E-Bezpečí 2019, 4(2): Page 98-100. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1712

PODVODY SPOJENÉ S M-PLATBAMI STÁLE ČASTĚJI CÍLÍ NA STARŠÍ UŽIVATELE INTERNETU.

Kamil KOPECKÝ

Podvody spojené s tzv. m-platbami (platbami prostřednictvím mobilních telefonů) patří v oblasti kybernetické kriminality ke stálicím, o kterých na našem portálu pravidelně informujeme. Stále častěji se k útoku využívá tzv. klonování profilu, které představuje dnes již klasickou invazivní techniku, která velmi dobře funguje jak na děti, tak i dospělé uživatele online služeb.

Před 14 dny kontaktovala naši poradnu starší uživatelka (55 let), která má s klonováním profilu a s podvodnými m-platbami osobní zkušenost:

Dobrý den, chtěla jsem se zeptat, zda je nějaká šance dostat peníze z osoby, která mě připravila o pro mne dost velkou částku. Tuto osobu já osobně znám, tato osoba mi napsala na FB o telefonní číslo. Poslala jsem jí ho, neměla jsem důvod ho neposlat. Tato osoba mi nechala na telefon poslat nějaký kód a chtěla po mně, abych jí ho nadiktovala. Ohradila jsem se, že mi přišla SMS zpráva, kde se píše, že pomocí tohoto kódu zaplatím 600 korun. Byla jsem opakovaně přesvědčována, že jde o hru, o získání nějaké výhry a já - blbec - jsem tomu uvěřila. Navíc mi dotyčná osoba tvrdila, že pokud budu muset něco zaplatit, tak že mi to uhradí. Pochopitelně jsem naletěla, zaplatila 5*600 korun. A dotyčná osoba mi následně na moje zprávy

neodpovídala, Povedlo se mi najít její nový FB profil, kde mi tvrdí, že ji někdo FB účet naboural a že to jsme vůbec nekomunikovaly spolu. Náhodou jsem narazila na tuto vaši stránku a chci se poradit, zda mohu něco dělat, když mi ta osoba tvrdí, že mi nic platit nebude. (Anežka, věk 55)

V tomto případu lze sledovat kombinaci hned dvou vzájemně propojených rizikových komunikačních jevů - na jedné straně manipulaci dospělé osoby prostřednictvím **vymyšleného příběhu o účasti ve hře**, na straně druhé pak možnou existenci **klonovaného profilu pachatelky/uživatelky** (což může, ale také nemusí být pravda), ze kterého byl útok proveden. Tato situace se jeví jako pravděpodobná, protože podvodník logicky k tomuto typu útoku nevyužije svůj vlastní profil, tím by riskoval snadné odhalení. Při dalším prověřování navíc bylo zjištěno, že se osoba s naklonovaným profilem vyšetřování nebrání a dokonce doporučuje oběti kontaktovat policii. Dalším možným scénářem je, že se skutečně do profilu "pachatelky" nabourala jiná osoba a komunikaci s obětí vedla skutečně ona.

Co lze tedy oběti doporučit?

1. Věc oznamte na Policii ČR pro podezření z podvodu, předložte komunikaci s dotyčnou osobou nejlépe v originální podobě. Komunikaci nemažte a při oznámení předložte také veškeré údaje k provedeným platbám a k předmětnému účtu pachatele (tj. SMS, DMS apod.).

2. Dotyčného pachatele v online prostředí neblokujte, neodstraňujte z přátel.

3. Kontaktujte všechny Vaše přátele na sociální síti a o daném podvodném jednání konkrétního falešného účtu je informujte. Váš účet na sociální síti si nastavte jako soukromý, aby obsah, který sdílíte (fotografie apod.), viděli pouze Vaši přátelé a mohli Vás kontaktovat jen ti, kterým dáte souhlas. Pokud někdo z Vašich přátel pachateli zaplatil, nechť si ponechá v originální podobě proběhlou komunikaci s pachatelem a věc oznámí na Policii ČR.

4. V případě dětských telefonů vypněte možnost používat

premium SMS a další zpoplatněné SMS služby. Vypnutí umožňuje každý mobilní operátor.

Další související zdroje:

Kopecký, K. Podvodné mobilní platby na Facebooku. E-Bezpečí, 2013.
Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/774-podvodne-platby-na-facebooku

Kopecký, K. 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.. E-Bezpečí, roč. 2, č. 2, s. 5-7. ISSN 2571-1679.
Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1253

Pro E-Bezpečí
Kamil Kopecký