Cyberdefence 24

26.03.2019

POLACY NIEŚWIADOMI PHISINGU

Metody ataków phishingowych na polskich internautów stają się coraz bardziej wyszukane. Ofiary oszustów tracą w sieci często niemałe pieniądze – a wszystko przez brak świadomości, a czasem nawet przez chwilową nieuwagę. Z badania przeprowadzonego na zlecenie Nest Banku wynika, że aż 30% Polaków w ogóle nie wie czym jest phishing, a 32% ma wrażenie, że wie ale nie jest pewna. – *Banki zapewniają nam bardzo nowoczesne i bezpieczne metody płatności. W korzystaniu z każdej z nich potrzebny jest jednak zdrowy rozsądek* – mówi Michał Sobiech, Członek Zarządu Nest Banku

Czym jest phishing i jak działa?

Ogólnie mówiąc phising jest metodą oszustwa internetowego, które polega na wyłudzeniu od użytkownika jego poufnych danych. W wyniku takiego działania oszuści internetowi uzyskują numery kart debetowych i kredytowych, dostępy do elektronicznego konta bankowego czy też inne informacje, które pozwalają na kradzież ich pieniędzy. Obecnie proceder phishingu w bankowości występuje najczęściej pod postacią spamu rozsyłanego na adresy e-mail. Jak wygląda to w praktyce?

Internetowi oszuści, licząc na nieuwagę lub niewiedzę użytkowników, wysyłają zainfekowane maile i smsy. Łudząco przypominają one wezwanie do zapłaty faktury np. za telefon czy usługę. Nazwa nadawcy również wydaje się identyczna z nazwą operatora lub innej znanej firmy. Wiadomość zawiera jednak niebezpieczny link, który kieruje na fikcyjną stronę logowania banku. Jest ona zazwyczaj niemal identyczna z oryginalną, różni się jednak kilkoma ważnymi szczegółami. Nieświadomy internauta wprowadzając na takiej stronie dane do logowania, przekazuje je oszustom, którzy wykorzystują je do zalogowania się na prawdziwej stronie banku. Zlecają wtedy przelew lub inną operację, a na komputerze internauty pojawia się niestandardowe okno z prośbą o potwierdzenie logowania hasłem sms. Jeśli wprowadzi kod otrzymany smsem, nie zapoznając się z jego treścią – oszust zatwierdzi operację, wyprowadzając tym samym środki z rachunku.

Polacy a phishing, czy wiemy co oznacza?

Okazuje się, że Polacy wciąż nie do końca wiedzą, co oznacza phishing. Z badania przeprowadzonego na zlecenie Nest Banku* wynika, że ponad 30% z nas nie zna tego pojęcia, a 32% nie ma pewności czy dobrze je definiuje. Respondenci zapytani, jak rozumieją phishing, najczęściej odpowiadali, że jest to podszywanie się pod inną osobę lub instytucję celem wyłudzenia danych, zdobycia korzyści finansowej – takie odpowiedzi wskazało łącznie 39% ankietowanych. 15% z nas rozumie phishing jako metodę oszustwa, 8,6% uważa, że jest to kradzież danych, a ponad 6% utożsamia go z oszustwem internetowym. – *Wyniki badania pokazują, że wielu Polaków zna poprawne znaczenie słowa phishing. Na przestrzeni kilku lat ataki phishingowe nasiliły się i paradoksalnie dzięki temu wzrosła także świadomość i wiedza w tym temacie. Jednak nasze doświadczenia pokazują, że wciąż jest wiele do zrobienia w zakresie edukacji klientów* – mówi Michał Sobiech, Członek Zarządu Nest Banku.

Czy wiemy jak chronić się przed atakami oszustów internetowych?

Polacy zapytani o to, czy wiedzą, jak chronić swoje pieniądze ulokowane na koncie bankowym, najczęściej odpowiadali asekuracyjnie „raczej tak” - 62%, odpowiedzi „zdecydowanie tak” udzieliło jedynie 13% z nas. Jeżeli chodzi o sposoby zabezpieczania pieniędzy przed oszustami, to 26% badanych regularnie zmienia hasło do bankowości elektronicznej, 19% dodatkowo zabezpiecza loginy i hasła, prawie 18% nie loguje się do konta w miejscach publicznych ani na innych komputerach. Niestety jedynie 17% z nas deklaruje, że posiada aktualny program antywirusowy i dokładnie weryfikuje otrzymywane e-maile. Jeszcze bardziej niepokojący jest fakt, że tylko 7% weryfikuje treść SMS-ów i kodów weryfikacyjnych, które otrzymuje od banku.

Polacy mają ogólną świadomość, jak chronić swoje pieniądze zgromadzone na kontach bankowych przed oszustami. Jednak należy pamiętać, że ataki phishingowe są coraz bardziej zaawansowane i wykorzystują różne metody, nie tylko technologiczne. Oszuści często chcą wywołać w użytkowniku natychmiastową, nieprzemyślaną reakcję. Posługują się komunikatami takimi, jak „zaktualizuj swoje dane osobowe, w przeciwnym przypadku Twój dostęp do konta zostanie zablokowany” czy „Twoje konto zostało zaatakowane, zaktualizuj dane i zmień hasło”. W obliczu takich komunikatów często „tracimy chłodną ocenę sytuacji” i postępujemy zgodnie z instrukcjami. Dlatego musimy być naprawdę ostrożni i uważnie czytać każdą wiadomość, która została rzekomo wysłana przez bank, operatora telefonii czy inną znaną firmę. Przede wszystkim jednak pamiętajmy, że nasze dane do logowania w systemie bankowym powinny być traktowane ze szczególną ostrożnością. Korzystajmy jedynie z zaufanych urządzeń (własnego komputera, telefonu, tabletu), chronionych dobrymi programami antywirusowymi. Pod żadnym pozorem nie klikajmy w linki prowadzące do stron do logowania, używając tylko oficjalnych stron i aplikacji bankowych. Nawet najlepsze systemy antywirusowe czy bankowe nie uchronią nas przed naszymi nieostrożnymi zachowaniami w sieci - mówi Michał Sobiech, Członek Zarządu Nest Banku.

Źródło: *Badanie opinii „Bezpieczeństwo kont bankowych” zrealizowane przez Agencję Badań Rynku i Opinii SW Research, w marcu 2019 roku, na grupie 800 dorosłych Polaków.*