OUCH! 2024. november

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Ne hagyjuk, hogy a kiberbűnözők lenyúlják a megtakarításainkat: Zároljuk a pénzügyi számláinkat!

Egy ravasz átverés és egy üres bankszámla

Emilynek egy átlagosan mozgalmas keddi napja volt. Felhörpintette a reggeli kávéját, rápillantott a telefonjára, és észrevette, hogy a bankja egy sms-t küldött neki: „Ön indította ezt a tranzakciót? Válaszoljon IGEN-nel vagy NEM-mel!" Emily meghökkent. Aznap még nem is vásárolt semmit. Talán csak egy hiba volt a rendszerben.

Azt válaszolta, hogy „NEM", majd perceken belül megcsörrent a telefonja. Egy nő volt a vonalban, aki azt állította, hogy a bankja csalási osztályától keresi. Nyugodt, professzionális hangnemben beszélt. „Szokatlan tevékenységet észleltünk a számláján, - mondta. - ezért ellenőriznünk kell néhány adatot az ön biztonsága érdekében". Emily, aki még mindig álmos volt, engedelmeskedett. A telefonáló végigvezette Emilyt egy sor lépésen, elkérte az online banki jelszavát, és még arra is rávette, hogy hagyjon jóvá egy értesítést a telefonján. „Ez megakadályozza a hacker hozzáférését" - magyarázta a nő. Emily követte, nem is sejtve, hogy csapdába esett.

Órákkal később Emily telefonja ismét megcsörrent. Ezúttal egy értesítést kapott: 5000 dollárt emeltek le a megtakarítási számlájáról. Pánikolva lépett be a banki alkalmazásba, de már túl késő volt. Az app nem fogadta el a jelszavát. A számláját zárolták. Aztán látta, hogy újabb és újabb pénzfelvétel történik.

Emily egy pillanat alatt megértette. A „csalási osztály" hívása csak egy csapda volt: egy kiberbűnöző jól megtervezett támadása, aki most már teljes mértékben irányítása alá vonta a számláját. Emily gyorsan felhívta a bankját, remélve, hogy még időben meg tudja menteni a számláját.

Miért kell megvédenünk a pénzügyi felhasználói fiókjainkat?

Online pénzügyi fiókjaink - csekkjeink, megtakarítási és befektetési számláink – többet rejtenek egyszerű pénznél: évek kemény munkáját, jövőbeli terveket és pénzügyi stabilitást képviselnek. A kiberbűnözők folyamatosan keresik a lehetőségeket, hogy hozzáférjenek a pénzünkhöz. Egyetlen hiba jelentős pénzügyi veszteséghez vezethet. Ha azt hisszük, hogy egy egyszerű jelszóval távol tarthatjuk ezeket a bűnözőket, akkor gondoljuk át újra!

A mai kiberbűnözők okosak, cselesek és könyörtelenek. Létfontosságú, hogy proaktívan védjük a pénzügyi számláinkat! Ez nem csak a jogosulatlan hozzáférés megakadályozásában segít, de így nyugodtabban hajthatjuk fejünket nyugovóra, tudván, hogy a nehéz munkával összegyűjtött pénzünk biztonságban van.

Öt lépés amivel rácsukhatjuk az ajtót a kiberbűnözőkre

1. **Kapcsoljuk be a többfaktoros hitelesítést (MFA):** A többfaktoros hitelesítés egy plusz biztonsági réteget ad online fiókjainkhoz azáltal, hogy két vagy több módszerrel kell igazolnunk személyazonosságunkat - valamivel, amit tudunk (jelszó), valamivel, ami a birtokunkban van (okostelefon vagy hardveres token), vagy valamivel, ami mi magunk vagyunk (ujjlenyomat vagy arcfelismerés). Még ha egy kiberbűnöző meg is szerzi a jelszavunkat, akkor is szüksége lesz egy második faktorra ahhoz, hogy hozzáférjen a fiókunkhoz. Mindig válasszuk az MFA-t, ahol csak lehetséges, különösen a pénzügyi fiókok esetében!

2. **Használjunk erős, egyedi jelszavakat:** Hozzunk létre erős, egyedi jelszavakat minden fiókhoz! Minél hosszabb és minél több karakterből áll a jelszó, annál jobb. Még ideálisabb, ha jelszó helyett jelmondatot használunk, azaz egy több kifejezésből álló jelszót. Nem vagy memóriazseni? Nem probléma. Használjunk jelszókezelőt, ami segít létrehozni és nyomon követni a hosszú, egyedi jelszavakat.

3. **Az átverések állandóak - ne dőljünk be nekik:** Az egyik legegyszerűbb módja annak, hogy a kibertámadók hozzáférjenek a fiókjainkhoz az, ha egyszerűen hozzáférést kérnek tőlünk. Olyan e-maileket, szöveges üzeneteket írnak vagy úgy telefonálnak velünk, mintha a bankunk keresne minket. Mindig ellenőrizzük a forrást, mielőtt linkekre kattintunk, mellékleteket töltünk le, vagy üzenetekre, telefonhívásokra válaszolunk! Minél nagyobb a sürgősség érzete, annál valószínűbb, hogy az e-mail, az üzenet vagy a telefonhívás támadás. A legjobb módja annak, hogy megvédjük magunkat, ha közvetlenül a bankunk hivatalos weboldalára látogatunk a webcímének beírásával, vagy ha visszahívjuk a bankunkat egy megbízható telefonszámon.

4. **Váljunk a számláink felügyelésének megszállottjaivá:** Gyakran ellenőrizzük a pénzügyi fiókjainkat, és kutassuk az illetéktelen belépés jeleit! Még jobb, ha engedélyezzük a legtöbb pénzintézet által automatikusan kínált értesítéseket a nagy összegű pénzmozgásokról vagy gyanús tevékenységekről. Az automatikus értesítések beállítása segíthet abban, hogy időben észrevegyük a csalárd tranzakciókat, és gyors lépéseket tegyünk a kár minimalizálásának érdekében. Ha valami nem stimmel, ne várjunk – cselekedjünk azonnal!

5. **Tartsuk zárolva az eszközeinket:** A telefonunk, laptopunk és táblagépeink olyanok, mintha a pénzügyi világunk páncélszekrényei lennének. Tartsuk őket biztonságban képernyőzárral és a legújabb szoftverfrissítésekkel! Javasoljuk az automatikus frissítések engedélyezését is!

Vendégszerkesztő

Elizabeth Rasnick a Nyugat-Floridai Egyetem Kiberbiztonsági Központjának adjunktusa, aki programozási tudással és incidenskezelő csoportban szerzett tapasztalattal is rendelkezik. A WiCyS floridai társszervezetének vezető alelnökeként tevékenykedik, informatikából doktorált.

Források

Top Három Módszer, Ahogy A (Kiber)támadók Célpontjává Válunk: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Érzelmi triggerek – Így csapnak be minket a kibertámadók: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

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