MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Spôsoby zneužitia osobných údajov

Zneužitie osobných údajov je stále častejším problémom v bežnom živote ľudí. Útočníci sa snažia využiť rôzne sofistikované metódy, vrátane web scrapingu a sociálneho inžinierstva, na získanie citlivých údajov obetí a ich následné zneužitie. Tieto údaje môžu zahŕňať osobné informácie, telefónne čísla, bankové údaje a oveľa viac. V nasledujúcom texte sa pozrieme na to, ako by útočník mohol získať a zneužiť tieto údaje v rôznych situáciách.

Telefón + Banková karta:

Útočník by mohol pomocou kombinácie web scrapingu a sociálneho inžinierstva získať osobné údaje, vrátane telefónneho čísla a údajov z bankovej karty. Existujú automatizované nástroje na web scraping, ktoré prehľadávajú verejne dostupné online zdroje (sociálne siete, fóra, web stránky..) a zbierajú z nich osobné údaje.

Na základe získaných dát dokáže útočník využiť taktiky sociálneho inžinierstva za účelom nadobudnutia konkrétnych údajov, ako sú telefónne číslo, číslo bankovej karty a podobne. Po získaní telefónneho čísla a údajov z bankovej karty by útočník mohol tieto informácie zneužiť na neoprávnené transakcie alebo finančné podvody. V prípade, že získa prístup k bankovým údajom, môže sa pokúsiť vykonať transakcie na účte obete a následne obeť kontaktovať telefonicky s cieľom získať ďalšie informácie, ktoré mu pomôžu s finančnými podvodmi.

Krádež účtu:

Pomocou metódy web scrapingu dokáže útočník získať meno a priezvisko, dátum narodenia, miesto bydliska, emailovú adresu a podobne. Na základe zberu týchto osobných údajov, dokáže útočník vytvoriť falošný profil alebo emailovú správu a pokúsi sa získať ďalšie citlivé informácie, ako sú heslá alebo odpovede na otázky k obnoveniu hesla. Tým získa úplnú kontrolu nad účtom alebo zablokuje Váš prístup do Vášho profilu.

Krádež identity:

Každá zverejnená fotografia môže obsahovať metadáta, ktoré poskytujú informácie o mieste, kde bola fotografia zachytená. Útočník môže zneužiť tieto informácie na vytvorenie falošnej identity a dokumentovať presný pohyb obete. S týmito informáciami o polohe môže útočník vytvoriť vymyslený príbeh alebo identitu a tým zvýšiť dôveryhodnosť svojho príbehu.

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Spôsoby zneužitia osobných údajov

Vydieranie a kyberšikana:

Útočník môže získať osobné údaje obete, vrátane jej fotografií a polohy miest, ktoré navštívila. Úspešné získanie informácií umožňuje vydierať alebo šikanovať obeť, napríklad vyhrážkami zverejnením citlivých fotografií alebo informácií na sociálnych sieťach.

Útok na firmy/organizácie:

Útočník môže vyhľadávať informácie o zamestnancoch a organizácii, vrátane ich fotografií na verejných profiloch (napríklad platforma LinkedIn). Tieto informácie dokáže zneužiť na vytvorenie falošnej identity, ktorú môže zneužiť na infiltráciu do organizácie za účelom získania citlivých vnútropodnikových informácií a špionáže.

Vlámanie:

Útočník by mohol vyhľadávať verejne dostupné informácie o bydlisku alebo pomocou GPS metadát z uverejnených fotografií na sociálnych sieťach. Môžu to byť informácie o adrese, veľkosti domu, plánovaných dovolenkách, naplánovanom programe v online kalendároch a iné. Na základe týchto informácií by útočník mohol vytvoriť falošný príbeh alebo vytvoriť dôveryhodný scenár, ktorý by mohol zneužiť pri plánovaní vlámania. Dokáže zistiť neprítomnosť majiteľov, čo by mu mohlo poskytnúť príležitosť na vlámanie.

Kombinácia osobných údajov:

Útočník môže zhromažďovať rôzne verejné údaje o obeti z rôznych zdrojov. Následne môže využiť tieto informácie na vytvorenie komplexného profilu obete a použiť ho na sofistikované útoky.

<u>Časté príklady:</u>

Veľmi častým príkladom môže byť telefonická komunikácia, kde sa útočník vydáva za príslušníka policajného zboru alebo analytika IT oddelenia v banke, na pošte a podobne. Primárnym nástrojom útočníka je sociálne inžinierstvo, kedy sa Vás snaží presvedčiť o zdieľaní citlivých údajov, autentifikačných dát, prípadne potvrdení notifikácie. **<u>Nikdy tieto informácie neprezrádzajte!</u>** Banka, pošta, kuriér alebo iné oficiálne inštitúcie nepotrebujú vedieť autentifikačné dáta, heslá alebo údaje z bankovej karty.

Ďalším príkladom môže byť nezodpovedné správanie zo strany obetí, napríklad keď sa pochvália novou bankovou kartou na sociálnych sieťach. **<u>Nikdy nezverejňujte fotografie svojich bankových údajov!</u>** Na obrázku môžeme vidieť zverejnenie prednej strany debetnej karty a po následnej interakcií ľudí v komentároch aj prezradenie CVV/CVC kódu.

Buďte obozretní pri zdieľaní osobných údajov online a chráňte svoje informácie! Dodržiavajte bezpečnostné opatrenia, aby ste minimalizovali pravdepodobnosť zneužitia osobných údajov útočníkmi. Silné heslá, dvojfaktorová autentifikácia a opatrnosť pri zdieľaní osobných informácií online sú nevyhnutné pre zachovanie Vašej digitálnej bezpečnosti.