HÍRLEVÉL 1

SAJÁT ESZKÖZEINEK BIZTONSÁGA: SZÁMÍTÓGÉP, TÁBLAGÉP ÉS MOBILTELEFON

Az internetbiztonság témája négy részre osztható: az eszközök és az otthoni hálózat védelme, jelszavak, böngészők, wifi hálózatok böngészése.

Mindegyik kategória esetében megvizsgáljuk mindazt, amit meg kell tenni a minimális biztonsági szint eléréséhez, amíg a rendszer és az interneten és a hálózaton keresztül továbbított összes adat teljes mértékben védett nem lesz.

1) **Computer, táblagép vagy mobiltelefon biztonsága**

Van telepítve vírusirtó? A vírusirtó minden nap automatikusan frissül?

Ha még nincs telepítve vírusirtó program, vagy ha elavult programmal rendelkezik, amely már nem frissül, akkor cselekednie kell.

Távolítsa el a jelenlegi vírusirtót, és töltse le az ajánlott ingyenes vírusirtó programok egyikét. Ahhoz, hogy egy vírusirtót mindenki számára értelmesen megítélhessünk, legalább 6 paramétert kell figyelembe vennünk, mielőtt bármilyen döntést hoznánk. Valójában egy jó vírusirtó.

- Nem szabad, hogy túlságosan lelassítsa a számítógépet, és kevés RAM-ot kell használnia.

- Meg kell állítania a vírusokat, mielőtt azok cselekedni tudnának (rezidens aktív szkennelés).

- Nem szabad, hogy túl sok téves pozitív eredményt észleljen, és olyan fenyegetéseket lásson, amelyek nem léteznek.

- Nem szabad, hogy az igény szerinti szkennelés vagy az időszakos automatikus szkennelés túl sokáig tartson: egy modern SSD-t kevesebb mint 2 óra alatt kell teljesen átvizsgálni.

- Automatikusan frissítenie kell magát, hogy azonnal meg tudja állítani az új fertőzéseket, és megakadályozza a rendszer létfontosságú részeihez való hozzáférést.

- Képesnek kell lennie a fel nem ismert rosszindulatú programok (0-napos fenyegetések) blokkolására, és a fenyegetést csak bizonyos összetevők gyanús viselkedése alapján kell felismernie.

Ezeken a paramétereken kívül, amelyek mind nagyon fontosak a vírusirtóknál, figyelembe kell vennünk a könnyű kezelhetőséget, a felhasználói felületet, az esetleges felhasználói problémákat és a hibák, hibák és inkompatibilitások jelenlétét is.

- Telepítettek tűzfalat (firewall-t)?

Ha Windows 7 operációs rendszerrel rendelkezik, és otthon routerrel böngészik az interneten, nincs szüksége tűzfalprogramra. Ha szüksége van rá, letölthet egy ingyenes tűzfalat, amely megvédi a hálózatát és megakadályozza a behatolásokat.

- **Naprakész-e a Windows (vagy a Mac), és frissül-e automatikusan és rendszeresen?**

Sokan elhanyagolják vagy elfelejtik frissíteni a Windows-t a Microsoft által hetente kiadott javításokkal. Ezek a frissítések mindig biztonsági javítások, amelyek a legújabb réseket fedik le, amelyek lehetővé teszik a rosszindulatú felhasználók számára, hogy kívülről betörjenek a számítógépekbe, és átvegyék az irányítást.

Ellenőrizze, hogy a Windows Update szolgáltatás aktív-e a vezérlőpulton.

A Mac felhasználóknak sem szabad alábecsülniük a biztonsági frissítéseket.

-**Létrehozott már biztonsági mentési tervet adatai, dokumentumai és fényképei számára?**

Annak érdekében, hogy ne veszítse el a számítógépen létrehozott és elmentett fájlokat, tervezze meg, hogy automatikusan biztonsági másolatot készít róluk, így egy duplikált biztonsági másolat áll rendelkezésére.

Ha nincs sok adat, amelyről biztonsági másolatot kell készítenie, sokkal egyszerűbb és gyorsabb lehet online biztonsági másolatot készíteni olyan felhőalapú tárolószolgáltatásokba, mint a Dropbox és a Skydrive.

- Naprakészen tartja a számítógépére telepített programokat?

A Windowshoz hasonlóan a programokhoz is gyakran adnak ki biztonsági frissítéseket.

Azok számára, akik szeretnék, vannak módszerek a számítógépre telepített programok és szoftverek automatikus frissítésére.

- Amikor programokat tölt le, ügyel arra, hogy a telepítési folyamat során ne telepítsen más "ajánlott" programokat?

Sajnos sok ingyenes program szponzorokkal, úgynevezett "crapware"-ekkel érkezik, kéretlen, automatikusan települő programok formájában.

2) Böngésző biztonság

Az a tény, hogy számítógépe, táblagépe vagy mobiltelefonja védve van a vírusok és külső behatolások ellen, még nem garantálja, hogy a böngészés továbbra is biztonságos és privát. Lehet, hogy sokakat nem érdekel a magánélet, de a biztonság még mindig elsődleges fontosságú.

Bármelyik böngészőt is használja, annak a legújabb verzióra kell frissülnie, és engedélyezni kell az automatikus frissítéseket. A naprakész és automatikus frissítéssel rendelkező böngészők: Chrome, Firefox, Opera és Microsoft Edge.

- Amikor jelszóval jelentkezik be egy webhelyre, mindig ellenőrizze, hogy a cím https?

A HTPPS a titkosított kapcsolati protokoll, és abban különbözik a normál http protokolltól, hogy a https protokollban továbbított adatok titkosítva vannak. Ez azt jelenti, hogy ami https-ben van írva, az senki számára nem olvasható, beleértve az adott webhely üzemeltetőit is.

A HTTPS Everywhere böngészőbővítmény kiemeli a biztonságos webhelyeket, és biztosítja, hogy mindig a HTTPS protokollon belül maradjon, ahol az elérhető (lásd a https-ben való navigálás a banki webhelyeken, online boltokban, Facebookon biztonságos kapcsolattal).

- Szemmel is felismeri a veszélyes oldalakat, ahol vigyázni kell, hova kattint?

Ha még mindig nem tudod szemmel megkülönböztetni a jó webhelyet a rossztól, és mindig paranoiás vagy rosszindulatú vagy a legnépszerűbbektől eltérő webhelyekkel kapcsolatban, akkor telepíthetsz néhány bővítményt, például a WOT-ot, hogy elkerüld a veszélyes linkekre és a gyanús webhelyekre való kattintást.

- Amikor egy nem csak Ön által használt számítógépről csatlakozik egy webhelyhez, mindig kijelentkezik?

Ne feledje mindig kijelentkezni minden olyan fiókból, amelyet nyilvános vagy másokkal - köztük családtagokkal - megosztott számítógépen használ.

- **Ismeri az online átverések és csalások alapjait?**

Az adathalászat, a rosszindulatú programok és más internetes veszélyek ismerete fontos ahhoz, hogy biztonságban maradjunk tőlük.

- Védi a böngészőjét az online nyomkövetéstől?

Amint azt már elmagyaráztuk, a weboldalak általi online nyomon követés megakadályozása az adatgyűjtés blokkolását jelenti. Ez bizonyos, a böngészőbe telepíthető bővítmények segítségével lehetséges.

Az interneten a legmagasabb szintű védelem és a magánélet védelme az anonim böngészés. A teljesen anonim szörfözés nem mindenki számára hasznos, és nem is lehet minden helyzetben. Hasznos lehet, ha valami illegális (de jó, például torrentek letöltése) tevékenységet folytat, ha nem akarja felfedni földrajzi helyzetét, vagy ha IP-címét szeretné meghamisítani, hogy hozzáférjen blokkolt webhelyekhez.

Bár az interneten sokféleképpen lehet névtelenül szörfölni, az online adatvédelem csak a TOR böngészővel garantált.

3) Az online használt jelszavak biztonsága

- Összetett jelszavakat használ?

Az egyik leggyakoribb hiba, amit az internetezők elkövetnek, hogy egyszerű jelszavakat vagy olyan jelszavakat használnak, amelyek a személyes életükben történt tényekre vagy eseményekre utalnak. Mindig olyan jelszavakat válasszon, amelyeket lehetetlen kideríteni, és mindenekelőtt minden weboldalhoz készítsen erős jelszót, anélkül, hogy bárkinek esélyt adna arra, hogy kitalálja (soha ne használja a születési dátumát, a kedvenc csapatát, a felesége vagy a kutyája nevét).

- Minden webhelyhez más jelszót használ?

Soha ne használja ugyanazt az e-mail és jelszó kombinációt több szolgáltatásban, mert ha egy hackernek sikerül bejutnia az e-mail fiókba, akkor minden személyes fiókjába gond nélkül be tud törni.

Használjon programot a webes fiókok jelszavainak létrehozására és kezelésére.

Ahol lehetséges (Dropbox, Google, Gmail és Facebook), használjon kétfaktoros hitelesítést.

Az extra védelem érdekében mindenképpen ellenőrizze a Facebook és a Twitter alkalmazások engedélyeit.

4) Hálózati biztonság

- Az otthoni WiFi hálózata védett-e a WPA2 kulccsal?

Ha nem, vagy ha fogalma sincs, mi az a WPA2, akkor tudnia kell, hogy a WPA a Wi-Fi Protected Access rövidítése, és hogy a Wi-Fi Protected Access II (WPA2) és a Wi-Fi Protected Access III (WPA3) három biztonsági protokoll és tanúsítási program, amelyeket a Wi-Fi Alliance fejlesztett ki a vezeték nélküli számítógépes hálózatok védelmére.

- **Tisztában van azzal, hogy amikor csatlakozik egy nyílt Wi-Fi hálózathoz, minden, amit csinál, látható a számítógépén kívülről?**

Az egyetlen dolog, ami védi a jelszavak biztonságát az interneten keresztül egy nyilvános wifi-hálózaton, az a második pont első kérdésében említett HTTPS protokoll.

- **Ellenőrizte a megosztott mappákat a számítógépén?**

Amint az már kiderült, nagyon könnyű betörni a számítógépekbe és betekinteni más számítógépek megosztott mappáiba. Nagyon gyakran a művelet azért sikeres, mert az emberek elfelejtik kizárni a megosztott mappákat vagy a teljes merevlemezt a számítógépen. Ha teljesen névtelenül szeretne számítógépet használni, és nyomok hátrahagyása nélkül csatlakozni a hálózathoz, használhat egy anonim és privát Linux rendszert, például a Tails-t.

A biztonság mindenki számára fontos, a tapasztalt technikusoktól a számítógépes analfabétákig. Az elővigyázatosság szintje csak Önön múlik, de ne feledje, hogy az online biztonság ma már ugyanolyan fontos (ha nem fontosabb), mint az otthona biztonsága.

A projekt az Európai Bizottság támogatásával valósult meg. Ez a dokumentum kizárólag a projektpartnerek véleményét tükrözi, és a Bizottság nem tehető felelőssé a benne foglalt információk bármilyen felhasználásáért.