OUCH! 2023. június

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A pénzügyi fiókok biztonsága

Áttekintés

Pénzügyi fiókjaink a kiberbűnözők elsődleges célpontjai. A kiberbűnözők mindent megtesznek annak érdekében, hogy megszerezzék a pénzünket. Pénzügyi fiók alatt ne csak a csekk- vagy megtakarítási számlákra gondoljunk, hanem bármilyen befektetési, nyugdíj- és olyan online fizetési számlákra is, mint például a PayPal. Szerencsére néhány egyszerű, alapvető lépéssel megvédhetjük magunkat.

Hogyan zajlik egy támadás?

A bankok hatalmas összegeket költenek rendszereik védelmére, ami rendkívül megnehezíti a kiberbűnözők számára, hogy feltörjék azokat. Ezért a kiberbűnözők inkább bennünket és a felhasználói fiókjainkat veszik célba. Tudják, hogy nincs saját biztonsági csapatunk, aki megvédene bennünket, ezért sokkal könnyebb rajtunk keresztül hozzáférést szerezniük, mint a bankon keresztül. Íme a két leggyakoribb módszer, amellyel célba vesznek minket, hogy megpróbálják ellopni a pénzünket:

Jelszavak: Minden pénzügyi fiókot jelszóval védünk. Ha egy számítógépes bűnöző kitalálja vagy feltöri ezeket a jelszavakat, bejelentkezhet a nevünkben, majd átutalhatja pénzünket az általa kezelt bankszámlákra. A jelszavak megszerzésének számos módja létezik. Az egyik gyakori módszer a számítógép rosszindulatú programokkal való megfertőzése. Ha a számítógépünk fertőzött, a bank webhelyére történő belépésnél a kiberbűnözők megszerezhetik a felhasználónevünket és a jelszavunkat. Egy másik gyakori módszer az adathalász e-mailek küldése, amelyeket a támadók a bankunkat megszemélyesítve küldenek. Amikor az e-mailben található linkre kattintunk, azt gondolhatjuk, hogy a bankunk weboldalát látjuk, azonban valójában egy hamis webhelyre jelentkezünk be, amely a bűnözők irányítása alatt áll. Ez lehetővé teszi számukra, hogy begyűjtsék a felhasználónevünket és jelszavunkat, amelyek segítségével a nevünkben bejelentkezhetnek a netbankos fiókunkba.

Kérés: A kiberbűnözők egyszerűen el is kérhetik a jelszavunkat, vagy megpróbálhatnak rávenni bennünket arra, hogy utaljuk át nekik a pénzünket. Az ilyen pszichológiai manipulációs támadások gyakran egy telefonhívással kezdődnek. A kiberbűnözők tisztában vannak vele, hogy érzelmeink kihasználásával sokkal könnyebben késztethetnek bennünket hibázásra. Ez az oka annak, hogy egyre több adathalász e-mail, hangposta és böngésző előugró ablak jelenik meg, amelyek sürgető érzést keltenek, például azáltal, hogy a lejárat előtt fel kell hívnunk egy telefonszámot egy probléma megoldásához, vagy ahhoz, hogy még időben kihasználhassunk egy „fantasztikus kedvezményt”. Amint felhívjuk a telefonszámot, a bűnözők óriási nyomást gyakorolnak ránk, hogy hozzáférést biztosítsunk számukra a netbankos fiókunkhoz vagy, hogy a pénzünket más számlákra utaljuk át. Például azt állítják, hogy egy technikai támogató terület vagy a kormányzat nevében keresnek bennünket, és közlik, hogy a számítógépünk fertőzött, és amennyiben nem cselekszünk azonnal, akkor minden pénzünket elveszítjük.

Így védekezhetünk

Szerencsére banki fiókjaink biztonságban tartása egyszerűbb, mint gondolnánk. Íme a legfontosabb lépések, amelyeket megtehetünk saját védelmünk érdekében:

1. **Legyünk óvatosak**:A legjobb védelmet mi magunk jelentjük. Ha furcsa e-mailt, szöveges vagy hangposta üzenetet kapunk vagy böngésző felugró ablakot látunk, máris felmerülhet a támadás gyanúja. Minél erőszakosabb a sürgetés, minél nagyobb a nyomás az AZONNALI cselekvésre, annál valószínűbb, hogy támadásról van szó.

2. **Erős jelszavak használata / MFA**: Védjük pénzügyi és személyes e-mail fiókjainkat hosszú, egyedi jelszóval! Nehézséget okoz fejben tartani az összes jelszavunkat? Fontoljuk meg egy jelszókezelő szoftver használatát, amivel biztonságosan megjegyezhetjük és tárolhatjuk jelszavainkat! Az egyes pénzügyi számlák védelmének legjobb módja, ha minden számlán engedélyezzük a többtényezős hitelesítés (MFA) nevű funkciót.

3. **Ellenőrzés**: Tartsuk folyamatos ellenőrzés alatt számláink forgalmát! Beállíthatunk automatikus figyelmeztetéseket, amelyek e-mailben vagy szöveges üzenetben érkeznek minden alkalommal, amikor pénzmozgás történik a számlánkon. Ezáltal gyorsan észlelhetünk minden jogosulatlan vagy gyanús tranzakciót. Minél hamarabb észlelünk és jelzünk valamilyen hibát a banknak, annál valószínűbb, hogy visszaszerezhetjük a pénzünket.

A szerzőről

Lynn Dohm a Women in CyberSecurity (WiCyS) ügyvezető igazgatója. Lynn a kiberbiztonsági oktatási szektorban szerzett tapasztalatával igyekszik felhívni a figyelmet a kiberbiztonsági munkaerő diverzifikálásának fontosságára kormányzati és nonprofit programokban egyaránt.
Twitter: @lynn_dohm. Linkedin: https://www.linkedin.com/in/lynndohm/.

Források

Érzelmi triggerek: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Egyre trükkösebbek az adathalász támadások: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/
Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
Többfaktoros autentikáció: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

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