

SZEMÉLYES (OTTHONI) INFORMÁCIÓBIZTONSÁG

1. A személyes (otthoni) információbiztonság felmérése

A jelenlegi helyzetben, amikor a közigazgatási intézmények, vállalkozások dolgozói otthonról fogják a feladataikat ellátni (home office), indokolt az otthoni információbiztonság általános állapotának felmérése, valamint az aktuális biztonsági szint fokozása speciális megoldások, alkalmazások (jelszókezelő rendszerek, titkosított adattároló konténerek) bevezetésével. Az elkövetkező időszakban várhatóak olyan kibertámadások, amelyek kifejezetten az óvatlan felhasználót célozva szereznek érzékeny információkat a munkáltatóról.

A felmérés lépései

#	Információbiztonsági kockázatok	Javasolt megoldások
1.	Otthoni WiFi elérés - Jelszavak ellenőrzése - SSID név azonosíthatósága	Otthoni WiFi elérés - Jelszóváltoztatás – lehetőleg ne utaljon sem lakhelyre, családra, személyes adatokra - Amennyiben szükséges rejtett SSID alkalmazása
2.	Antivirus szoftver Sok esetben tapasztalható, hogy a felhasználók nem használnak semmilyen antivirus szoftvert az otthoni számítógépen.	Antivirus szoftver - minden esetben használjuk valamilyen lehetőleg licence köteles antivirus programot - válasszunk a nagyobb jó hírű gyártók termék palettájából - Symantec/Norton - ESET Nod32 - Avast - AVG - Bitdefender - F-Secure - AviRa
3.	Böngésző Az internet világában elengedhetetlen, hogy használjuk valamilyen böngészőt. Nagyon nehéz volna az egyes típusokat rangsorolni. Azonban biztonsági szempontból jelenleg a google chrome áll az első helyen.	Böngésző - ne mentünk a jelszavainkat a böngészőben, kényelmes, azonban egyszerűen kihasználható - mindig használjuk legfrissebb verziót.
4.	Biztonsági mentés Biztonságban vannak az adataink - mondják a felhasználók megtettem mindent annak érdekében, hogy ne érjen meglepetés. Mindent egy külső meghajtóra...	Biztonsági mentés - javasolt megoldás a titkosított adatokat biztonságosan kell menteni. - a mentett állomány visszaállítható? Nem csak a mentés fontos, hanem használható-e a mentett állomány - jó megoldás lehet egy SOHO eszköz (pl.: NAS) alkalmazása, de csak a megfelelő biztonsági beállítások használatával vagy csupán egy külső meghajtó.

5. Jelszókezelés Az átlagos felhasználó a következő jelszavakat használja: • minden jelszó ugyanaz (könnyű megjegyezhetőség) • a jelszavak valamilyen egyszerűen kitalálható elv alapján épülnek fel (gyerekek neve, kutyanéve, születési vagy aktuális év)	Jelszókezelés • jelszókezelő alkalmazás használata – a jelszavak egyszerűen változtathatóak • nyilvános helyen (vonat, busz, repülőgép) az alkalmazás működéséből fakadóan nem „leshetők” le a jelszavak • Mindössze egy mester jelszó megjegyzése szükséges
6. Adatvédelem • a notebookon vagy PC-n az adatok tárolása titkosítatlanul történik • ha van valamilyen adatmentés a mentett adatok védelme (titkosítás) nem megoldott	Adatvédelem • titkosított adattároló konténerek alkalmazása • szükség esetén a teljes gép titkosítása – ebben az esetben az operációs rendszer egy „preboot” azonosítással indul A biztonsági mentés legyen titkosított meghajtóra mentve vagy titkosított formában. • jó megoldás lehet egy SOHO eszköz (pl.: NAS) alkalmazása. Mert a fenti összes elvárásnak megfelel
7. Notebook használat nyilvános helyeken • utazás vagy nyilvános helyeken történő használat esetén óvatlanságból gyakorta láthatóvá válnak információk ○ közlekedési eszközökön (repülő, vonat, busz) végzett munka ○ Nagyobb projektben végzett csoportmunka során láthatóvá válik az eszköz képernyője. Így illetéktelenek is érzékeny információkhoz férhetnek hozzá.	Notebook használat nyilvános helyeken • utazás vagy nyilvános helyeken történő használat esetén gondoskodni kell arról, hogy a képernyő tartalma illetéktelenek számára rejtve maradjon. ○ ne használjuk az eszközt abban az esetben, ha nem tudjuk biztosítani az információk biztonságát. ○ projekt munka során használjunk rálátás gátló fóliát – így csak egy bizonyos látószög esetén olvasható a képernyő tartalma.
8. Notebook használat utazás során Minden utazás kockázatokkal jár, a mai rohanó világban az utazás alatt sem akarunk kiszakadni az információk áramlásából. Ezért az utazásainkra magunkkal visszük elektronikus berendezéseinket.	Notebook használat utazás során • ha a notebookon vagy táblagépen vannak számunkra érzékeny információk, a szállodában elérhető ingyenes WiFi-t csak mértékkel használjuk. Sajnos minden huszadik ingyenes WiFi hozzáférési pontot adathalászat miatt telepítik. Javasolt a saját mobil telefonunkkal megosztott mobil HotSpot használata. • Utazásra nem vigyünk olyan notebookot, ami nincs titkosítva és tartalmaz érzékeny adatokat. • Már a szobafoglalás során győződjünk meg arról, hogy a szállodai szobában van-e a notebook vagy táblagép elzárására alkalmas szobaszéf.

9. Internetről származó tartalmak Ingyenesen letölthető volt az internetről miért volna veszélyes...	Internetről származó tartalmak Nem megbízható tartalmak esetében javasolt a letöltött tartalmak ellenőrzése. A 3. pontban említett antivirus programok végeznek ellenőrzéseket. Azonban ha biztosak akarunk lenni a letöltött tartalom megbízhatóságában, használjuk valamilyen online ellenőrző rendszert ilyen pl.: virustotal - https://www.virustotal.com/#/home/upload ahol a feltölthető a fájl és 67 víruskereső ellenőrzi a használni kívánt tartalmat.
--	---

**TEGYÜNK MEG MINDENT A BIZTONSÁGUNK ÉRDEKÉBEN
LEGYÜNK BIZTONSÁGTUDATOSSAK!**