan különálló biztonsági alkalmazás, amely sokkal több védelmi funkcióval rendelkezik**.**

Bővítmények: A böngészőkbe beépített modulok vagy bővítmények olyan kis szoftverek, amelyekkel még több funkció érhető el. Azonban, minden új bővítmény egyben új sebezhetőséget is jelenthet. Munkahelyi számítógépünkre csakis jóváhagyott és engedélyezett bővítményeket telepítsünk, és a böngészőhöz hasonlóan ezeket is frissítsük rendszeresen! Távolítsuk el azokat a bővítményeket, amelyeket már nem használunk!

Privát böngészés: A legtöbb böngésző lehetőséget ad a privát böngészésre, az úgynevezett „inkognitó módra". Ha inkognitó módban nyitunk meg egy böngészőlapot, azzal korlátozzuk, hogy az milyen információkat gyűjthet rólunk. Ilyen esetben böngészőnk nem gyűjti például a webes „sütiket" (cookie-kat), nem követi nyomon a böngészési előzményeket, nem tárolja és nem terjeszti az érzékeny információinkat.

Élő csevegés: Egyes webhelyek már élő csevegés funkciót is kínálnak, ahol kérdéseket tehetünk fel. Fontos, hogy csak jól ismert, megbízható oldalakon vegyünk részt online beszélgetésekben! Ezenkívül lehetőleg korlátozzuk az élő csevegés során megosztott infomációkat, mivel fogalmunk sincs arról, hogy ki gyűjti az adatainkat, mit csinál velük, és kinek adja el vagy osztja meg azokat!

Legyünk óvatosak a távoli hozzáféréssel: A csaló webhelyek gyakran úgy próbálják meg feltörni a gépünket, hogy egy felugró ablakban hamis biztonsági figyelmeztetést jelenítenek meg arról, hogy számítógépünk fertőzött, és online csevegésre próbálnak rávenni minket. Ezután azt kérik tőlünk, hogy sürgősen adjunk engedélyt, hogy távolról hozzáférjenek a gépünkhöz, és megjavíthassák azt. Valójában a számítógépünk nem is fertőzött. Ellenkezőleg, a kiberbűnözők éppen most próbálnak revenni bennünket egy rosszindulatú szoftver telepítésére, hogy azzal ellophassák jelszavainkat, személyes adatainkat és nyomon követhessék online tevékenységünket**.**

Kijelentkezés: Ha befejeztük egy adott weboldalon a böngészést, mielőtt bezárnánk az ablakot, mindenképpen jelentkezzünk ki onnan, ezzel eltávolítva a bizalmas bejelentkezési és jelszóadatainkat!

A szerzőről

Dean Parsons az ICS Defense Force vezérigazgatója, aki több mint 20 éves IT/ICS kibervédelmi tapasztalattal rendelkezik. Emellett az ICS515 minősített SANS oktatója, valamint az ICS418 társszerzője/instruktora, aki aktív kibervédelmet, incidenskezelést, valamint az ipari vezérlőrendszerekre vonatkozóan vezetést és kockázatkezelést oktat. www.linkedin.com/in/dean-parsons-cybersecurity.

Források

Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
A frissítés ereje: https://www.sans.org/security-awareness-training/resources/power-updating
Pszichológiai manipuláción alapuló támadások: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Adatvédelem: https://www.sans.org/newsletters/ouch/privacy/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)