

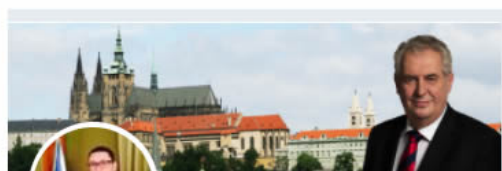
KLONOVÁNÍ PROFILŮ JAKO KLASICKÁ INVAZIVNÍ TECHNIKA FUNGUJE VELMI DOBŘE NA DĚTI. V POLOVINĚ PŘÍPADŮ SI NEOVĚŘUJÍ, ZDA JE O PŘÁTELSTVÍ ŽÁDAJÍ SKUTEČNĚ JEJICH SPOLUŽÁCI A KAMARÁDI Z REÁLNÉHO SVĚTA.

Kamil KOPECKÝ

Klonování profilů uživatelů sociálních sítí a následné přebírání jejich identity představuje klasickou invazivní techniku využívanou v rámci různých druhů internetových podvodů (lze ji zařadit mezi tzv. scam). Často se klonované profily využívají v rámci podvodných mobilních plateb, o kterých jsme vás informovali již v minulosti a na jejichž rizika upozornila v současnosti také Policie ČR a národní bezpečnostní tým (CSIRT).

Postup útoku je v zásadě stejný, jako byl již před lety: útočník naklonuje profil vybrané osoby a pošle do jejího seznamu přátel žádost o přátelství. Oběť útoku pak obdrží zprávu s prosbou o telefonní číslo a uvedení kódu ze zaslané SMS zprávy. Kód je od platební brány a potvrzuje platbu, která se aktuálně pohybuje kolem 1000-2000 Kč.

Kromě tohoto typu podvodu nám může internetový “přítel” s naklonovaným profilem podstrčit např. odkaz na infikované www stránky, zavirovanou fotografii či video, odkaz na stránky zaměřené na phishing apod.



Jiří Ovčáček

@PREZIDENTmluvci

Tiskový mluvčí prezidenta republiky a ředitel Tiskového odboru Kanceláře prezidenta republiky

Follow



Jiří Ovčáček

@PREZIDENTmlufci

Ředitel Odboru tiskového a tiskový mluvčí prezidenta republiky. Oficiální profil kandidáta na post Prezidenta republiky 2018.

Follow

Řadu naklonovaných profilů má také tiskový mluvčí prezidenta Jiří Ovčáček. Profily jsou však využívány k humoristickým a recesistickým účelům. Často je velmi těžké rozpoznat, který z nich je ten originální.

S klonovanými profily a komunikací s neznámými lidmi v prostředí internetu mají samozřejmě zkušenosti i dětští uživatelé sociálních sítí. Podle výzkumu Sexting a rizikové seznamování českých dětí v kyberprostoru, který realizovalo Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci se společností O2 Czech Republic, s neznámými uživateli v prostředí internetu komunikuje téměř polovina dětí (48,59 %). **Žádosti o přátelství v prostředí Facebooku pak vyhoví třetina dětí (31,10 %), aniž by si ověřila identitu člověka, který je o přátelství požádal.** Mezi přátele si pak děti často řadí neznámé osoby - třeba jen na základě profilové fotografie a atraktivních fotografií na online "zdech". Nachytat se však nechávají nejenom děti, ale i dospělí.

Téměř polovina českých dětí (48,09 %) je přesvědčena o tom, že dokáže rozeznat podezřelý - pravděpodobně "fejkový" profil jiného uživatele v rámci sociální sítě. Stejně tak si však **polovina českých dětí (49,49 %) neověřuje identitu svých spolužáků a kamarádů z reálného světa, kteří je žádají o přátelství např. na Facebooku, prostřednictvím Skype apod.** Právě tito uživatelé však mohou využívat naklonovaný profil a získat tak přístup k přátelům daného dítěte či dospělého.

Více než třetina dětí (36,37 %) je přesvědčena o tom, že dokáže rozeznat komunikaci s dospělým člověkem. V praxi je však situace

jiná, komunikace totiž bývá velmi krátká, útržkovitá, nelze podle ní s jistotou říci, zda jde o dospělé osobu nebo dítě.

Obrana před útoky spojenými s klonovanými profily je jednoduchá:

- 1. Nastavit si soukromí na svém účtu tak, aby neznámí lidé neviděli seznam přátel.**
- 2. Ověřit si identitu žadatele o přátelství - třeba tím, že mu zatelefonujeme.**
- 3. Nikdy nevyužívat v prostředí sociálních sítí m-platby, nikomu neposílat platební kódy.**

dr. Kamil Kopecký
Centrum PRVoK PdF UP, E-Bezpečí