ELBIR
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

Az ÜGYFÉLKAPU biztonságos használata

Biztonságtudat

MAGYARORSZÁG.HU Kormányzati Portál

A reális biztonságtudat első feltétele, hogy tisztában legyenek az Önök által kezelt adatok fontosságával, és a bűnözők általi visszaélés lehetőségeivel.

A veszély nem ismerete hamis biztonságtudatot ébresztheti, ám a baj bekövetkeztekor pánik jelentkezhet. Az Internet minden használójának – így a kormányzati elektronikus ügyintézéssel kapcsolatos szolgáltatások igénybevevőjének is – a rendszer használatakor tudomással kell bírnia az internetes kapcsolat biztonságtechnikai és egyéb veszélyeiről.

Jelen dokumentumban az oldal üzemeltetői szeretnék felhívni a figyelmet szolgáltatásaik biztonságos, körültekintő használatára. A kormányzati elektronikus ügyintézés szolgáltatás igénybevételével kapcsolatban számos védelmi intézkedést megvalósítottak, amelyek az Önök biztonságát szolgálják. Emellett azonban az Önök közreműködésére is feltétlenül szükség van ahhoz, hogy a rendszer használatából eredő kockázatot minimálisra tudják csökkenteni.

Adatvédelem

Kérjük, olvassák el a honlapon a meghatározást a személyes adatokvédelemmel kapcsolatos politikáról és a mindennapos gyakorlatot a szolgáltatások bemutatásáról, mely során a látogatóktól személyes adatokat kérnek, nyilatkoznak arról, hogy milyen célokra, és hogyan használják fel az ilyen jellegű adatokat, hogyan biztosítják a személyes adatok megőrzését és védelmét.

A számítógép védelme

A portál üzemeltetői javasolják, hogy az Ügyfél a szolgáltatás igénybevételekor és általában az Internet használatakor a számítógépe védelme érdekében a lehető legnagyobb gondossággal járjon el; a vírusfertőzésekkel, betörési kísérletekkel szemben védjék számítógépét tűzfalakkal, víruskeresőkkel. A vírusok károsíthatják számítógépüket, tönkretehetik tárolt adataikat, és nem kizárt, hogy bizalmas adatokat, a használat során alkalmazott kódokat illetéktelenek részére juttatják el, amelyekkel vissza is élhetnek.

Bármely Internetről letölthető szoftver tartalmazhat vírust. Egy email is tartalmazhat olyan csatolmányt, mely vírusos. Győződjenek meg arról, hogy van vírusellenőrző a számítógépén, amely a csatolmányokat is szűri. Napról napra újabb vírusok születnek, ezért érdemes a legújabb verziót használni, naponta frissíteni a vírusdefiníciókat. Amint új vírusokat fejlesztenek, új megoldásokat kell találni eltávolításukra.

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, Mobil:: +3620/560-5146
e-mail: elbir@bacs.police.hu web: http://www.police.hu/hirek-es-informaciok/bunmegelozes

Amikor Önök hatásos biztonsági védelem nélkül lépnek ki az Internetre, behatolhatnak az Önök számítógépébe illegálisan, az Önök tudta nélkül is. Az Interneten folyamatosan elérhetők és ingyenesen letölthetők díjmentesen használható tűzfalak, melyek megfelelő vélelmet nyújtanak a behatolók, DoS-támadások, kíváncsiskodó spyware programok, trójai programok ellen.

A magasabb szintű biztonság elérése érdekében javasolják a rendszeres letöltést az Önök által használt operációs rendszerhez, böngészőhöz elérhető biztonsági frissítéseket, javító verziókat, és az alkalmazott böngésző adatbiztonsági beállításainak a szükséges legnagyobb biztonságot garantáló szintre beállítását. Ebben az esetben a program figyelmeztet a böngésző használata során potenciálisan kárt okozó tartalom megnyitása előtt. A biztonság tovább növelhető, amennyiben leállítják a számítógépén futó nem szükséges alkalmazásokat.

Felhasználói azonosító és jelszó kezelése

Az Önök azonosítása a rendszerben felhasználói azonosítóval és jelszó segítségével történik, ezért fontos, hogy ezt a két érzékeny adatot senki más számára ne tegyék megismerhetővé.

Jelszavukat megbízható ismerősnek se árulják el! A szolgáltatáshoz érvényes jelszót sem a hatóságok, sem munkatársak nem kérhetik Önöktől!
Igyekezzenek megjegyezni jelszavakat! A legjobb, ha egyáltalán nem írják le. Ha mégis ezt teszik, akkor:

- se legyen nyilvánvaló, hogy mire használatos a leírt karaktersor,
- tárolják biztonságos helyen.

A rendszer a jelenleg hatályos törvényi szabályozásoknak megfelelően nem kényszeríti ki a nagy rendszerességgel történő jelszóváltoztatást, de javasoljuk, hogy jelszavát a minél nagyobb biztonság elérése érdekében rendszeresen, legalább egy-két havonta változtassa meg.

A szolgáltatás nyilvános helyen való használata

Lehetőség szerint tartózkodjanak a kormányzati elektronikus ügyintézés mások jelenlétében, vagy nyilvános helyen (pl. Internet kávézó, munkahelyen többek által közösen használt gép, stb.) történő használatától.
Amennyiben mégis így veszik igénybe szolgáltatást, a rendszerben megvalósított védelmi intézkedések mellett szükség van az Önök közreműködésére. Ebben az esetben – ha fennáll a lehetősége, hogy mások is hozzáférnek az Önök által használt számítógéphez – az alábbi biztonsági lépéseket javasolt végrehajtani:

- A szolgáltatás Bejelentkezés funkciója lehetőséget biztosít a kijelentkezésig a titkos jelszó egyszeri megadására a tranzakciós, illetve a lekérdezés képernyőkön. Fontos! Ha nyilvános helyen használják az internetes szolgáltatást, ezen kényelmi funkció igénybevételét nem javasolják, minden esetben a tranzakciónkénti azonosítás szükséges.

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, Mobil:: +3620/560-5146
e-mail: elbir@bacs.police.hu web: http://www.police.hu/hirek-es-informaciok/bunmegelozes

- A HTML technológiából adódó sajátosságok miatt a felhasználó által látogatott oldalak tárolásra kerülnek a számítógép Temporary Internet Files (ideiglenes internetfájlok) könyvtárában. A böngészők alapértelmezés szerinti beállítása mellett ez minden HTML alapú internetes oldal esetében, így a kormányzati elektronikus ügyintézés internetes szolgáltatás használatakor is megtörténik. Amennyiben Önök a szolgáltatást nem saját gépen veszik igénybe, a böngészőben ne engedélyezzék az ideiglenes internet fájlok tárolását.

Ügyeljenek arra, hogy senki se lássa a jelszót és a kódot, semmilyen körülmények között ne hozzák nyilvánosságra azokat. Amennyiben úgy érzik, hogy illetéktelen személyek megtudták jelszavukat, változtassák meg az ügyfélkapu rendszeren keresztül. Ne hagyják soha sem őrizetlenül azt a számítógépet, ahol az éppen ügyintézési folyamat történik!

A szolgáltatás használatának befejezése

Fontos, hogy a szolgáltatást minden esetben a KILÉPÉS gomb alkalmazásával, ne pedig a böngésző ablak bezárásával (X-gomb megnyomása) hagyják el! Ez esetben a bejelentkezéskor létrehozott titkosított kapcsolat véglegesen megszakításra kerül.
Amennyiben Önök a szolgáltatást mások jelenlétében, vagy nyilvános helyen használták, és a bejelentkezés során engedélyezték az Ideiglenes internet file-ok tárolását, a Kilépést követően töröljék a böngészőben az Ideiglenes internet file-ok könyvtár tartalmát. A törlés a különböző böngészők esetében máshogy történik, a leggyakrabban használt böngészők esetében ennek módja a következő:

- Internet Explorer: Eszközök (Tools) / Internet beállítások (Internet options) oldalon Ideiglenes Internet file-ok (Temporary Internet files) File-ok törlése (Delete files) opciót választva.
- Netscape: Edit / Preferences oldalon Advanced / Cache opciót választva Clear Memory Cache és Clear Disk Cache funkcióval.
- Opera 6.05: File / Preferences oldalon History and Cache opciót választva Disc cache Empty now funkcióval.
- Mozilla 1.3: Edit / Preferences oldalon Advanced / Cache opciót választva Clear Cache funkcióval.

Ha a szolgáltatást az Önök ellenőrzése alatt álló számítógépről veszik igénybe, az említett biztonsági lépések alkalmazása nem feltétlenül indokolt, de mindenképpen ajánlott.

Social engineering

A social engineering az emberek természetes, bizalomra való hajlamának kihasználása. Hackerek vagy akár egyszerűen rossz szándékú emberek is gyakran használják ezt a módszert a számítógépekhez való illetéktelen hozzáférésre és információk megszerzésére.A social engineering nem a hardver, a szoftver vagy a hálózat hibáit, hanem az emberi természet gyengeségeit használja ki a számítógépek feltörésére. Alkalmazásával bárki, aki csak minimális hackelési képességekkel is rendelkezik, behatolhat egy biztonságosnak tartott rendszerbe, majd hozzáférhet, módosíthatja vagy akár törölheti az ott tárolt adatokat.

A legjellemzőbb ilyen jellegű bűncselekmények körébe az "adathalászat" tartozik, amelynél a csalók különböző **eszközökkel** (például telefonhívás, e-mail) ráveszik a gyanútlan felhasználót, hogy árulja el jelszavát, adjon meg bizalmas adatokat, illetve számítógépén töltsön le, indítson

el kormányzati elektronikus ügyintézésnek látszó alkalmazást az elektronikus üzenetben kapott link segítségével.
A billentyűzetet figyelő programok láthatatlanul regisztrálják, hogyan használják a klaviatúrát, milyen banki jelszavakat, kódokat ütnek be. E figyelőprogramok észrevétlenül bejuthatnak a személyi számítógépekbe, ami azonban nem jelent teljesen védtelenséget. A kockázat teljes megszüntetése nem lehetséges, de jelentősen csökkenthető az alábbi tanácsok betartásával:

• Soha ne válaszoljanak kormányzati elektronikus ügyintézéssel kapcsolatos e-mailekre! Soha nem kérnek bizalmas adatokat e-mail útján, és nem szüntetik meg valakinek a hozzáférését azért, mert nem ad meg ilyen adatokat e-mailen!

• Soha ne nyissanak meg elektronikus levélben található mellékletet, mielőtt nem vizsgálták át alaposan vírus- és kémirtó program segítségével!

• Telefonos megkereséskor soha ne adjanak meg bizalmas információkat! Előfordulhat, hogy telefonon megkeresik Önöket, azzal, hogy bizalmas adatokat szeretnének kapni, hivatkozhatnak jelszócserére, karbantartásra, stb. A személyes hozzáféréshez tartozó jelszót csak Önöknek szabad tudni. A rendszergazdáknak, karbantartó technikusoknak nincs szüksége a jelszavukra, hiszen rendelkeznek saját azonosítóval, ami olyan rendszerjogokat biztosít számukra, mellyel az Önök jelszava nélkül is mindent el tudnak intézni. Ha egy rendszergazda a jelszavuk után érdeklődik, legyenek gyanakvók! Semmi esetre se adják meg a felhasználó-nevét és jelszavát!

• Keltsen Önökben gyanút, amennyiben olyan e-mailt vagy telefonhívást kapnak, melyben tájékoztatják, hogy a kormányzati elektronikus ügyintézés szolgáltatáshoz használt adatait illetéktelenek megszerezték, és arra kérik, hogy vegyék fel ügyfélszolgálattal a kapcsolatot a megadott telefonszámon. Ezt sose tegyék. Haladéktalanul értesítsék az oldal üzemeltetőjét az ugyfelkapu@magyarorszag.hu e-mail címen, vagy a 06-40-200-195-ös kékszámon.

• A telefonos adatlopás ellen kellő óvatossággal, az elektronikus adatlopás ellen a legfrissebb vírusirtó, tűzfal és anti-kém programok együttes alkalmazásával és azok folyamatos frissítésével védekezhetnek a legjobban. Mindez azonban csak akkor segít, ha az operációs rendszert is naponta frissítik, és lehetőség szerint kikapcsolják a nem kívánt szolgáltatásokat.

• A kormányzati elektronikus ügyintézést csak kizárólagosan, más oldalakat nem látogatva, a címet mindig a böngészőbe beleírva, vagy a "Kedvencek" menüpontból használják, sohasem elektronikus levélből. Utóbbiakban a bűnelkövetők esetenként olyan internet-címeket adnak meg, amelyek alig térnek el a valós címtől, ezért megtévesztők. A kormányzati elektronikus ügyintézéshez kapcsolódás előtt célszerű egy friss vírus- és kémirtó programot elindítani.

A szolgáltatás használata során – a bejelentkezést megelőzően – győződjenek meg arról, hogy számítógépük a megfelelő szerverrel kommunikál! A honlap címe: http://www.magyarorszag.hu .

Mielőtt bármilyen érzékeny adatot adnának ki magukról, győződjenek meg arról, hogy az internetes kapcsolata biztonságos, a cím https-sel kezdődik, melyet a böngésző jobb alsó részen megjelenő kis lakat is jelzi.

Forrás: https://magyarorszag.hu/informacio/biztonsagtudat.html

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, Mobil:: +3620/560-5146
e-mail: *elbir@bacs.police.hu* web: *http://www.police.hu/hirek-es-informaciok/bunmegelozes*