OUCH! 2024. december

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A Misztikum Feloldása: Hogyan lopják el a jelszavakat a kiberbűnözők?

Egy digitális rémálom: Liza nem kívánt kitettsége

Liza, egy igazán kreatív grafikus, aki élete nagy részét online élte. Banki ügyeit, vásárlásait és a társasági életét is különböző alkalmazásokon és weboldalakon keresztül intézte. Egy nap furcsa költekezésekre lett figyelmes banki alkalmazásában - olyan árucikkekre, amelyeket ő soha nem vásárolt, olyan üzletekből, ahol még sohasem járt. Ezután a közösségi média fiókjaiból spam üzenetek kezdtek terjedni furcsa termékekről és szolgáltatásokról, ezen felül barátai arról számoltak be, hogy szokatlan e-maileket kaptak tőle.

Liza pánikba esett amikor rájött, hogy elvesztette az irányítást digitális élete felett. Személyes fotói kiszivárogtak, és a magán jellegű beszélgetései is nyilvánosságra kerültek. Az ügyfelei elkezdték megkérdőjelezni megbízhatóságát, csorba esett a jó hírnevén. Miután kiberbiztonsági szakértőkkel konzultált, Liza rájött, hogy jelszavai komoly veszélybe kerültek. A kiberbűnözők hozzáférést szereztek a legszemélyesebb fiókjaihoz, és így darabról-darabra rombolták szét digitális világát. A kérdés továbbra is fennállt: Hogyan történhetett ez?

A kiberbűnözők alattomos taktikái: Öt gyakori módszer

A kiberbűnözők sokféle technikát alkalmaznak a jelszavak begyűjtésére. Íme öt gyakori módszer, amivel Liza esetéhez hasonlóan a mi jelszavainkat is megszerezhetik:

1. **Social Engineering Támadások**

   Social Engineering-nek hívjuk, amikor a támadók olyasvalakinek vagy valaminek adják ki magukat, akit ismerünk vagy akiben megbízunk, és ezzel rávesznek arra, hogy olyasmit tegyünk, amit nem kellene megtennünk. Olyan e-maileket vagy üzeneteket küldenek, amelyek legitimnek tűnnek, és gyakran a sürgősség, a félelem vagy a kíváncsiság erős érzetét keltik.

   Hogyan történt: Liza kapott egy e-mailt, ami látszólag a bankjától érkezett, még a bank hivatalos logói is benne voltak. Az e-mail állítása szerint gyanús tevékenységet észleltek Liza számláján. Ezért felszólították, hogy kattintson az üzenetben kapott linkre, hogy így igazolja a személyazonosságát. A link egy hamis weboldalra vezetett, amely rögzítette a bejelentkezési adatait, amikor megadta azokat.

2. **Malware**

   A malware-ek olyan kártékony szoftverek, amelyeket számítógépek megfertőzésére terveztek. Ha egy számítógép megfertőződött, utána a kiberbűnözők azt tehetnek vele, amit csak szeretnének. A keyloggerek (amiket más néven *információ lopó káros programoknak is hívnak*) olyan malware-ek, amelyek minden billentyűleütést rögzítenek, beleértve a bejelentkezési adatokat, jelszavakat és egyéb érzékeny adatokat is.

   Hogyan történt: Liza letöltött egy a munkájához szükséges, látszólag legitim betűtípus csomagot. Ebben azonban egy keylogger volt elrejtve, ami telepítette magát a számítógépére. Idővel rögzítette a különböző fiókok bejelentkezési adatait, és visszaküldte azokat a támadónak.

3. **Brute Force Támadások**

   Brute Force támadások során a kiberbűnözők automatizált eszközökkel számos jelszó-kombinációt próbálnak ki, amíg meg nem találják a helyeset. A gyenge jelszavak ellen különösen hatékony ez a módszer.

   Hogyan történt: Liza számos fiókjához olyan egyszerű jelszavakat használt, mint a "liza2020". A támadó olyan szoftvert használt, amely szisztematikusan próbálkozott a gyakori jelszavakkal, és ezzel könnyedén feltörte a fiókjait.

4. **Adatszivárgások**

   Ha egy weboldalt vagy szolgáltatást feltörnek, az hatással lehet az összes azon a szerveren tárolt fiókra. Ha ugyanazt a jelszót használjuk több felhasználói fiókunkhoz is, akkor amennyiben az egyik fiókunk kompromittálódik, az az összes többi fiókunkat is veszélyezteti.

   Hogyan történt: Az egyik Liza által is használt népszerű közösségi média platformon adatvédelmi incidens történt. Mivel más platformokon ugyanazt a jelszót használta, a támadók a kiszivárgott belépési adatokkal hozzáférést szereztek a többi fiókjához is.

5. **Megvásárolt Belépési Adatok**

   A kiberbűnözők egyszerűen megvásárolhatják a népszerű jelszavakat az interneten, leggyakrabban a Dark Weben. Bizonyos kiberbűnözők az áldozatok jelszavainak ellopására specializálódtak, az eddig tárgyalt módszerek alkalmazásával. Ezután tárolják és eladják az ellopott jelszavakat más kiberbűnözőknek.

   Hogyan történt: Egy kiberbűnöző úgy döntött, hogy a hétvégén a lehető legtöbb pénzt akarja keresni, ezért a Dark Webre látogatott, ahol több mint 100 000 kompromittált fiókot vásárolt meg jelszavaikkal együtt. Liza egyik fiókja is rajta volt ezen a listán.

Három kulcsfontosságú óvintézkedés, amit tehetünk

Szerencsére három egyszerű lépéssel nagyban hozzájárulhatunk fiókjaink és online digitális életünk védelméhez.

1. Használjunk hosszú, egyedi jelszavakat mindegyik fiókunkhoz! Javasoljuk a jelmondatok használatát, amik több szóból álló, igazán hosszú jelszavak.
2. Használjunk jelszószéfet, hogy biztonságban tároljuk és kezeljük az összes egyedi jelszavunkat!
3. A legfontosabb fiókjaink védelmének érdekében kapcsoljuk be a többfaktoros hitelesítést ahol csak lehetséges!

Vendégszerkesztő

Lekshmi Nair egy senior kiberbiztonsági vezető, 22 éves szakmai tapasztalattal az információbiztonsági tanácsadás és a kiberbiztonsági stratégia területén. Jelenleg a BlackDuck Software alkalmazásbiztonsági tanácsadó részlegének rangidős igazgatója. Ő a WiCyS India alapítója és elnöke.

Források

Fantomhangok: Védekezés a hangklónozásos támadások ellen: https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
SMS-támadások: Egy smishing történet: https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/
Top Három Módszer, Ahogy A (Kiber)támadók Célpontjává Válunk: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
A Jelmondatok Ereje: https://www.sans.org/newsletters/ouch/power-passphrase/
A jelszókezelők ereje: https://www.sans.org/newsletters/ouch/power-password-managers/

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