

ELBIR

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer



Veszprém

Megyei

Rendőr-főkapitányság

2018.
JANUÁR



BIZTONSÁG



(2-3. old.)

**BIZTONSÁGOS
INTERNETHASZNÁLAT**

**A LAKÁSBETÖRÉS
MEGELŐZHETŐ**



(4. old.)

FŐKAPITÁNY AJÁNLÁSÁVAL

Kedves Olvasó!

Tisztelettel ajánlom a Veszprém Megyei Rendőr-főkapitányság Bűnmegelőzési Osztálya által szerkesztett, 2018. január havi bűnmegelőzési hírlevelet, amelyben az „Egy hónap – egy téma” kampány keretében felhívjuk a figyelmet és hasznos tanácsokat adunk az „adathalászattal” kapcsolatosan.

Hírlevelünk további részében pedig a betörések megelőzéséhez adunk hasznos tanácsokat, ajánlásokat.

Dr. Tarcsa Csaba r. dandártábornok
rendőrségi főtanácsos
megyei rendőrfőkapitány



EGY HÓNAP – EGY TÉMA ADATHALÁSZAT

Az egy hónap – egy téma a biztonságos internethasználatért kampány keretében ezen hírlevelünkben az adathalászcikkről lesz szó. A rendőrség új kampányában minden hónapban más-más témát érintő, a biztonságos internethasználatot elősegítő információs anyagot tesz közzé honlapján, a www.police.hu-n. Az Országos Rendőr-főkapitányság 2017 májusától indította el online kampányát. Az internet biztonságos használatával kapcsolatos témák közül minden hónapban az időszakra jellemző aktualitások szerint választják ki a hónap központi kérdését.



A rendőrség ebben a hónapban ahhoz ad tanácsot, mitévők legyünk, ha megtévesztő e-mailekben és üzenetekben próbálják meg személyes, illetve pénzügyi adatainkat megszerezni.

Személyes és pénzügyi adataink komoly értéket képviselnek. Ha ezek illetéktelen személyek számára hozzáférhetővé válnak, az komoly anyagi károkat is okozhat. A bűnözők megtévesztő e-mailek és közösségi oldalakon küldött üzenetek segítségével próbálnak meg hozzájutni a felhasználók adataihoz. Az üzeneteket nagyon sok embernek elküldik, bízva abban, hogy néhányan megadják az adataikat.

Az adathalászok jellemzően hamisított weboldalon keresztül próbálnak személyes és pénzügyi adatokhoz (tipikusan felhasználónév, jelszó, bankkártya adatok) jutni. Megbízható szervezetek, bankok, elektronikus kereskedelemmel foglalkozó weboldalak, online fizetési szolgáltatók ismertségét kihasználva, azok weboldalait lemásolva igyekeznek a felhasználók bizalmába férkőzni.

A csalók e-mailt vagy üzenetet küldenek a címzettnek, amiben ráveszik egy hivatkozásra való kattintásra. Arra kérik a felhasználót, hogy jelentkezzen be valamilyen megbízható cég (például: levelezési szolgáltató, bank stb.) honlapjához nagyon hasonló weboldalra, amit azonban a csalók üzemeltetnek, és itt a megadott személyes és pénzügyi adatok a hozzájuk kerülnek.

Árulkodó jelek – e-mailek, üzenetek

Bár az adathalász-üzenetek egyre kifinomultabbak, felismerhető, ha csalók küldték:

- a küldő e-mailcíme megtévesztésig hasonlít egy megbízható cég hivatalos e-mailcímére (például: a feladó címében o-betű helyett 0 szerepel)
- a cég hivatalos e-mailcíme helyett privát e-mailcímről érkezik
- olyan szolgáltató nevében küldték ki, akivel nem állunk kapcsolatban
- a levélben használt megszólítás általános, nem szerepel benne a címzett neve
- amennyiben a szöveg helyesírási hibákat tartalmaz, magyartalan, valószínű, hogy fordítóprogrammal készült
- bár a megadott link látszólag hasonlít az eredeti oldal címére, a kattintás után a címsorban teljesen más jelenik meg

Árulkodó jelek – adathalász-weboldalak

Az áloldalak sokszor kinézetükben, szerkezetükben nagyon hasonlítanak az eredeti oldalhoz, más esetben azonban csak az adott cég arculati elemeit (színek, logók) alkalmazzák egyszerűsített formában. Vannak olyan egyértelmű jelek, amelyek arra utalnak, hogy áloldalról van szó:

- A böngésző címsorában nem a cég hivatalos honlapjának hivatkozása szerepel.
- Az URL-címben https helyett http szerepel, vagyis az oldal nem rendelkezik tanúsítvánnyal és a felhasználó számítógépe, valamint az oldal közötti kommunikáció sem titkosított.
- A megbízható tanúsítvánnyal rendelkező oldalakat a böngészők általában jelzik (többnyire kis lakattal vagy zöld jelzéssel a böngésző címsorában).
- **Tipikus adathalászatra utaló üzenetek**
- Frissítse jelszavát az alábbi linken!
- Lépjön be a fiókjába, ellenkező esetben 24 órán belül törlődik!
- A mellékelt számla befizetéséhez az alábbi linken adja meg a bankkártyaadatokat!

Javaslatok

- **Mindig ellenőrizzük, hogy a feladó az, akinek kiadja magát!**
- **A bankok nem kérnek e-mailben bankkártya adatokat, más cégeknek pedig ne adjuk meg azokat!**
- **Online történő bankkártyás fizetésnél mindig győződjünk meg arról, hogy valóban egy bank által üzemeltetett oldalon adjuk-e meg az adatokat!**
- **Felhasználói nevet és jelszót csak tanúsítvánnyal rendelkező (https-előtagú) oldalon adjunk meg!**

A LAKÁSBETÖRÉS MEGELŐZHETŐ!

Egy lakás vagy családi ház biztonsága mindenki számára fontos, hiszen lakberendezési és egyéb vagyontárgyaink eszmei értékkel is bírnak, ráadásul senki sem szeretné, ha idegenek lépnék át kéretlenül lakása küszöbét. De vajon mindent megteszünk lakóhelyünk biztonsága érdekében? Nyugodtan hagyhatjuk el reggelente lakásunkat?

Napi rutinunk része, hogy mielőtt elindulnánk otthonról, amellett, hogy végiggondoljuk, kikapcsoltuk-e az elektromos berendezéseket vagy elzártuk-e a gáztűzhelyet, ellenőrizzük azt is, hogy becsuktuk-e az ablakokat. Miután gondosan bezártuk az ajtónkat is, már nyugodtan indítjuk a napot.

Sok esetben ez azonban nem elég, hiszen a nyílászárók gondos zárása mellett azok minősége és betörésbiztonsága is fontos szempont. előírások teljesülése és megléte.

Kulcs a biztonsághoz – milyen a jó zár?

A legtöbb bejárati ajtóban hengerzár-betéteket alkalmaznak, így ez a zártípus a legelterjedtebb. „A hengerzárak szerkezetében a legsérülékenyebb rész a betét könnyített része, amelynek eltörésével a betörők könnyedén be tudnak jutni a lakásba. Éppen ezért fontos, hogy úgy alakítsuk ki a zárbetét elhelyezését, hogy az ne álljon ki az ajtólap síkjából, így ne tudják egyszerűen, egy mozdulattal kitörni a betétet. Általános tapasztalat, hogy a lebukás veszélye miatt a betörők öt perc után feladják a behatolási kísérletet, ne könnyítsük meg a dolgukat.



Annak érdekében, hogy elkerüljük a betörést, érdemes egy törésmentes, minőségi gyártó által készített, 7-8 milliméter vastagságú alumínium öntvény címkét szerelni a bejárati ajtóra, amely a belső sík felől átmenő csavarokkal rögzíthető. Így a betét a címke síkjából nem áll ki, nem lehet eltörni. A korszerű, mai gyári ajtók már rendelkeznek ilyen betéttel, betétvédelemmel, címke kialakítással, így a zárszerkezet elhelyezése is megfelelő, ezért ezek az ajtók alapvetően megfelelnek ennek a biztonsági védelemnek. Érdemes ügyelni arra is, hogy a betörők néhány esetben a betét kifúrásával jutnak be a lakásba, így érdemes olyan zárbetétet vásárolni, mely fúrásmentes kivitelű. A zárszaküzletekben vásárlás előtt érdemes rákérdezni erre.

A Veszprém Megyei Rendőr-főkapitányság szakemberei a „Házhoz megyünk!” országos bűnmegelőzési program keretében igény esetén elvégzik az ingatlanok biztonsági auditját, és javaslatokat tesznek az esetlegesen meglévő hiányosságok kiküszöbölésére.

Amennyiben bűncselekmény áldozatává vált, kérjük, jelentse be az ingyenesen hívható 107, vagy a 112 központi telefonszámok valamelyikén.

Bármely információkéréssel kapcsolatban forduljon hozzánk bizalommal az impresszumban található elérhetőségeken:

Hozzájárulásunkat adjuk ahhoz, hogy Kedves Olvasóink a Hírlevél tartalmát részben vagy egészben szabadon felhasználják, a célcsoportok felé eljuttassák.

Kérjük azonban, hogy a terjesztés során hivatkozzanak arra, hogy a Hírlevelet a Veszprém Megyei Rendőr-főkapitányság Bűnmegelőzési Osztálya készítette.

IMPRESSZUM

Kiadja: a Veszprém Megyei Rendőr-főkapitányság
Bűnügyi Igazgatóság Bűnmegelőzési Osztálya
Telefon / fax: 06-88/ 544-683

E-mail: futtaton@veszprem.police.hu

Kiadásért felel: Dr. Tarcsa Csaba r. dandártábornok, rendőrfőkapitány

