E-Bezpečí 2022, 7(1): Page 52-53. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=2625

SMISHING ČILI PHISHING REALIZOVANÝ PROSTŘEDNICTVÍM SMS OPĚT ŘÁDÍ

Kamil KOPECKÝ

Termínem smishing označujeme formu phishingu, který využívá SMS zprávy (odtud název smishing = SMS + phishing). Tento druh podvodu je v současnosti velmi populární a přibývá obětí, které zareagovaly na podezřelou SMS zprávu, která dorazila do jejich mobilního telefonu.

V posledních měsících zaznamenala většina českých bank vlnu této formy phishingu zneužívající SMS zpráv - snahu o získání citlivých údajů a proniknutí na účty zaznamenali např. klienti ČSOB, FIO banky, Raiffeisenbank, Monety, České spořitelny a dalších bankovních institucí. Podle seriózních odhadů se v každé phishingové vlně (která zasahuje přibližně desetitisíce uživatelů) nechají nachytat desítky klientů bankovních institucí, celkové odhadované škody se pak pohybují v desítkách až stovkách milionů korun.

Jak rozpoznat smishing?

1. SMS obsahuje chyby, naznačuje, že by mohlo jít o strojový překlad zprávy z cizího jazyka.
2. SMS obsahuje výzvu k přihlášení se k našemu bankovnímu (či jinému účtu) a odkazy, které vedou na podvržené stránky bankovní instituce. Ty nás pak vyzývají k zadávání citlivých údajů (osobních údajů, PINů, detailů k naši platební kartě apod.). SMS využívají klasické phishingové legendy, např.

vaše karta byla zablokována, pro odblokování se přihlaste zde, jinak přijdete o finance. Názvy stránek mají podezřelé adresy (např. koncovky .info, v názvu slovo bezpecnost, bezpecnostni apod.). Pokud se pokusíte přihlásit pod svými přihlašovacími údaji, dorazí na váš telefon přihlašovací kód, pod kterým se máte na stránky přihlásit. Jde však o kód, který umožní přístup do skutečného internetového bankovnictví u vaší banky.

3. SMS zprávy obvykle obsahují odkazy, které jsou vytvořeny tzv. zkracovači - tj. například http://goo.gl/ či http://bit.ly/. Na první pohled pak nevidíte, kam ve skutečnosti vedou.
4. SMS obsahují zprávy o tom, že jste např. vyhráli v soutěži (přestože jste se do soutěže nepřihlásili) a vyzývají k potvrzení vaší výhry (opět přes odkaz).

Základní pravidlo zní: Nikdy nereagovat na podobné typy zpráv, bankovní instituce se svými klienty tímto způsobem nekomunikují a zadávání osobních údajů či přihlašování přes speciální odkazy v SMS nepožadují. Pokud si nejste jisti, zavolejte přímo na oficiální telefonní linku vaší bankovní instituce. Doporučujeme také nahlásit pokus o zneužití účtu Policii ČR.

Další informace o smishingu najdete na stránkách Policie ČR (zde a zde). A jak vlastně funguje phishing prozradí Převíti na síti.

Pro E-Bezpečí
Kamil Kopecký,
Univerzita Palackého v Olomouci