**Nowa forma oszustwa – "Smishing".**

Smishing to rodzaj oszustwa ( rodzaj ataku phishingowego), który poprzez wykorzystanie komunikacji SMS dokonuje kradzieży danych osobowych, na przykład numeru SSN lub karty kredytowej, z telefonu komórkowego ofiary. Wszystko zaczyna się od wysłania fałszywej wiadomość SMS, stąd nazwa SMiShing. Należy zatem szczególnie uważać na wszelkie SMS-y z informacją o konieczności dopłaty. Takie SMS-y z żądaniem dopłaty kilku złotych do przesyłki od firmy kurierskiej czy do rachunku za prąd od dostawcy energii mogą stanowić właśnie tzw. "smishing", czyli oszustwo wykorzystujące komunikację SMS . Warto mieć się na baczności i nie klikać w linki w takich wiadomościach.

Urząd Komunikacji Elektronicznej oficjalnie poinformował, iż smishing to odmiana phishingu, czyli różnego rodzaju oszustw, w których przestępcy podszywają się pod inne osoby lub instytucje. Cel ataku może być różny, ale najpopularniejsze z nich to przede wszystkim zdobycie danych osobowych lub informacji o karcie kredytowej, a także zainfekowanie sprzętu szkodliwym oprogramowaniem, które może zapewnić cyberprzestępcom zdalny dostęp do urządzenia.

W wypadku smishingu oszuści wykorzystują komunikację SMS, np. rzekomą wiadomość od firmy kurierskiej z informacją o konieczności uiszczenia dopłaty do przesyłki, albo od dostawcy energii, że brakuje kilku złotych do ostatniego rachunku.

W przypadku smishingu przestępcy, przygotowując ataki, świetnie potrafią dopasować się do aktualnej sytuacji w kraju i na świecie. Na obecną chwilę zdarzają się już przypadki wiadomości informujących o konieczności rejestracji na szczepienia, a także takie przypominające o rozliczeniu [PIT](https://mojafirma.infor.pl/tematy/pit/). Liczba SMS-ów od firmy kurierskiej wzrasta przede wszystkim w okresie przedświątecznym. Należy pamiętać, iż mimo wielu wariantów główny schemat działania jest bardzo podobny. Link w SMS-ie prowadzi zwykle do podstawionej strony z fałszywym panelem płatności. Inna opcja to otwarcie strony z odnośnikiem do pobrania aplikacji. Otwierane witryny do złudzenia mają przypominać te oryginalne. Warto podkreślić, iż jest to bardzo niebezpieczne , gdyż mając do dopłacenia niewielką kwotę, zwykle nie analizujemy tego zbyt długo. Wchodzimy w link, widzimy stronę, którą – jak sądzimy – dobrze znamy (np. portal służący do płatności), wybieramy swój bank i logujemy się do niego. Dlatego też warto szczególnie zwrócić uwagę na adres strony, na której się jest. Zasadniczo ma on w swojej treści fragment oryginału, ale to jedyne, co łączy go z rzeczywistym adresem. Na nasze szybkie, często impulsywne działanie liczą oszuści. Taka niska kwota do zapłaty, która wskazana jest w fałszywym sms-sie, ma sprawić, że potraktujemy ją jako błahostkę i szybko zechcemy załatwić sprawę i o niej zapomnieć, bo przecież tyle mamy na głowie. Jeżeli mamy jakiekolwiek wątpliwości, czy faktycznie nie trzeba czegoś dopłacić bądź uzupełnić danych, nigdy nie powinniśmy tego robić poprzez link z SMS-a. Najlepiej samemu skontaktować się z firmą, która ma być nadawcą wiadomości, i potwierdzić jej treść telefonicznie. Warto również zaznaczyć, iż wiele osób do chwili obecnej bardziej ufa wiadomościom otrzymywanym w SMS-ach niż tym, które przychodzą w wiadomościach e-mail. Najwyraźniej wielu osobom nie mieści się w głowie, że haker może mieć ich numer. Prawda jednak jest taka, że łatwiej jest zdobyć czyjś numer telefonu niż adres e-mail. Liczba możliwych numerów telefonu jest ograniczona, natomiast długość adresu e-mail nie ma ograniczeń. Wprawdzie są jakieś zdroworozsądkowe wytyczne, ale dodatkowo adres poczty elektronicznej może zawierać cyfry, znaki alfabetu (a, b, c, etc.) i symbole (!, #, %, itd.). Dlatego o wiele trudniej jest odgadnąć losowy adres e-mail niż losowy numer telefonu.

Haker, który dokonuje przestępstwa smishingu,może po prostu wysyłać wiadomości tekstowe na numery, które są losowymi kombinacjami dziesięciu cyfr. Jeśli trafi na nieistniejący numer telefoniczny, to jego wiadomość nigdzie nie trafia, więc może do woli ponawiać próby z kolejnymi kombinacjami. Za pomocą takich metod oszust może próbować osiągnąć wiele różnych celów .Może na przykład próbować wydobyć czyjeś dane osobowe, podszywając się pod bank. W takim przypadku wysyła na przykład wiadomość z łączem, które ofiara ma kliknąć, aby połączyć się z bankiem i zweryfikować szczegóły niedawnej transakcji, która została uznana za podejrzaną. Ewentualnie haker może zawrzeć w wiadomości prośbę o zadzwonienie pod podany numer, aby uzyskać więcej informacji o ostatnio wykrytej podejrzanej transakcji lub podejrzeniu włamania na konto. Za pomocą wiadomości tekstowych hakerzy próbują także wyłudzić numery kart kredytowych, grając na naszych uczuciach. Przestępca może wykorzystać jakiś szczytny cel i poprosić nas o przekazanie darowizny. Może to być na przykład fundusz odbudowy lub uzupełnienia zapasów, takich jak woda pitna lub odzież, po jakiejś katastrofie, na przykład huraganie. Wystarczy użyć podanego łącza, aby przejść do strony, na której należy wpisać dane swojej karty kredytowej, w tym swój adres. W ten sposób przestępca zdobywa możliwość robienia własnych zakupów przy pomocy naszej karty a nawet może ustalić na niej miesięczną kwotę darowizny .

Istnieje również taki rodzaj ataku smishingowego , który polega na podszywaniu się pod operatora sieci komórkowej, który rzekomo wysyła nam fantastyczną ofertę ulepszenia usługi lub nowego telefonu. Oczywiście wystarczy kliknąć łącze lub zadzwonić pod podany numer telefonu. Wtedy haker prosi o weryfikację wszystkich danych, od numeru SSN po numer karty kredytowej. Potem okazuje się, że nie było żadnej wspaniałej oferty, a jedynie skradziono numer karty kredytowej.

Urząd Komunikacji elektronicznej wypowiedział, się w przedmiotowej sprawie i wskazał, aby podobne wiadomości zgłaszać do CERT [Polska](https://mojafirma.infor.pl/tematy/polska/).(CERT Polska jest to zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci) Dzięki funkcji "przekaż" lub "udostępnij" można przesłać treść wiadomości na nr 799 448 084. Ważne, aby przesłać całą wiadomość w oryginalnej formie. Po weryfikacji analityków strona zostanie wpisana na Listę Ostrzeżeń. Jeśli próba wyłudzenia nastąpiła przy wykorzystaniu wiadomości email lub bezpośrednio na jakiejś stronie, także można to zgłosić do NASK na stronie: incydent.cert.pl/phishing lub emailem na adres: [cert@cert.pl](mailto:cert@cert.pl).

r.pr. Magdalena Piech