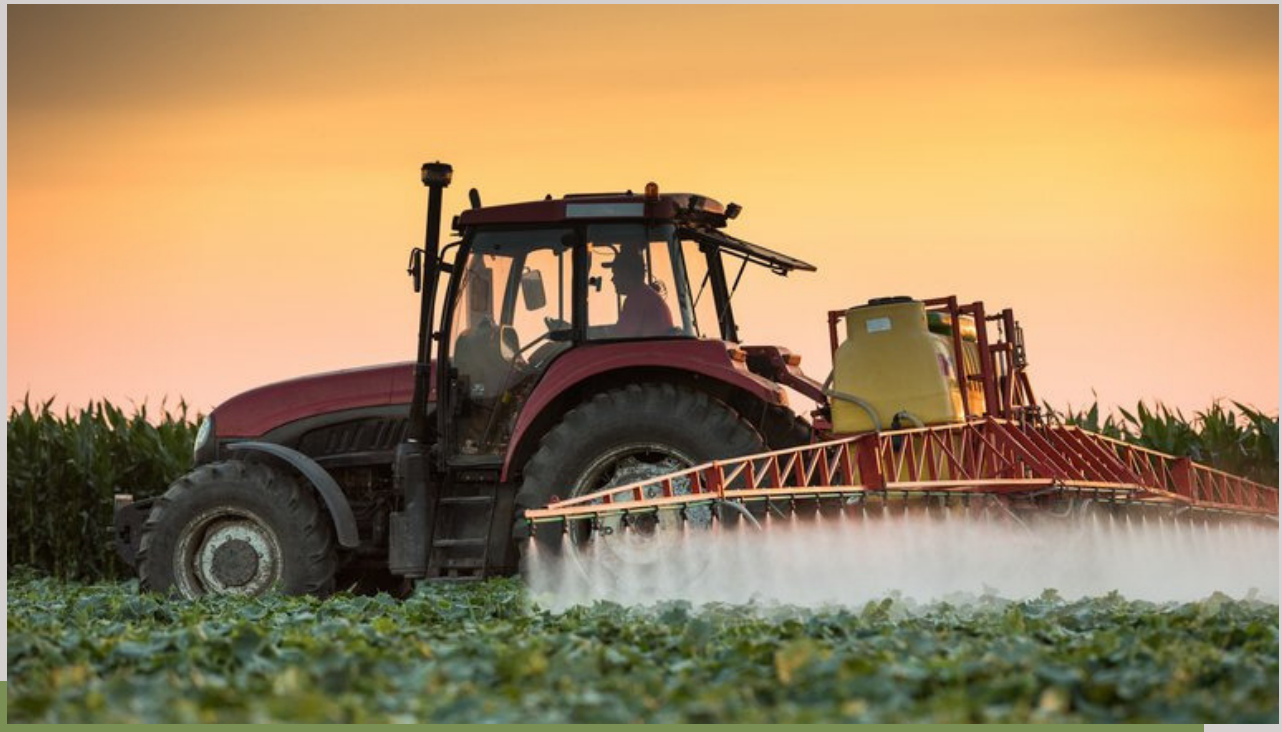
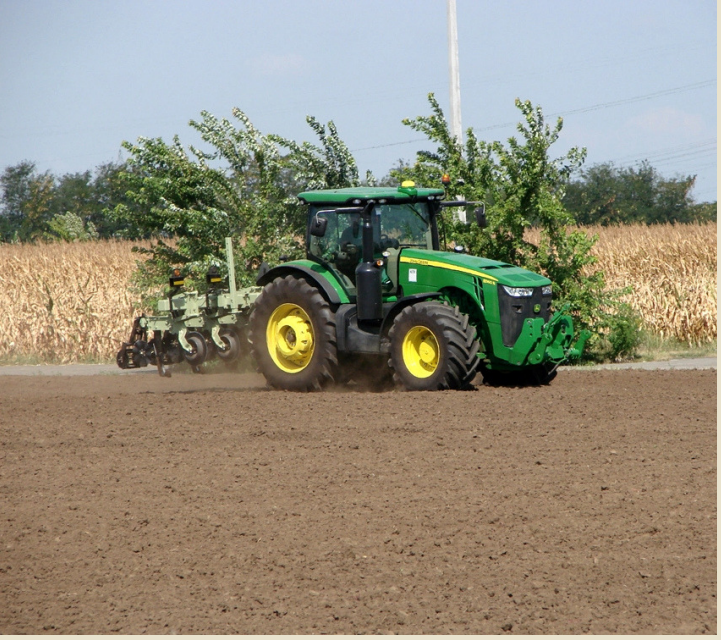


E L B I R

A Jász-Nagykun-Szolnok Megyei Rendőr-főkapitányság
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer
- február havi hírlevele -

V E G Y S Z E R L O P Á S O K M E G E L Ő Z É S E

B I Z T O N S Á G O S I N T E R N E T N A P

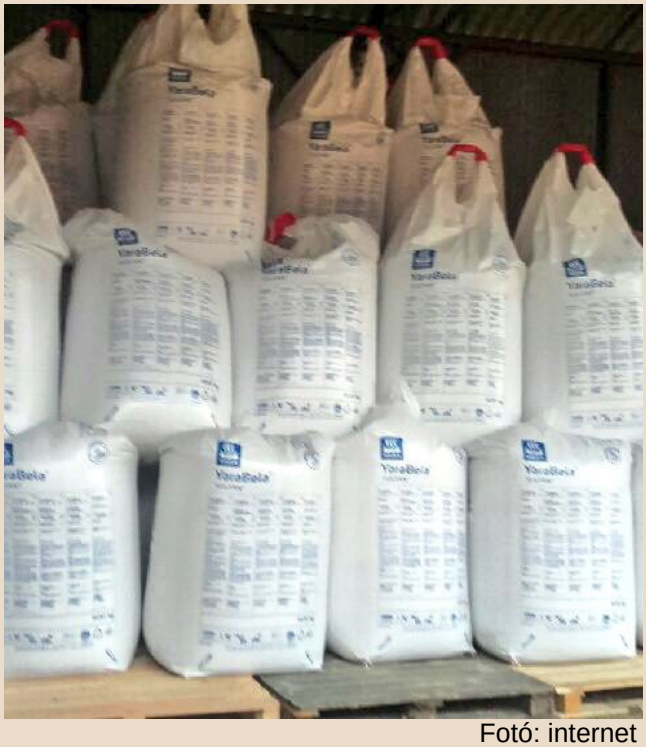


ELŐZZE MEG A VEGYSZERLOPÁSOKAT!

Hamarosan elkezdődnek a tavaszi mezőgazdasági munkálatok.
A vegyszerek tárolására szolgáló épületek állapotát, még az új vegyi anyagok beszerzése előtt át kell vizsgálni, mert ezek a tárolók bűncselekmények elkövetőinek célpontjává válhatnak!
A vegyszerlopások elkövetői több millió forintos kárt okozhatnak, hiszen ezen szerek beszerzési ára kis mennyiség esetén is igen magas.
FONTOS, hogy a vegyszerek beszerzésének időpontjáról, szállításáról, illetve a felhasználás idejéről csak megbízható személyt tájékoztasson!

Az áldozattá válás elkerülése érdekében fogadják meg tanácsainkat!

Elsődleges szempont a nyílászárók épsége, biztonságos zárhatósága.
Az ajtókra, ablakokra célszerű rácsokat felszerelni.
Az ajtókat biztonsági zárakkal, és törésbiztos lakattal kell ellátni.



Fotó: internet

Ajánlatos elektronikai védelmet is alkalmazni. A mozgás-, és törésérzékelőkkel felszerelt riasztók sok esetben visszatartják a betörőt szándékától. Ezek az eszközök hang- és fényjelzéssel riaszhatnak akár helyben vagy egy vagyonvédelmi szolgáltató távfelügyeleti központjában.
A riasztók azonban csak akkor tudnak védelmet nyújtani, ha működőképesek és használják őket. Hatékonyságuk rendszeres karbantartással biztosítható. A riasztó lehetőleg szabotázsvédett legyen (ha valaki megrongálja vagy a falról letépi esetleg a vezetéket elvágja azonnali riasztást fog eredményezni és közel 125dB hangerőn szirénázik).

Nagy mennyiségű és értékű vegyszerek tárolását nem ajánlott külterületen, lakott területektől távol megoldani. Amennyiben a tárolás más módon nem kivitelezhető, célszerű az épület őrzéséről vagyonvédelmi szolgáltató bevonásával gondoskodni.

Bűncselekmény észlelésekor értesítse a rendőrséget az ingyenesen hívható segélyhívó telefonszámok egyikén (107, 112)!

Biztonságos Internet nap

Safer Internet Day

A Biztonságos Internet Napot világszerte február második keddjén rendezik meg.
A program célja, hogy felhívja a figyelmet a veszélyekre és a megelőzés lehetőségeire.
A gyermekek és fiatalkorúak védelme az Internet káros tartalmával szemben egyre fontosabb, mert a gyermekek folyamatosan a digitális térben mozognak, ott élik a mindennapjaikat. Ugyanakkor a legtöbb fiatal tapasztalatlan, nem tudja, hogyan kell okosan, biztonsággal használni az internetet, és nincs tisztában, - a digitális térben - rájuk leselkedő veszélyekkel. A tudás hiánya együtt jár a kiszolgáltatottsággal, így elengedhetetlen, hogy minél korábban és minél többet halljanak a biztonságos netezésről.

Fontos tudnivalók

Internetfüggőség

Az internetfüggőség fokozatosan alakul ki. Először rövidebb ideig, majd egyre hosszabban foglalkoznak a nettel az érintettek. Végül a függőség állapotában az egyén számára "megszűnik a számítógépen kívüli világ". Az internetfüggőség tünetei sokszor nem az internetezőnek "tűnnek fel", hanem a környezetének. Az internetfüggők súlyosabb esetekben a munkahelyüket vesztik el, romlik az iskolai tanulmányi eredményük vagy éppen a kapcsolatukban lépnek fel problémák. Az érintettek saját elhatározásukból képtelenek csökkenteni az internethasználatot, amitől ha megfosztják őket, szinte elvonási tüneteik lesznek: idegessé, nyugtalanná, ingerlékennyé válnak. A számítógépes játékokat játszók körében felborulhat a napi életritmus: az evés, az alvás, a munkába járás, a tanulás teljesen rapszodikussá válhat.

Néhány tanács a függőség elkerülése érdekében:

- Töltsön több időt a barátokkal, családdal, akik elterelik a figyelmet a netezésről, és nem utolsó sorban meghallgatják a problémáit!
- Határozza meg előre, mennyi időt szeretne a számítógép előtt tölteni. Minden este azonos időben kapcsolja ki a gépet!
- Töltse mással a szabadidejét: hívjon át egy barátot, menjen el sportolni, koncertre, színházba, múzeumba, vagy hallgasson zenét, olvasson.
- Kérjen segítséget, ha szükséges!

Ingyenes wifiszolgáltatás veszélyei

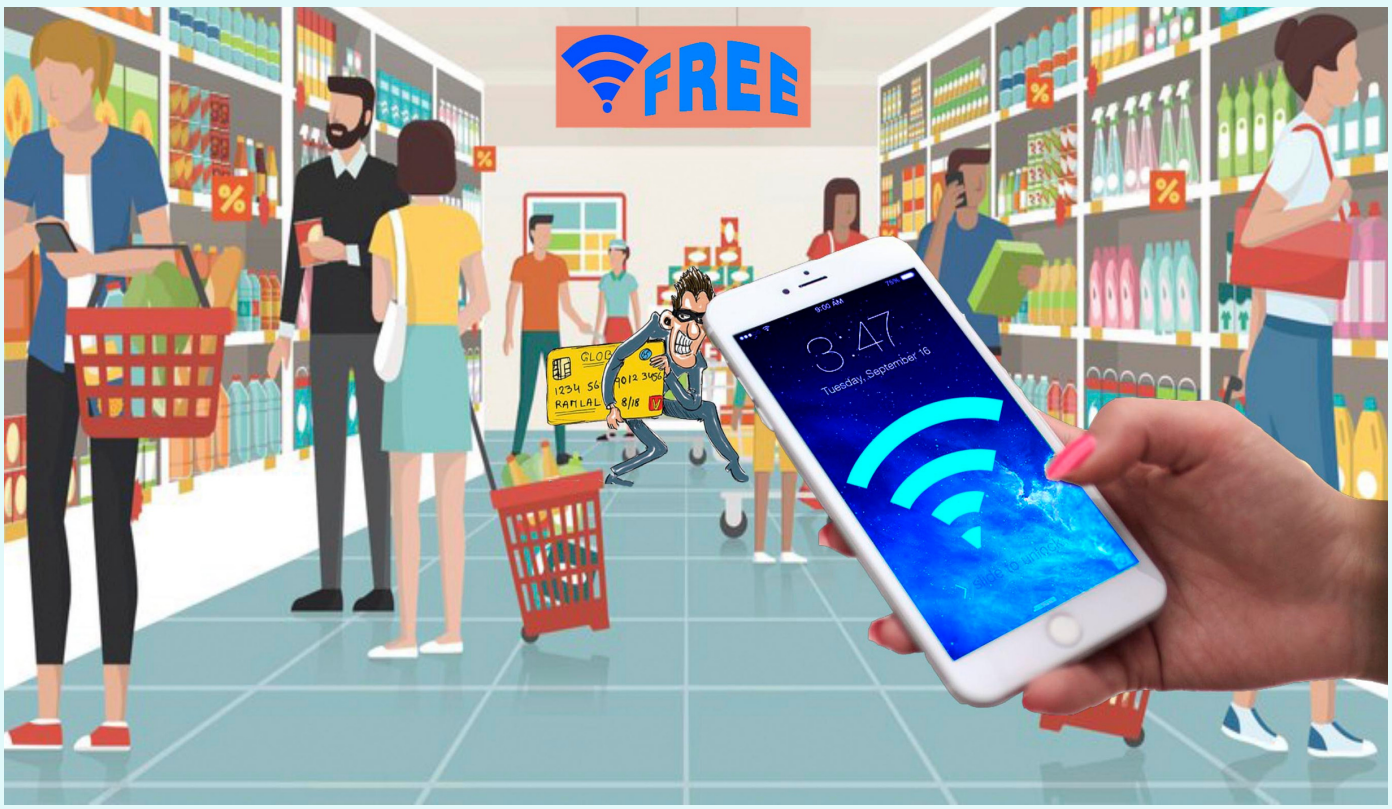
Ingyenes wifiszolgáltatás szinte már mindenhol elérhető, de ha felelőtlenül használják, annak súlyos ára lehet. Ingyenes, publikus wifihálózatra csatlakozáskor, a böngészés során megadott adatok nem titkosított csatornán közlekednek, ezért hatalmas veszélyben vannak, hiszen viszonylag egyszerűen rájöhet valaki, hogy az illető milyen honlapokat látogat, de belenézhet az üzenetekbe vagy megszerezheti a jelszavakat. Ezért alaposan meg kell gondolni, hogy hogyan és pontosan mire használja az ingyenes netezési lehetőséget!

Mielőtt nyilvános wifi hálózatra csatlakozik:

- Az eszközén kapcsolja ki a fájlmegosztó funkciót, hogy biztonságban legyenek a fájljai és dokumentumai!
- Csak a https:/ előtagú honlapokat nyissa meg!
- Kapcsolja be a tűzfalat, ha nem rendelkezik ilyennel, akkor minél hamarabb telepítsen az eszközére!
- Használjon antivírus szoftvert!
- Kapcsolja ki eszközén a publikus wifihálózatrokra történő automatikus kapcsolódást!

Az alábbiakat soha ne tegye, ha publikus wifire csatlakozik!

- Kerülje az online vásárlásokat és banki ügyintézéseket!
- Ne küldjön érzékeny információkat tartalmazó üzeneteket!
- Ne küldjön munkahelyi, bizalmas információkat a nyílt hálózaton!
- Ne frissítse eszközeit, hiszen sok esetben valódinak látszó, de igazából hamis frissítések ugorhatnak fel a képernyőn, amik telepítésével valójában rosszindulatú programok kerülhetnek az eszközeikre!

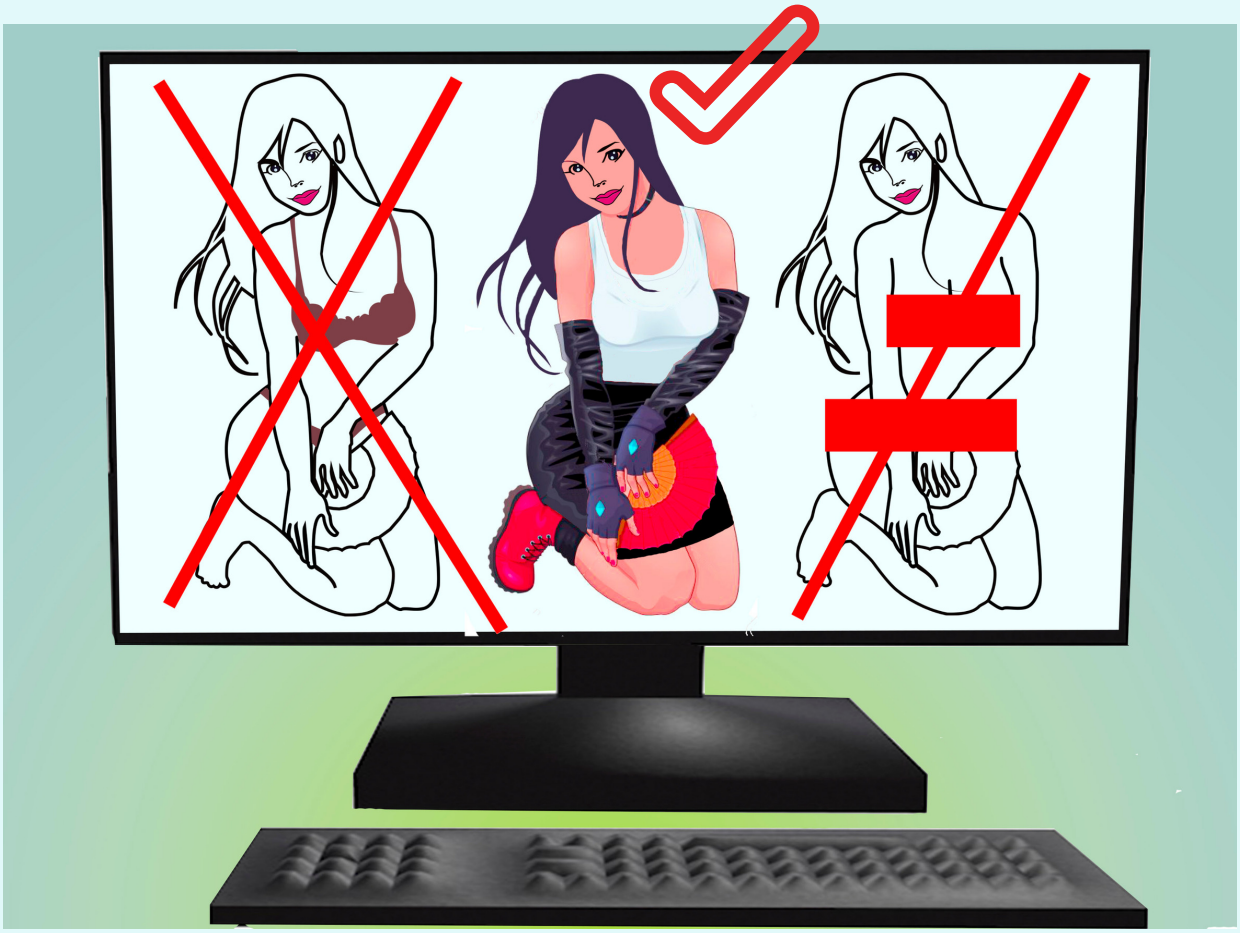


Mit takar a "szexting" szó?

A szó, az angol „szex” és „texting” szavak összeolvadásából keletkezett. Nem más, mint szexuális tartalmú, erotikus, meztelen vagy félig meztelen képek és videók küldése a mobiltelefonról a másik mobiljára vagy e-mail címére.

A szexting veszélyei

Az egyik legfontosabb tudnivaló a szexting veszélyeiről, hogy nincs arra garancia, hogy ezek a képek nem kerülnek illetéktelen kezekbe.



Tudatosítsa gyermekében, hogy erotikus tartalmú képeket soha senkinek ne küldjön, mert bárki bármikor visszaélhet vele, akár zsarolhatják is miatta! A meztelen fotó, akár örökké a neten keringhet, és súlyos következményei lehetnek, ha felismeri valamelyik családtag, barát, osztálytárs. Az ezzel járó szégyenérzet, illetve az állandó ugratások nehéz lelki terhet jelenthetnek az áldozatnak, és akár depressziót vagy öngyilkossági gondolatokat is okozhat!

Adathalászok

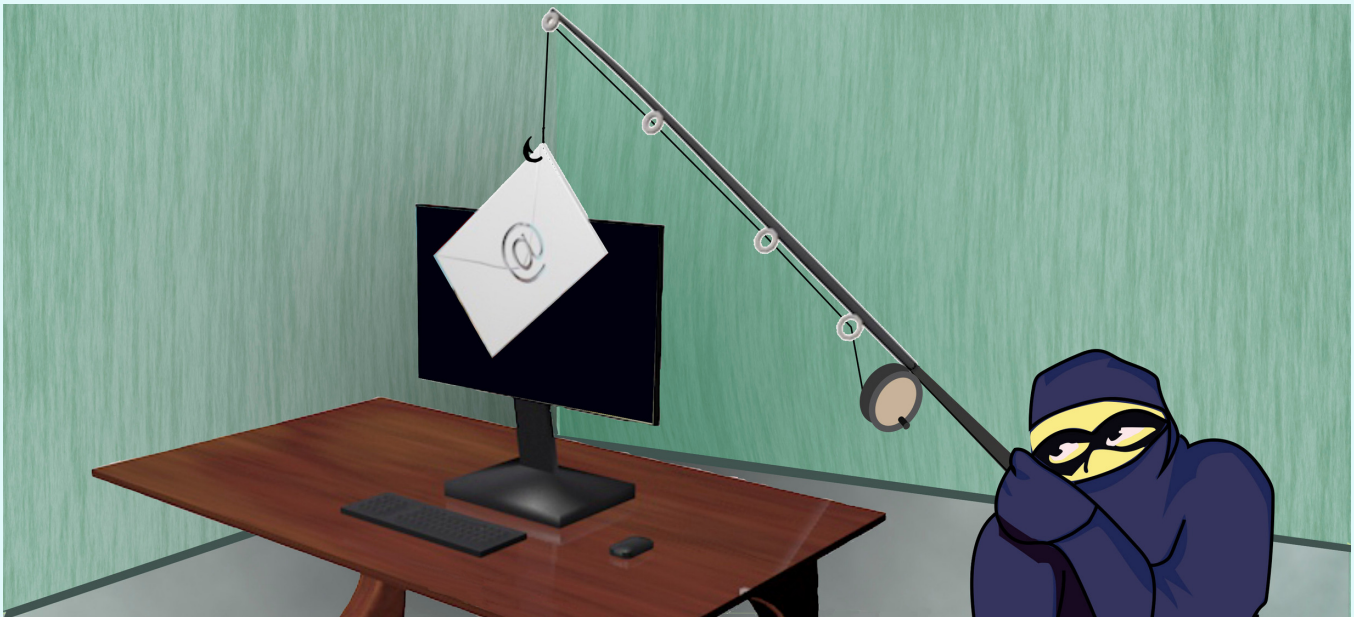
A csalók folyamatosan újabb és újabb módszerekkel, trükkökkel próbálkoznak, egyre ügyesebben próbálnak meg pénzt kicsalni áldozatuktól.
Újabban e-mailt küldenek a címzettnek, amiben ráveszik egy hivatkozásra való kattintásra. Gyakran tartozásra, vagy épp pénzvisszafizetésre utalnak levelükben. Arra kérik a felhasználót, hogy kattintson a levélben szereplő linkre, jelentkezzen be valamilyen megbízható cég (például: állami szervezetek, bankok, szolgáltatók stb.) honlapjához nagyon hasonlító weboldalra, amit azonban a csalók üzemeltetnek, és itt a megadott személyes és pénzügyi adatok hozzájuk kerülnek.

Hogyan ismerhető fel egy adathalász próbálkozása?

- Az áloldalak sokszor kinézetükben, szerkezetükben nagyon hasonlítanak az eredeti oldalhoz, más esetben azonban csak az adott cég arculati elemeit (színek, logók) alkalmazzák egyszerűsített formában.
- Ha az Ön által kapott e-mail tele van nyelvtani hibákkal – a ragozás helytelen, néha tegeződő, néha magázódó a szöveg - úgymond magyartalan, akkor az bizony, csalásra utaló jel.
- Ha egy olyan e-mailt kap valakitől, akit nem ismer, és egy weboldalra irányítja el, hogy ott jelentkezzen be, akkor legyen óvatos! Különösen akkor, ha ez a személy sürgeti Önt a jelszavának vagy bármilyen személyes adatának, kódszámának megadására!
- A levélben használt megszólítás általános, nem szerepel benne a címzett pontos neve.
- Az üzenetben kérik, hogy a megadott linken frissítse jelszavát.

Az áldozattá válás elkerülése érdekében fogadja meg tanácsainkat!

- Ellenőrizze figyelmesen a küldő e-mail címét! Gyakran egy betűnyi különbség húzódik meg a valós és a hamis címek között.
- Ne az e-mail fiókjából, ne a beérkezett üzenetből jelentkezzen be a szolgáltató, vagy szervezet oldalára!
- Ha kissé elbizonytalanodott, akkor ne nyissa meg az e-mailt és ne kattintson semmilyen hivatkozásra!
- Hívja fel a bankját, a szolgáltatót vagy a szervezetet, győződjön meg az e-mail tartalmának valódiságáról!
- Ne kattintson ismeretlen hivatkozásokra!
- Felhasználónevet és jelszót, csak tanúsítvánnyal rendelkező (https-előtagú) oldalon adjon meg!



Kérjük a szülőket, hogy gyermekeikkel ismertessék ajánlásainkat!

- Más által is használt számítógépen - ha befejezte az internet használatát - minden esetben jelentkezzen ki a közösségi oldalról, levelezéséből! A böngésző bezárása nem elegendő!
- Ne adjon meg senkinek személyes információt magáról (jelszavát, e-mail címét, lakcímét), amikor chetel vagy posztol!
- Közösségi oldalon ne legyen nyilvános a profilja, a személyes adatait, a megosztott tartalmakat csak az ismerősei láthassák!
- Válasszon biztonságos jelszót, ami nem kötődik hozzá!
- Ismeretlen eredetű szoftvereket ne telepítsen!
- Nem mindenki az, akinek mondja magát!
- Ha megfélemlítik, zaklatják, azonnal kérjen segítséget! A szülőkön, nevelőkön túl segítséget nyújtanak a DADA az ELLEN-SZER oktatók, és az iskolai bűnmegelőzési tanácsadók!
- Legyen óvatos a selfie készítésekor – a fotón ne látszódjon a család anyagi helyzete.
- Csak olyan fotót tegyen közzé, amit később nem bán meg!
- Engedély nélkül ne tegyen fel másokról fotókat!
- Amit az internetre felrak, az örökre ott is marad!
- Ne nyisson meg ismeretlen személytől érkező e-mailt, mert káros tartalmak lehetnek benne!

Drogprevenciós összekötő tisztek elérhetőségei

Jászberényi Rendőrkapitányság
Orosz Tibor c. r. főtörzszászlós 06-57-504-296

Karcagi Rendőrkapitányság
Fekete András r. főtörzszászlós 06-59-500-250

Kunszentmártoni Rendőrkapitányság
Jordán Katalin c. r. őrnagy 06-70-337-1657

Szolnoki Rendőrkapitányság
Mészáros János r. alezredes 06-20-464-2019

Tiszafüredi Rendőrkapitányság
Lányi Zsolt r. hadnagy 06-70-337-1655