Biztonságosabb Internet Napja (Safer Internet Day)

Adatvédelem

Az alkalmazások letöltése előtt nézze át, hogy azok milyen adatokhoz kérnek hozzáférést! Kapcsolja ki az adatgyűjtő funkciókat (pl. helymeghatározás), amikor a program éppen nincs használatban! A felesleges alkalmazásokat távolítsa el eszközeiről, felhasználói fiókját törölje az applikációban!

Erős és egyedi jelszavakat használjon! Minden fiókhoz más kódot adjon meg! Kerülje a személyéhez köthető információk használatát!

Olyan vírusirtót használjon, amelynek van adathalászat elleni funkciója is!

Ha többen használnak egy számítógépet, mindenkinek legyen jelszóval védett, saját felhasználói fiókja! Használat után a böngészőből és számítógépből jelentkezzen ki!

Felhasználói nevet és jelszót csak tanúsítvánnyal (https előtaggal) rendelkező oldalon adjon meg!

Mindig ellenőrizze, hogy valóban a feladónak tűnő személy, illetve szervezet küldte-e az e-mailt! Nézze meg, hogy az e-mailcím @ utáni része helyesen tartalmazza-e a cégnevet!

Közösségi oldalak

Csak azt igazolja vissza ismerősként, akit valóban ismer. Ellenőrizze ismerőseinek listáját! Távolítsa el azokat, akiket valójában nem is ismer! Állítsa be, hogy csak az ismerősei láthassák posztjait!

Csak olyan tartalmakat tegyen közzé, amelyek a későbbiekben sem okozhatnak kellemetlenséget! Mellőzze az aktuális tartózkodási helyének beazonosítását lehetővé tevő információk megosztását! Az érintettek beleegyezése nélkül nem szabad fényképet közzétenni.

A legnépszerűbb közösségi oldalon, a Facebook-on a jelenlegi szabályozás szerint tizenhárom éves kortól lehet regisztrálni.

Internetes ismerkedés

Az interneten történő ismerkedés kockázattal járhat. Vannak, akik az anonimitást kihasználva valótlan, megtévesztésre alkalmas dolgokat állítanak magukról, és kedves szavakkal a beszélgetőpartner bizalmába férkőznek.

Intim kérdésekre ne válaszoljon, elérhetőségeit ne adja meg újdonsült ismerősének! Ha a partner rámenőssé, tolakodóvá válik, és ezáltal kényelmetlenül érzi magát, fejezze be a beszélgetést, és mentse le az üzenetváltást, vagy készítsen képernyőképet róla!

Kifejezetten jó benyomást keltő profilkép mögé bújó – magukat külföldi katonatisztnek, színésznek kiadó – férfiak gyakran próbálnak hölgyekkel ismerkedni a közösségi oldalakon. A bizalom kialakulását követően nagyobb pénzösszeg átutalását kérik a személyes találkozáshoz szükséges útiköltségre, vagy a közös élet megkezdéséhez szükséges válás rendezésére hivatkozva.

Az interneten keresztül megismert partnerrel történő találkozás különösen veszélyes lehet, ezért célszerű előtte elmondani egy családtagnak, rokonnak, ismerősnek, kivel, mikor, hol találkozik, illetve milyen internetes profillal rendelkezik újdonsült ismerőse. Amennyiben egy gyermek készül ilyen jellegű találkozóra, mindig kísérje el valaki!

Internetes vásárlások

Internetes apróhirdetés esetében gyanút kell, hogy keltsen a rendkívül kedvezőnek tűnő ár-érték arány.

Ilyen vásárlások esetében mindenképpen utánvétes fizetési módot célszerű választani.

Nagyobb terjedelmű termék (pl. mobilgarázs) megrendelése esetén az utánvétes fizetés biztonságot nyújthat, mivel az áru átvételkor könnyen leellenőrizhető, hogy rendben megtörtént-e a teljesítés.

Kisebb méretű cikk vásárlásakor az utánvétes fizetés sem jelent garanciát, hiszen a csomag tartalma csak a fizetést követően válik ismertté.

Online bankkártyás fizetés esetében győződjön meg arról, hogy valódi banki oldalon adja meg az adatait!

Az internetes apróhirdetések az eladók szempontjából is kockázatot jelentenek. Amennyiben a vevő egy népszerű csomagküldő szolgáltatás igénybevételével kívánja átvenni a megrendelt csomagot, és a tranzakció lebonyolításához egy linket is küld, ez rendkívüli óvatosságra kell, hogy intsen!

Ha hirdetőként ilyen linket kap, arra semmi esetre se kattintson rá!

Amennyiben mégis megnyitotta az oldalt, internetbankos felhasználónevét, jelszavát, illetve az sms-ben kapott kódot ezen a felületen sohase adja meg!

Banki tranzakció?!

Ha banki tranzakció ellenőrzésére, letiltására hivatkozva keresik, akkor is óvatossággal kezelje a hívást, ha a hívószám valós pénzintézeti telefonszámnak tűnik!

Minden esetben szakítsa meg a vonalat és hívja vissza bankjának központi telefonszámát!

Bankkártyájának adatait, illetve az sms-ben kapott kódot senkinek ne adja meg!

A pénzintézetek telefonon keresztül, e-mailben, sms-ben sohasem kérnek az internetbanki bejelentkezéshez és azonosításhoz szükséges jelszót, illetve PIN-kódot.

Telefonos kérésre sohase lépjen be internetbankjába, illetve pénzintézetének mobilalkalmazásába, ne módosítsa banki limitbeállítását!

A számítógépére, illetve a telefonjára idegen személy kérésére ne telepítsen semmilyen alkalmazást!

További információk a kiberpajzs.hu oldalon.

Vas Vármegyei Rendőr-főkapitányság Bűnmegelőzési Alosztálya