**Użytkownicy Facebooka stanowią jeden z najbardziej prawdopodobnych celów kradzieży kont**

**Facebook pozostaje preferowanym celem cyberprzestępców, którzy specjalizują się w kradzieży kont na portalach społecznościowych: według statystyk Kaspersky Lab, w I kwartale 2014 r. fałszywe strony imitujące Facebooka stanowiły 10,85% wszystkich wykryć modułów ochrony antyphishingowej.**

Więcej alarmów phishingowych wywołały jedynie fałszywe strony Yahoo, Facebook natomiast stanowił główny cel wśród portali społecznościowych.

Dzisiaj fałszowanie Facebooka to zjawisko globalne – cyberprzestępcy atakują ten portal w różnych językach: angielskim, francuskim, niemieckim, portugalskim, włoskim, tureckim, arabskim i innych.

Nieautoryzowany dostęp do kont na Facebooku lub jakimkolwiek innym portalu społecznościowym może być wykorzystany do rozprzestrzeniania odsyłaczy do stron phishingowych lub szkodliwego oprogramowania. Cyberprzestępcy wykorzystują również skradzione konta w celu wysyłania spamu na listy kontaktowe swoich ofiar oraz publikowania spamu na osiach czasu ich znajomych. Porwane konta mogą być również wykorzystywane do gromadzenia informacji dotyczących indywidualnych osób w celu wykorzystania ich w przyszłych atakach ukierunkowanych.

Właściciele smartfonów lub tabletów, którzy odwiedzają portale społecznościowe na swoich urządzeniach mobilnych, ryzykują również, że ich prywatne dane zostaną skradzione. Sprawę pogarsza dodatkowo fakt, że niektóre przeglądarki mobilne ukrywają pasek adresu podczas otwierania strony, co utrudnia użytkownikom rozpoznanie fałszywych zasobów.

„Cyberprzestępcy wymyślili wiele sposobów, aby nakłonić swoje ofiary do odwiedzenia stron zawierających treści phishingowe. Wysyłają odsyłacze za pośrednictwem poczty e-mail lub umieszczają je na portalach społecznościowych, lub banerach zlokalizowanych w zasobach osób trzecich. Oszuści często wabią swoje ofiary obietnicą ‘interesujących treści’. Po kliknięciu odpowiedniego odsyłacza użytkownicy trafiają na fałszywą stronę logowania, która zawiera standardowy komunikat proszący o zalogowanie się przed obejrzeniem strony. Jeżeli niczego niepodejrzewający użytkownicy podadzą swoje dane uwierzytelniające, zostaną one natychmiast przesłane cyberprzetępcom” – powiedziała **Nadieżda Demidowa**, analityk zawartości internetowej, Kaspersky Lab.

**Jak się chronić - porady ekspertów z Kaspersky Lab**

- Jeśli otrzymasz powiadomienie e-mail z Facebooka lub komunikat ostrzegający, że Twoje konto może zostać zablokowane, nigdy nie podawaj swoich danych uwierzytelniających w załączonym do takiej wiadomości formularzu. Facebook nigdy nie prosi użytkowników o podanie hasła w wiadomości e-mail ani o wysłanie go za pośrednictwem takiej wiadomości.

- Najedź kursorem na odsyłacz i sprawdź, czy prowadzi do oficjalnej strony Facebooka. Powinieneś ponadto wpisać ręcznie adres Facebooka na pasku adresu – cyberprzestępcy potrafią ukrywać adresy stron, do których zostaje w rzeczywistości skierowany użytkownik.

- Gdy adres URL zostanie wpisany ręcznie na pasku adresu, należy sprawdzić go ponownie po załadowaniu się strony, aby mieć pewność, że nie jest sfałszowana.

- Należy pamiętać, że Facebook wykorzystuje protokół HTTPS do transmitowania danych. Brak bezpiecznego połączenia prawdopodobnie oznacza, że odwiedzasz oszukańczą stronę, nawet jeśli adres URL wygląda na poprawny.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.