Tippek és tanácsok

Ebben a fejezetben – amely az Egyesült Királyságban futó *Get Safe Online* (Szörfölj biztonságosan) kampány és az Egyesült Államok Belbiztonsági Minisztériuma közös gondozásában készült – néhány olyan hasznos tippet és tanácsot talál, amelyek betartásával biztonsággal internetezhet.

- Gondoskodjon számítógépe és hordozható eszközei védelméről
- Személyes adatok védelme
- Munkahelyén kívül is óvja a céges adatait
- Csatlakozzon óvatosan
- Legyen webrekész

Gondoskodjon számítógépe és hordozható eszközei védelméről

Asztali számítógép

- Használjon tűzfalat – saját hálózatát ezzel nemcsak a különböző vírusoktól, de a hackertámadásoktól is megóvhatja.
- Telepítsen vírusirtó alkalmazást – használatukkal elkerülhető, hogy gépe fertőzés áldozatává váljon.
- Mindig töltse le a legújabb biztonsági frissítéseket – alkalmazásait és operációs rendszerét így folyamatosan naprakészen tarthatja.
- Védekezzen a kémprogramok ellen – ne engedje, hogy illetéktelenek hozzáférést szerezzenek gépéhez, óvakodjon a gyanús tartalmú e-mailek és csatolmányok megnyitásától.
- Rendszeresen készítsen biztonsági mentéseket – adatait csak így tudhatja igazán biztonságban.

Hordozható számítógépek

- Vezeték nélküli hálózati adapterét csak akkor kapcsolja be, ha szükséges.
- A biztonsági alkalmazások frissítéséhez laptopját megbízható hálózatra csatlakoztassa.
- A gépen tárolt adatairól készítsen biztonsági mentéseket.
- Ne hagyja laptopját őrizetlenül.

USB pendrive-ok

- Használjon titkosított pendrive-ot
- A vírusfertőzések elkerülése érdekében állítsa a pendrive-on található kapcsolót írásvédett (read only) állásba: egyes modelleket külön erre a célra kialakított gombbal lehet írásvédett

üzemmódba helyezni, így a pendrive-on tárolt adatok felülírása, illetve módosítása elkerülhető.
- A nem megbízható és/vagy illetéktelen számítógépről történő fájlmentést követően futtasson a pendrive-on vírusellenőrzést a fertőzések elkerülése érdekében.
- Mielőtt pendrive-ját idegen számítógéphez csatlakoztatná, töröljön róla minden olyan állományt, amely nem szükséges az adott feladathoz.
- A pendrive-on tárolt adatokról készítsen biztonsági mentéseket, így azok adatvesztés esetén visszaállíthatók.
- Apró méretéből adódóan különösen fennáll az elvesztés, illetve a lopás veszélye. Tartsa pendrive-ját kulcscsomóján vagy egy pántra fűzve. Ne feledje, hogy minél nagyobb az eszköz tárolókapacitása, annál nagyobb mennyiségű adat kerülhet illetéktelenek kezébe. Pendrive-jainkat előszeretettel tartjuk táskában, hátizsákban, laptoptáskában, kabát-, vagy nadrágzsebben, ám gyakran maradnak az íróasztalon őrizetlenül. Az utóbbi időben megnőtt a pendrive-ok elvesztéséből, eltűnéséből, engedély nélküli kölcsönvételéből, illetve eltulajdonításából adódó nemkívánatos esetek száma.

Mobiltelefonok és kéziszámítógépek

A Palm kéziszámítógépek, valamint a különböző platformokon – Windows Mobile, iOS, Android és BlackBerry – működő okostelefonok internetkapcsolattal rendelkeznek és óriási mennyiségű adat tárolására képesek. Hordozhatóságuk miatt használatuk különös körültekintést igényel.

- A vezeték nélküli csatlakozásokat (pl. Bluetooth és WLAN) csak akkor használja, ha szükséges. A Bluetooth technológia lehetővé teszi, hogy különböző elektronikus eszközök rövid hatótávolságú rádiókapcsolaton keresztül kommunikáljanak egymással.
- Az adatvesztés elkerülése érdekében mobiltelefonját, illetve kéziszámítógépét soha ne hagyja őrizetlenül.
- Okostelefonja távoli hackertámadásoknak is ki van téve: jelszó használatával védje készülékét.

Személyes adatok védelme

- **Erős jelszót használjon**: az interneten található képzeletbeli házhoz, amelyben adatait tárolja, a jelszó jelenti a kulcsot és a zárat. A jelszó használata igen lényeges védelmi megoldás; a megfelelő jelszó kiválasztásával nemcsak az Ön számára fontos adatokat, de személyazonosságát is nagyobb biztonságban tudhatja. A számítógépén, illetve a különböző online felületeken tárolt személyes és céges adataihoz egyaránt a számítógépéhez használt jelszó jelenti a kulcsot. Adatainak védelme érdekében erős, több különböző karaktertípusból (betűkből, számokból és írásjelekből) álló, kis- és nagybetűket is tartalmazó jelszót használjon. Minél összetettebb karakterlánc alkotja a jelszót, annál nehezebb megfejteni. Kerülje a mások által is ismert személyes adatok – saját vagy gyermekének neve, születési dátumok stb. –, valamint a leggyakrabban előforduló szavak használatát,

léteznek ugyanis olyan hackerprogramok, amelyek a szótárak összes bejegyzéseit végigpróbálgatják.

- **Rendszeresen változtassa meg jelszavát**: amennyiben illetéktelen hozzáférésre gyanakszik, jelszavát azonnal változtassa meg.
- **Soha ne adja ki jelszavát**: saját egyedi jelszavát soha ne ossza meg senkivel. Lehetőség szerint próbálja megjegyezni; ehhez saját módszert is kidolgozhat. Ha mégis leírná jelszavát, nem mindegy, hol tárolja. Soha ne hagyja a jelszót tartalmazó jegyzeteit olyan helyen, ahol a jelszóval védett adatokat sem hagyná.
- **Egyedi fiók, egyedi jelszó**: minden egyes online fiókhoz külön jelszót (de legalábbis ne mindhez ugyanazt) használjon. Ha több fiók esetében is ugyanazt a jelszót használja, az egyiket feltörő támadó egyúttal az összes többihez is hozzáférést nyer.
- **Gondoskodjon fiókjai biztonságáról**: az azonosításhoz számos szolgáltatónál további lépések is igénybe vehetők.
- **Az interneten is maradjon saját maga ura:** amikor csak lehet, az egyes weboldalak adatvédelmi és biztonsági beállításait saját komfortérzetének megfelelően módosítsa. Tanácsos megszabni azoknak a körét, akikkel információt oszt meg.
- **A közösségi hálókat körültekintéssel használja:** ne feledje, hogy a különböző közösségi hálóknál az internethasználat rejtett veszélyei egyszerre jelentkezhetnek. Ezek közé tartozik a számítógépes zaklatás (cyber bullying), a személyes adatok közzététele, a zaklató online követés, a korhatáros tartalmak hozzáférése, valamint – a legdurvább esetekben – a gyermekek behálózása és a gyermekek szexuális zaklatása.

Munkahelyén kívül is óvja a céges adatait

- **Ügyeljen arra, hogy a bizalmas információk biztonságban legyenek**: a lopás, illetve elvesztés megelőzése érdekében munkahelyétől távol is gondoskodjon a bizalmas információk és eszközök folyamatos védelméről. Adatait nyilvános helyeken különös körültekintéssel kezelje.
- **A céges információkat tartsa bizalmasan**: ügyeljen arra, hogy beszélgetése illetéktelen fülekbe ne jusson el. Cége bizalmas információit ne tegye bárki által hozzáférhetővé.
- **Ügyeljen a fürkésző tekintetekre**: utazás vagy távoli munkavégzés során védekezzen a kifigyelés ellen.
- **A webes levelező rendszereket körültekintéssel használja:** a böngészőben megnyitott e-mailek olvasása néhány sajátos kockázattal jár és ugyanolyan óvatosságot igényel, mintha asztali levelezőrendszert használna.

Csatlakozzon óvatosan

- **Vezeték nélküli hálózati adapterét csak akkor kapcsolja be, ha szükséges**
- **Tudjon meg mindent a wifi-hotspotokról**: ha az internetre wifi-hotspoton keresztül csatlakozik, csak az adott feladatra használja az adatkapcsolatot, biztonsági beállításait pedig úgy módosítsa, hogy kizárólag az arra illetékesek férjenek gépéhez.

- **Ügyeljen pénze biztonságára**: online vásárláskor, illetve banki szolgáltatások használatakor ellenőrizze, hogy biztonságos-e a kapcsolat. Ha az adott weboldal címében „https://” vagy „shttp://” található, ez arra utal, hogy adatai védelme érdekében az oldal több megoldást is használ. Nem biztonságos az a weboldal, amelynek címében „http://” szerepel.
- **Szabjon gátat a kéretlen e-maileknek**: a levélszemét (spam) biztonsági veszélyforrást jelent. Ne nyissa meg az ismeretlen feladótól származó e-maileket, illetve azok csatolmányait.
- **Kétely esetén töröljön**: az e-mailekben, tweetekben, bejegyzésekben és internetes reklámokban szereplő gyanús linkek esetén a legjobb megoldás – még ha tudja is, hogy honnan származnak –, ha törli őket, de legalábbis jelölje ezeket levélszemétként.
- **Csak akkor továbbítson e-mailt, ha az szükséges.** mielőtt továbbítaná, fontolja meg az adott üzenethez tartozó előzmények törlését.
- **Körültekintéssel barangoljon az interneten**
- **Dokumentumokat, illetve bármilyen tartalmat csak megbízható felektől töltsön le.**
- **A nyilvános számítógépeket óvatosan használja:** nyilvános számítógépről csak titkosítást alkalmazó kapcsolatot létesítsen (ezt a böngészőjének jobb alsó sarkában megjelenő lakat, valamint a weboldal címének elején szereplő „https://” jelzi).
- **Csak ismert és megbízható vállalatok webmail-szolgáltatásait használja!**

Legyen webrekész:

- **Tartson lépést:** kövesse a biztonságos internethasználat terén végbemenő fejlesztéseket. Tudja meg a megbízható weboldalakkal kapcsolatos legfrissebb információkat, és ossza meg családtagjaival, barátaival és munkatársaival. Tartsa őket is webrekészen! Tegye biztonságossá böngészőjét.
- **Gondolkodjon, mielőtt cselekedne**: óvatosan kezelje azokat az üzeneteket, amelyek azonnali választ várnak Öntől, túl szépek ahhoz, hogy igazak legyenek, vagy személyes adatai megadását kérik.
- **Biztonsági mentés mindenek felett**: munkáját, hang- és képfájljait, valamint egyéb digitálisan tárolt adatairól megóvásuk érdekében készítsen elektronikus másolatot, és tartsa azt biztonságos helyen.