OUCH! 2023. február

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Van-e szükségünk kibervédelmi szoftverekre?

Áttekintés

Néhány évvel ezelőttig, ha egy újonnan vásárolt számítógépet biztonságban akartuk tudni a hackerektől, ahhoz biztonsági szoftvereket kellett telepítenünk rá. Manapság azonban a legtöbb eszközben már több beépített biztonsági funkció is elérhető, mint például az automatikus frissítés, a tűzfal, a háttértár titkosítás és a fájlvédelem. Illetve a Windows-os gépeken ott van a Microsoft Defender is, ami antivírus funkcióval is rendelkezik. A mai rendszerek sok szempontból gyárilag biztonságosabbnak tekinthetőek. Sőt, a legnagyobb biztonsági kockázatot valójában mi, a felhasználók jelentjük. Ez az oka annak, hogy a kibertámadók folyamatosan az embert célozzák, és olyan dolgokra próbálnak meg rávenni bennünket, amelyeket nem kellene megtennünk, például megadni a jelszavunkat, rákattintani egy hivatkozásra, vagy megnyitni egy e-mail üzenet mellékletét, mert könnyen lehet, hogy ezek káros kódot telepítenek az eszközünkre, vagy általuk lopják el a bankkártyaadatainkat.

Minek a használatát érdemes megfontolni?

Amennyiben extra védelmet szeretnénk rendszerünkön, többféle biztonsági szoftvert is igénybe vehetünk.

Jelszókezelők: A komplex jelszavak megjegyzése nem könnyű – főképp, ha ezekből több százzal rendelkezünk. A jelszókezelő egy olyan megbízható digitális széf, ahol az összes jelszavunkat biztonságban tárolhatjuk, miközben egyetlen, ún. mesterjelszóra kell csupán emlékeznünk. A jelszószéfek további funkciókkal is rendelkeznek, például segítségükkel biztonságosan jelentkezhetünk be a weboldalakra és jelszavakat is generálnak nekünk.

Virtuális magánhálózat (VPN): A VPN-ek legfőbb célja a magánszféránk védelme, azáltal, hogy titkosítják a netes kommunikációnkat és elrejtik, hogy honnan Internetezünk.

Biztonsági termékek: Ezek olyan kibervédelmi szoftverek, amelyek az operációs rendszer védelmi funkcióin felül extra biztonsági funkciókat kínálnak, mint például a veszélyes weboldalak kiszűrését, szülői felügyeleti funkciókat és sok esetben VPN szolgáltatást. A biztonsági termékek azonban eltérő funkciókkal rendelkezhetnek, emiatt érdemes alaposan utánajárni, hogy melyik termék felel meg leginkább az igényeinknek.

A gyártó kiválasztása

Ha további biztonsági szoftverre van szükségünk, számos cég közül választhatunk. Hogyan válasszunk közülük? A különböző gyártók a legtöbbször nagyon hasonló funkciókat kínálnak. A kulcs az, hogy egy megbízható céget válasszunk. Amit mindenképpen el szeretnénk kerülni, az az, hogy véletlenül egy kiberbűnözők által terjesztett vírusos szoftvert töltsünk le.

Kizárólag olyan cégtől vásároljunk, amiről már hallottunk és amit megbízhatónak tartuk! Véletlenül se vegyünk szoftvert olyan gyártótól, amelyikről semmit sem tudunk, amelyik nemrég kezdte meg a működését, amelyiknél nem érhető el vásárlói vélemény vagy éppen, hogy sok negatív vélemény található róla. Szeretnénk biztosra menni, hogy amit megvásárolunk, az egy valódi, legitim szoftver, amihez érkeznek majd hibajavítások. A döntésünk során lehet szempont az is, hogy az adott gyártó melyik országban van bejegyezve. Léteznek olyan online oldalak, amelyek összehasonlítják a megbízható gyártókat és a biztonsági termékeik közti funkcióbeli és árbeli különbségeket.

Mindig legyünk óvatosak az ingyenes eszközökkel! Habár léteznek valóban kiváló ingyenes biztonsági termékek is, azért aggályok is merülhetnek fel. Ezek a szoftverek ugyanis sok esetben korlátozott funkciókkal rendelkeznek, nehezen használhatóak, vagy nem frissülnek elég gyakran. Egyes esetekben az ingyenes eszközöket pont a kiberbűnözők készítik, amikben kártékony kódokat helyeznek el.

Ne feledjük, miközben ezek a biztonsági eszközök hasznosak, éredemes először a számítógép beépített biztonsági funkcióival kezdenünk, mint például az automatikus frissítés engedélyezése! A modern operációs rendszerek önmagukban is elég biztonságosak. A legjobb védelmet mi magunk jelentjük. Legyünk óvatosak a furcsa telefonhívásokkal, e-mailekkel vagy szöveges üzenetekkel! Nincs az a biztonsági szoftver, ami képes lenne megvédeni bennünket attól, ha valaki olyan dologra akar rávenni, amit nem kellene megtennünk.

A szerzőről

Nico „Dutch_OsintGuy” Deken tanúsított SANS instruktor és korábbi kormányzati hírszerzési elemző, aki a nyílt információszerzésre (OSINT) szakosodott.
Nicóról további információ érhető el itt: https://www.sans.org/profiles/nico-dekens/
valamint itt: https://www.dutchosintguy.com.

Források

Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
A frissítés ereje: https://www.sans.org/security-awareness-training/resources/power-updating/
Virtuális magánhálózatokról: https://www.privacyguides.org/vpn/
Pszichológiai manipulációról: https://www.youtube.com/watch?v=lc7scxvKQOo
Biztonsági termékbemutatók: https://www.pcmag.com/picks/the-best-security-suites

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