Az Ön havi biztonságtudatossági hírlevele

Négy egyszerű lépés, hogy biztonságban maradjon

Áttekintés

A legtöbb technológia megbízható és biztonságos használata túl nehéznek és zavarosnak tűnhet. Azonban függetlenül attól, hogy Ön milyen technológiát és hogyan használ a továbbiakban ismertetett néhány egyszerű lépés segítségével biztonságban maradhat.

1. Ön: Mindenekelőtt, a technológia önmagában nem védi meg teljesen, a legjobb védelmet Ön jelenti saját maga számára. A támadók megtanulták, hogy a számukra szükséges adatok megszerzésének legegyszerűbb módja, ha inkább Önt veszik célba számítógépe, vagy egyéb eszköze helyett. Ha meg akarják szerezni jelszavát, bankkártyájának adatait, vagy a számítógépe feletti irányítást, különböző trükkökkel megpróbálják majd rávenni arra, hogy ezekhez Ön hozzáférést adjon, amelynek érdekében gyakran sürgetéshez folyamodnak. Például felhívhatják Önt a Microsoft technikai támogatásának nevében, azt állítva, hogy a számítógépe fertőzött, miközben ők valójában kiberbűnözők, akik hozzáférést akarnak szerezni a számítógépéhez. Vagy előfordulhat, hogy egy e-mail-t küldenek, amelyben figyelmeztetik, hogy a csomagját nem tudják kézbesíteni és e-mail címének megerősítésére hivatkozva arra igyekeznek rávenni Önt, hogy kattintson egy hivatkozásra. Valójában azonban egy káros kódot tartalmazó weboldal felkeresésére próbálják rábírni, aminek segítségével fel fogják törni a számítógépét. Végső soron Ön a legerősebb védelem a támadókkal szemben. Józan ésszel gondolkozva, számos támadást felismerhet és megakadályozhat.

2. Jelmondatok: A modern számítógépek sebessége elavulttá és sérülékennyé tette a régi, 8 karakter hosszú jelszavakat. Ha egy weboldal jelszó létrehozására kéri, inkább egy erős és egyedi jelmondatot adjon meg. A jelmondatok olyan jelszavak, amelyek könnyen megjegyezhető szavak sorozatából állnak, mint például „méh méz bourbon eső”. Minél hosszabb egy jelmondat, annál erősebb. Az egyedi jelmondat azt jelenti, hogy különbözőt használ minden eszközén, illetve felhasználói fiókjánál. Ilyen módon, ha egyik jelmondata kompromittálódik, a többi fiókja és eszköze még mindig biztonságban marad. Nem tudja megjegyezni az összes jelmondatát? Használjon jelszókezelőt, ami egy speciális program a jelmondatok biztonságos, titkosított formátumú tárolására (és sok más nagyszerű szolgáltatásra).

Végezetül, engedélyezze a kétlépcsős azonosítást (gyakran hívják kétfaktoros vagy többfaktoros azonosításnak). Ez a jelszavát használja, de közbeiktat egy második lépést is, mint például egy okostelefonra küldött, vagy

alkalmazás által generált kód. A kétlépcsős azonosítás valószínűleg a legfontosabb lépés, amit megtehet online fiókjának védelmében, ráadásul sokkal könnyebben, mint azt gondolná.

3. Frissítés: Bizonyosodjon meg róla, hogy az összes számítógépe, mobil eszköze, programja és alkalmazása a legújabb verziójú szoftvert futtatja. A kiberbűnözők folyamatosan keresik az új sérülékenységeket a programokban, amiket az eszközei használnak. Ha felfedeznek egy sérülékenységet, speciális programok segítségével kihasználják azt és feltörik az Ön készülékét. Eközben a társaságok, amelyek az eszközök által használt szoftvereket fejlesztik, sok munkát fordítanak a frissítések kiadására. Ezeknek a frissítéseknek az azonnali telepítésével nehezítheti meg, hogy eszközeit feltörjék. Annak érdekében, hogy mindig naprakész legyen, egyszerűen csak engedélyezze az automatikus frissítést, amikor csak lehetséges. Ez a szabály szinte bármilyen technológiára érvényes, ami a hálózatra kapcsolódik, beleértve az internet kapcsolattal rendelkező TV-t, baba figyelőt, biztonsági kamerát, otthoni routert, játékkonzolt és még az autóját is.

4. Biztonsági mentések: Néha, függetlenül attól, hogy mennyire óvatos, feltörhetik rendszerét. Ebben az esetben, gyakran az egyetlen út, hogy személyes adatait visszanyerje, a biztonsági mentés. Bizonyosodjon meg róla, hogy rendszeresen készít biztonsági mentést a fontos adatokról és ellenőrizze, hogy vissza is tudja-e állítani őket. A legtöbb operációs rendszer és mobil eszköz támogatja az automatikus mentést, akár külső meghajtóra, akár a felhőbe.

Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a https://nki.gov.hu oldalon olvasható.

A szerzőről

Steve Anson *SANS tanúsítvánnyal rendelkező oktató, aki IT biztonsági csapatok és kormányok számára ad útmutatást szerte a világon, biztonsági képességük javítása érdekében. Steve az „Applied Incident Response" – „Alkalmazott incidenskezelés" című, kiadás előtt álló könyv szerzője, emellett ingyenes forrásokat biztosít kezdő IT biztonsági szakembereknek a `v* www.AppliedIncidentResponse.com *weboldalon.*

Források

Pszichológiai befolyásolás:	https://www.sans.org/u/W3G
Megszemélyesítéses átverések:	https://www.sans.org/u/W3Q
Egyszerű jelszókezelés:	https://www.sans.org/u/W3V
Rendelkezik biztonsági mentéssel:	https://www.sans.org/u/W40