OUCH! 2024. február

OUCH!

SANS SECURITY AWARENESS

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Személyazonosság-lopás: megelőzés, detektálás és reagálás

Áttekintés

A mai digitális világban, személyes adatai értékesebbek, mint valaha. Sajnálatos módon, emiatt elsődleges célpontja lett a személyazonosság-lopásnak. Alapvető eleme az online digitális életnek ennek a fenyegetésnek a megértése, észlelése és annak ismerete, hogyan védheti meg magát.

Mi az a személyazonosság-lopás?

Személyazonosság-lopásról akkor beszélünk, ha valaki illegálisan megszerzi az Ön személyes adatait – például a nevét, azonosítószámait, társadalombiztosítási vagy útlevélszámát, hitelkártyaadatokat – csalás vagy más bűncselekmény elkövetése céljából. A leggyakoribb formája a személyazonosság-lopásnak a pénzügyi személyazonosság-lopás, ahol adatait pénzügyi csalásra használják. Például ellopják a személyazonosságát, és hitelkártyát, jelzálog- vagy autókölcsönt íratnak a nevére, aminek számláit később Önnek kell kifizetnie. Azonban több fajta személyazonosság-lopás létezik. Például az egészségügyi személyazonosság-lopás, ahol az Ön egészségügyi adatait lopják el és egészségügyi biztosításokat vesznek fel a nevében olyan orvosi ellátásokért, amikben Ön soha nem részesült. Másik az adóügyi személyazonosság-lopás, ahol a csalást elkövető személy felhasználja az Ön adóazonosító számát, hogy adó-visszatérítést kezdeményezzen az Ön nevében. Ennek következtében Ön már nem fog tudni adó-visszafizetést kezdeményezni, mert valaki más ezt már megtette az Ön nevében.

Megelőző intézkedések

Mit tehet a védelme érdekében? Sajnálatos módon ez nem olyan egyszerű, mint amilyennek hangzik mivel sok szervezet már alapból rendelkezik az Ön adataival és rajtuk múlik, hogy megvédik-e. Van azonban néhány kulcsfontosságú lépés, amelyet megtehet.

- **Erős jelszavak**: Az egyik leghatékonyabb módja annak, hogy megvédje magát, ha minden fiókját egyedi és hosszú jelszóval védi, és amikor lehetséges, engedélyezi a többlépcsős hitelesítést.
- **Rendszeres szoftverfrissítések**: Győződjön meg arról, hogy eszközei a legújabb biztonsági javításokkal és funkciókkal rendelkeznek. Ennek érdekében engedélyezze az automatikus frissítést minden eszközén**.**
- **Bankkártyák**: Hitelkártya helyett használjon bankkártyákat az online vásárlásokhoz, mivel a bankkártyák jóval több védelmet biztosítanak a csalások ellen. Még egy megoldás lehet külön kártyákat használni az online és a személyes vásárlásokhoz. Néhány szolgáltató virtuális egyszeri használatos bankkártyát is biztosít az online vásárláshoz.
- **Hitelkártya:** befagyasztás: A hitelkártya befagyasztása zárolja a hiteljelentését, megakadályozva a csalókat abban, hogy új számlákat nyissanak az Ön nevében. Ezt ingyenesen megteheti, ha kapcsolatba lép a főbb hitelintézetekkel. Ez a szolgáltatás nem biztos, hogy minden országban elérhető.

Személyazonosság-lopás

A leghatékonyabb módja a védekezésnek a korai felismerés. Minél hamarabb észre tudja venni, hogy a személyazonosságával visszaélnek, annál előbb tud cselekedni. Néhány nagyon gyakori példa:

- **Szokatlan pénzügyi tranzakciók:** Rendszeresen ellenőrizze bank és- hitelkártya-kivonatait. Olyan terheléseket vagy utalásokat keressen, amelyekről tudja hogy nem Ön hajtotta végre. A legjobb módja ennek, ha bekapcsolja az automatikus értesítéseket. Így azonnal értesítést fog kapni, ha terhelés vagy változás történik a hitelkártyáján vagy folyószámláján.
- **Szabálytalan hiteljelentések**: Tekintse át évente hiteljelentéseit és közben keresse a gyanús tevékenységet. Keressen olyan új kölcsönöket, amelyek az Ön nevére szólnak és tudja, hogy nem Ön nyújtotta be, vagy keressen bármilyen jelentős változást a hitelminősítésében.
- **Titokzatos számlák vagy értesítések**: Legyen óvatos, ha olyan tételekről, szolgáltatásokról kap számlákat vagy díjbekérőket, amelyekről tudja, hogy soha nem vásárolta meg.
- **Váratlan elutasítások**: Ha váratlanul megtagadják az adó-visszatérítését, jóváírását vagy hitelkérelmét, akkor nézzen utána, hogy miért.

Személyazonosság-lopásra való reagálás

Ha úgy véli személyazonosságát ellopták, azonnal cselekedjen.

- **Azonnali jelentés**: Azonnal jelentse az esetet, amennyiben incidenst vélt felfedezni. Például amennyiben csalárd tevékenységet észlel bankszámláján vagy hitelkártyáján, lépjen kapcsolatba bankjával. Ugyanakkor tegyen feljelentést a helyi rendvédelmi szerveknél. Ez fontos lehet a bűncselekmény bizonyítása, költségek behajtása vagy a biztosítási igények benyújtása szempontjából.
- **Csalással kapcsolatos riasztások és bankszámla fagyasztások**: Helyezzen el csalási riasztást a hiteljelentéseire, és fontolja meg a hitelkártya befagyasztását, ha még nem tette meg. Emellett segítse a hitelintézetek munkáját a csaló információk eltávolítása érdekében.
- **Dokumentáljon mindent**: Amikor a helyreállítás érdekében felhívja az érintett szervezeteket, ügyeljen arra, hogy részletes feljegyzéseket vezessen a kommunikációjáról, a megtett lépésekről, beleértve azt is, hogy kivel, mikor és miről beszélt.
- **Jelszóváltoztatás**: Minden kulcsfontosságú fiókjában változtassa meg jelszavát. Amennyiben nem rendelkezik jelszókezelővel az összes új jelszava nyomonkövetésére, fontolja meg annak beszerzését.

Következtetés

Nagyban csökkenti az áldozattá válás kockázatát, amennyiben megérti a személyazonosság-lopás lényegét és alkalmazza a felsorolt intézkedéseket.

Források

Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
Mobileszközök biztonságos használata: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
A hitel befagyasztás: https://www.usa.gov/credit
Azonosítólopások bejelentése: https://www.identitytheft.gov

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)