OUCH! 2026. augusztus

Az Ön Havi Biztonsági Tudatosságról Szóló hírlevele

Értesítés adatszivárgásról? Ne essünk kétségbe - vegyük át az irányítást!

Egy e-mail, ami mindent megváltoztatott

Justin éppen befejezte vacsoráját, amikor e-mailt kapott attól a szervíztől, ahol nemrégiben autójának motorját szerelték. Az e-mail tárgya a következő volt:

"Fontos biztonsági értesítés a felhasználói fiókjáról"

Először majdnem kitörölte, mert azt gondolta, ez megint valami átverés. De a kíváncsisága erősebb volt. Az e-mailben azt írták, hogy az autószervíznél adatszivárgás történt, amelynek során kiszivárogtak az ügyfelek adatai, beleértve a neveket, e-mail címeket, lakcímeket és telefonszámokat is. A jó hír pedig az volt, hogy a bankkártya adatokat nem érintette a támadás. Ebben az időszakban Justin elfoglalt volt, szóval nem is foglalkozott különösebben az emaillel.

Eltelt néhány nap. Ezt követően Justin egyre több különös e-mailt kezdett kapni az autószerviztől, amelyekben több, már lejárt és továbbra is kiegyenlítetlen számlára hívták fel a figyelmét. Az üzenetekben megfenyegették, hogy börtönbe kell vonulnia, ha nem törleszti a tartozását azonnal. Az e-mailek valódnak tűntek, mivel nem csak a vállalat logója volt rajtuk, hanem a nevét, telefonszámát és lakcímét is tudták. Justin pánikba esett, és befizette a számlát. Az eset után több hét telt el, mire Justin egy barátjával történő beszélgetés során rájött, hogy csalás áldozatává vált. A számlák nem voltak legitimek - adathalász e-mailek voltak, amiket a kiberbűnözők hoztak létre olyan információkból, amelyeket elloptak a meghackelt autószervíztől. Justin személyes információit felhasználva a támadóknak sikerült egy valósághű támadást lebonyolítaniuk. Sajnos Justin története egyre gyakoribbá válik.

Mi az az adatszivárgás?

Az adatszivárgás egy azokra az esetekre utaló kifejezés, amely során egy szervezet által tárolt személyes adatok véletlenül nyilvánosságra kerülnek, vagy a kiberbűnözők ellopják azokat. Néhány esetben ezeket a szervezeteket a jog arra kötelezi, hogy értesítsenek minden olyan ügyfelet vagy partnert, akinek az adatai érintettek lehetnek a támadásban. És itt a kérdés: mit kell csinálnunk, ha értesítést kapunk?

Mit csináljunk, ha ilyen értesítést kapunk?

A jó hír az, hogy egy ilyen szivárgás nem jelenti automatikusan, hogy áldozattá válunk. Az számít a legjobban, hogy miként reagálunk rá.

1. **Azonnal változtassuk meg a jelszavunkat!** Ha van felhasználói fiókunk egy érintett szervezetnél, változtassuk meg jelszavunkat! Ami még ennél is fontosabb, ha ugyan azt a jelszót több helyen is felhasználtuk, minden fiók esetében cselekedjünk így. Minden fiókunknak egyedi jelszóval kell rendelkeznie. Így, ha egy fiók azonosítói ki is szivárognak, az ellopott jelszót nem tudják felhasználni arra, hogy a többi fiókunkhoz is hozzáférjenek.

Az online csalók tudják, hogy az emberek gyakran újra felhasználják a jelszavaikat, így gyakran megpróbálnak más oldalakon is hozzáférni fiókjainkhoz. Az egyedi jelszavaink tárolásának legegyszerűbb módja egy jelszómenedzser használata, amely képes jelszavakat létrehozni, tárolni, és a megfelelő helyeken kitölteni számunkra.

2. **Kapcsoljuk be a többfaktoros azonosítást!** A többfaktoros azonosítás (rövidítve MFA) egy extra védelmi réteget biztosít a felhasználóinknak a jelszavakon túl. Ha egy támadó meg is szerzi a jelszavunkat, az MFA-val képesek lehetünk megállítani őket a belépéstől.
3. **Figyeljünk az utánkövető csalásokra!** Adatszivárgást követően a csalók megpróbálhatnak hamis e-maileket vagy üzeneteket küldeni, vagy az érintett szervezetnek, a bankunknak vagy ügyfélszolgálatnak kiadva magukat telefonálni nekünk. Felhasználva az ellopott információkat, sokkal valósághűbb e-mailek és üzenetek megfogalmazására lehetnek képesek. Csak azért, mert valaki tud rólunk néhány személyes információt, mint például azt, hogy hol élünk, kinek dolgozunk, milyen típusú autót vezetünk nem jelenti azt, hogy legitim. Ne kattintsunk ezekre a linkekre, illetve ne hívjunk fel olyan telefonszámokat, amik ezekben az üzenetekben szerepelnek. Ehelyett látogassunk el a szervezet hivatalos weboldalára vagy mobilapplikációjára, hogy megerősítést nyerjünk a probléma valódiságáról!
4. **Kövessük nyomon pénzügyi számláinkat!** Figyeljük pénzügyi és hitelkártya-számláinkat, hogy időben észlelni tudjuk az olyan gyanús tevékenységeket, mint például a váratlan vásárlások, készpénzfelvételek, jelszó-visszaállítási értesítések vagy a profilunkban történt változások. Több bank és online szolgáltató biztosít lehetőséget szöveges üzenetben vagy e-mailben történő értesítésre minden új tranzakcióról vagy a számlákon történő változásokról. Ezekkel az értesítésekkel hamarabb észrevehetjük, ha valamilyen probléma van.

Néhány esetben az adatszivárgásban érintett szervezetek valamilyen személyazonosság-lopás elleni védelmi szolgáltatást is felajánlhatnak egy külső szolgáltatón keresztül. Bár ezek a szolgáltatások nem sokat tesznek adataink védelméért, segíthetnek pénzügyi számláink és a hitelmonitorozás beállításában, illetve gyakran biztosítást vagy más védelmet is nyújtanak arra az esetre, ha a támadás következtében személyazonosság-lopás áldozatává válnánk. Mindig győződjünk meg arról, hogy a személyazonosság-monitorozó cég megbízható, hiszen a fiók létrehozásakor személyes adatokat fogunk megadni nekik.

Sajnos nem sokat tehetünk az olyan adataink védelme érdekében, amelyeket más szervezetek tárolnak, mivel a legtöbb esetben nincs felettük hatalmunk. De ezen egyszerű lépések betartásával jelentősen hozzájárulhatunk ahhoz, hogy sokkal nagyobb biztonságban legyünk, ha mégis adatvédelmi incidens történne.

Vendégszerkesztő

Brandi Narvaez vezető kiberbiztonsági tanácsadó, aki több mint 25 éves tapasztalattal rendelkezik az információbiztonsági és infrastruktúra-projektek megvalósításában. Szakterülete a szervezeti felhasználók és eszközök védelme, az érzékeny adatok biztonságának biztosítása, valamint a kiberbiztonsági stratégiák és az üzleti célok összehangolása a kiberreziliencia növelése és a működési hatékonyság optimalizálása érdekében.

Források

Hogyan használják ki a kiberbűnözők érzelmeinket: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions
A jelmondatok ereje: miért jobb a hosszabb, mint az okosabb?: https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
Tegyük könnyebbé a jelszókezelést: használjunk megbízható jelszószéfet: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
Megvédeni magunkat, mikor a magánéletünk védelme lehetetlen: https://www.sans.org/newsletters/ouch/protecting-yourself-when-true-privacy-is-impossible

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI)