Számítógépes adatvédelem, adatbiztonság

Mi az adat?

Az adat tények, fogalmak olyan megjelenési formája, amely alkalmas emberi eszközökkel történő értelmezésre, feldolgozásra, továbbításra. Az adatokból gondolkodás vagy gépi feldolgozás útján információkat, azaz új ismereteket nyerünk.

Mi a személyes adat? Miért kell védeni az adatokat?

Az adatok egyre inkább elektronikus formában kerülnek tárolásra, ezért egyre fontosabb a számítógépes adatok védelme, a számítógép-biztonság.

A számítógép-biztonság: az adatok fizikai védelmét, és az adatok illetéktelenektől való védelmét, elsősorban a titkosságot értjük alatta.

Az adatokat fizikailag azért kell védenünk, mert az eszközeink elromolhatnak, megsemmisülhetnek, elveszhetnek, sőt ellophatják őket.

Megoldás:

- **biztonsági mentés, a fontos adatoknak mindig legyen egy biztos helyen tárolt másolata,**
- **mindig legyen bekapcsolva Tűzfal a számítógépeden (**Tűzfal, angolul Firewall, olyan hálózati biztonsági rendszer, amely felügyeli és szabályozza a bejövő és kimenő hálózati forgalmat előre meghatározott biztonsági szabályok alapján**)**
- **használj vírus és kém programok elleni védelmet (**pl. Avast, Kaspersky, Defender stb.**)**

5 biztonsági aranyszabály internetezőknek

1. Védjük magunkat!

Gondosan válasszuk meg az internetes bejelentkezésekhez szükséges jelszavainkat, és frissítsük őket rendszeresen! A weboldalak, applikációk, okoseszközök által előre beállított jelszavakat cseréljük le sajátra, amely legalább 8-12 karakter hosszú (de nem értelmes szöveg), tartalmaz kisbetűt, nagybetűt, számot és speciális karaktereket. Ezeket azonban nehéz megjegyezni, ezért jó ötlet egy általunk kitalált, könnyen felidézhető jelszógeneráló módszer létrehozása (pl.: válasszunk egy mondatot, és használjuk a szavak kezdőbetűit), vagy használjunk egy jelszótároló alkalmazást. A szakemberek szerint **könnyen megjegyezhető, rövid mondatokat** is használhatunk, mint „Szer3tem@zAlmát!”. Ez számunka könnyen megjegyezhető, van benne szám, kis- és nagybetű és speciális karakter is.

(**Böngészőbe épülő jelszókezelő elérhető a G DATA TOTAL SECURITY programban is.**
)(Egyúttal a gyerekek hozzáféréseit is érdemes ismerni, és néha azt is változtatni kell velük együtt, hogy megszokják a folyamatot.)

2. Mit szólna a nagymama?

Bár az interneten sok minden látszólag névtelenül történik, de ez csak egy illúzió. Az online téren keresztül is a valóságos világban maradunk, igazi veszélyekkel. Éppen ezért jó ötlet követni azt az **egyszerű szabályt**, hogy ne tegyünk semmi olyat a neten, amit nem szeretnénk, hogy megtudjanak a tanáraink, barátaink és igen, a nagymamánk. Többek között ne álljunk szóba idegenekkel, ne bántsunk senkit az online térben, ne írjunk le olyat, amit később jó eséllyel megbánhatunk, és – amit nem lehet eléggé hangsúlyozni – ne osszunk meg a nyilvánossággal privát információkat.

3. Ne menjünk a divat után!

Azért, mert valami éppen menő, nem biztos, hogy hosszú távon jó ötlet. Például ne használjunk biometrikus felismeréssel (ujjlenyomat, arcfelismerés) dolgozó **ismeretlen appokat**, csak azért, mert ez a legújabb dili! Vagy ne töltsünk fel fehérneműs képeket azért, mert minden barátunk ezt csinálja. Ha az ujjlenyomatunk vagy a képeink ártó szándékú emberek kezébe kerülnek, nagy baj lehet belőle.

4. Az interneten nincsenek titkok

Sajnos tudomásul kell vennünk, hogy ami felkerül az internetre, az jó eséllyel ott is marad. Hiszen előfordulhat, hogy az általunk törölt képet egy barátunk vagy a szolgáltató már tárolja valahol másolatként. Ezért a kényes információkat – például kínos fotók, személyes titkok, stb. – soha ne osszuk meg a neten. *(Ennek fényében gondoljuk át azt is, hogy milyen tartalmakat teszünk fel a gyerekeinkről, hiszen nem biztos, hogy 20 év múlva is hálásak lesznek a pelenkás képeik feltöltéséért.)*

5. Óvakodjunk a nyilvános Wi-Fi hálózatoktól!

Jó, ha tudjuk, hogy a hálózatokon az eszközök látják egymást, és azt is, hogy a másik eszköz mit csinál, például adatokat tölt le, chatel vagy facebookozik. Megfelelő technikai feltételekkel és tudással pedig ártó szándékú emberek olvashatják és támadhatják a laptopunkat vagy telefonunkat. Ha lehet, ezért ne netezzünk például bevásárlóközpontokban vagy gyorséttermekben, vagy alaposan fontoljuk meg, hogy mire használjuk ilyenkor a gépünket! **Ugyancsak fontos szabály, hogy ha valami gyanúsnak tűnik, akkor az általában az is.** Érdemes résen lenni és nem kattintgatni mindenre, ami felugrik. Ha valamit nem értünk kérdezzünk, keressünk rá, nézzünk utána.