OUCH! 2021. április

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Adatvédelem – Így védjük digitális lábnyomunkat

Mit jelent az adatvédelem?

Az „adatvédelem” kifejezés többféleképp is értelmezhető. E kiadványban a magánélet védelmére fókuszálunk, mindazon információkra, amelyeket rólunk gyűjthetnek. Jelenkorunk digitális világában megdöbbentően sok szervezet gyűjt rólunk információkat, amelyekkel legálisan kereskedik is. Minden alkalommal, amikor böngészünk, vagy valamit online vásárolunk, megnézünk egy videót, ellátogatunk a háziorvoshoz vagy megnyitunk egy alkalmazást a telefonunkon, információ keletkezik rólunk, ami valakinél, valahol gyűjtésre kerül. Az ilyen adatok felhasználhatóak arra, hogy termékeket vagy szolgáltatásokat adjanak el számunkra, meghatározható, hogy milyen orvosi kezelésben részesülünk, vagy hogy milyen munkát szeretnénk, sőt az is előfordulhat, hogy ezek alapján döntenek arról, hogy milyen kamatlábbal kapunk hitelt. Továbbá, ha ezek az információk rossz kezekbe kerülnek, arra is lehetőséget adhatnak, hogy kiberbűnözők célpontjává váljunk.

A személyes adatvédelem célja, hogy kezeljük digitális lábnyomunkat, például: - megkíséreljük korlátozni, hogy milyen információk kerülhetnek rólunk gyűjtésre. Azonban jó, ha tisztában vagyunk vele, hogy az szinte lehetetlen, hogy digitális lábnyomunkat teljesen eltüntessük, vagy hogy minden szervezet adatgyűjtését megakadályozzuk. Csupán csökkenteni tudjuk ezek mértékét.

Lépések, amelyek segíthetnek személyes adataink védelmében

Szögezzük le: nem létezik olyan átfogó lépés, ami megoldást jelent minden adatvédelmi problémára. Valójában rengeteg lépést kell tennünk, és ezek közül mindegyik egy kicsit hozzájárul a célhoz. Minél több lépést végzünk el, annál többet teszünk a magánszféránk védelme érdekében.

- Korlátozzuk, hogy mit osztunk meg másokkal az online térben, mint például fórumokon vagy a közösségi média oldalakon! Ebbe beleértendő az is, hogy milyen képeket (például szelfiket) osztunk meg. Még a privát fórumokon is, vagy ha erős adatvédelmi beállításokat alkalmazunk, azt kell feltételeznünk, hogy posztjaink előbb-utóbb napvilágra kerülnek.
- Amikor online fikókot regisztrálunk, nézzük át, hogy az adott oldal milyen információkat gyűjt rólunk – ezt az adatvédelmi irányelvek alatt találjuk – és csak annyi információt tegyünk elérhetővé, amennyi abszolút szükséges. Amennyiben aggodalom támad bennünk azzal kapcsolatban, hogy milyen információkat gyűjtenek rólunk, inkább ne vegyük igénybe a szolgáltatást!

- Vegyük azonban figyelembe, hogy attól függetlenül, hogy milyen adatvédelmi beállításokat alkalmazunk, vélhetően történik majd adatgyűjtés, különösen az olyan ingyenes szolgáltatások esetében, mint a Facebook vagy a WhatsApp. Az ilyen szolgáltatások teljes üzleti modelljüket arra alapozzák, hogy begyűjtik a felhasználók tevékenységéről és interakcióiról keletkező információkat. Ha igazán fontos számunkra az adatvédelem, legjobb, ha mellőzzük az ilyen szolgáltatások használatát.
- Alaposan nézzünk utána minden egyes mobil alkalmazásnak, mielőtt letöltjük és telepítjük azokat! Biztosan megbízható fejlesztőtől származnak? Elég hosszú ideje elérhetőek? Elég sok pozitív értékeléssel rendelkeznek? Ellenőrizzük az alkalmazásengedélyeket! Biztos hogy az appnak hozzá kell férnie a földrajzi helyzetünkhöz, vagy a kontaktjainkhoz? Amennyiben kétségeink vannak, válasszunk inkább egy másik appot! Részesítsük előnyben azokat az alkalmazásokat, amelyek adatvédelmi szemléletűek, és ennek megfelelően részletes beállítási lehetőségeket nyújtanak. Habár előfordulhat, hogy többet kell fizetnünk egy olyan alkalmazásért, amelyik tiszteletben tartja a magánszféránkat, lehet, hogy ez így is jobban megéri.
- Fontoljuk meg egy VPN (Virtual Private Network) szoftver alkalmazását az internetre való kapcsolódáshoz, különösen nyílt hálózatok használatakor, mint amilyen az ingyenes Wi-Fi.
- Webböngészők esetén az adatvédelmi beállításokat állítsuk privátra, és használjunk inkognitó módot, ezáltal korlátozhatjuk a megosztott információkat, a böngészési sütik használatát, és védhetjük a böngészési előzményeinket. Vegyük fontolóra adatvédelmi kiegészítők alkalmazását, mint a Privacy Badger, vagy váltsunk magánszférát tiszteletben tartó böngészőre.
- Használhatunk anonimizáló webkeresőket, mint a DuckDuckGo vagy a StartPage.

A privát szféra védelme nem könnyű, ugyanis ez nagyban függ a hatályos adatvédelmi törvényektől is – amelyek országonként eltérőek lehetnek –, valamint azoknak a vállalatoknak az etikai hozzáállásától, amelyekkel kapcsolatba kerülünk. Habár jelen technikai korban, nem tudjuk teljes mértékben megőrizni magánszféránk érintetlenségét, a fentebb sorolt lépések segítségével csökkenthetjük a rólunk gyűjtött adatok mennyiségét.

A szerzőről

Kenton Smith egy elismert kanadai kiberbiztonsági tanácsadó, aki biztonsági program-fejlesztésre, menedzsmentre és értékelésre specializálódott. Mindemellett SANS oktató, aki mendzsment kurzusokat vezet. Elérhető a Twitteren, mint @kentonsmith vagy, esetenként a kentonsmith.neten.

Források

Adatvédelmi beállításokról: https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/
Személyazonosság-lopás elleni védelem:https://www.sans.org/security-awareness-training/resources/identity-theft
Virtuális magánhálózatok (VPN): https://www.sans.org/security-awareness-training/resources/virtual-private-networks-vpns
Nyílt forrású információszerzés: https://www.sans.org/security-awareness-training/resources/search-yourself-online

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