**Nowa fala ataków phishingowych na użytkowników produktów Apple**

**Kaspersky Lab Polska informuje o wykryciu nowej fali ataków phishingowych, w których cyberprzestępcy wyłudzają identyfikator Apple ID wykorzystywany przez użytkowników urządzeń Apple. Dostęp do tych danych pozwala atakującym na uzyskanie informacji osobowych oraz finansowych użytkowników. Atak rozprzestrzenia się m.in. w Polsce.**

Phishingowa wiadomość e-mail o temacie „Important Note: Unusual Access Acitivity in your account” (tłum.: Ważna wiadomość: Nietypowa aktywność związana z dostępem do Twojego konta) dociera do polskich użytkowników z rzekomego adresu „Apple”. W rzeczywistości adres ten jest zupełnie inny i można go zobaczyć wyświetlając pełny nagłówek e-maila.

Treść wiadomości zawiera odnośnik, który prowadzi do sfałszowanej strony przygotowanej tak, by wyglądała na oficjalną witrynę logowania Apple – znajdują się tam pola pozwalające na podanie identyfikatora Apple ID oraz hasła. Dane wprowadzone na tej stronie trafiają wprost do rąk cyberprzestępców, którzy automatycznie zyskują pełny dostęp do konta użytkownika w serwisach Apple (np. sklep z aplikacjami App Store czy chmura iCloud), łącznie z informacjami osobowymi i danymi dotyczącymi kart płatniczych.

Treść wiadomości wygląda następująco:

Wiadomość e-mail docierająca do użytkowników w ramach nowego ataku phishingowego

Po kliknięciu odnośnika „Update your information” (tłum.: Uaktualnij swoje informacje) następuje seria przekierowań, a użytkownik ostatecznie ląduje na sfałszowanej stronie logowania.

Sfałszowana strona logowania, na której cyberprzestępcy nakłaniają użytkowników do podania identyfikatora Apple ID oraz hasła

**Porady dla użytkowników: Jak zidentyfikować phishingowe strony i e-maile**

Jednym ze sposobów na odróżnienie strony fałszywej od prawdziwej jest przyjrzenie się paskowi adresu w przeglądarce internetowej. W omawianym ataku zamiast „apple.com” widnieje tam długi ciąg znaków rozpoczynający się od „pctechief.com”. Warto pamiętać, że identyfikacja strony phishingowej jest znacznie trudniejsza, gdy użytkownik korzystający z iPhone'a lub iPada nie widzi całego adresu URL strony - co jest typowe dla przeglądarki Safari dla systemów iOS.

Aby zidentyfikować sfałszowaną wiadomość e-mail, należy przede wszystkim zweryfikować pełny adres nadawcy e-maila. Na komputerze wystarczy ustawić kursor myszy nad adresem nadawcy, w wyniku czego pojawi się pole przedstawiające pełny, prawdziwy adres, a nie tylko alias widoczny w oknie programu pocztowego. W przypadku smartfona lub tabletu należy dotknąć adres nadawcy - spowoduje to pojawienie się pełnego adresu.

Aby zabezpieczyć się przed wyciekiem danych, użytkownicy powinni zastosować dwustopniową weryfikację identyfikatora Apple ID. Po włączeniu tej opcji użytkownik otrzyma SMS-a z czterocyfrowym kodem na jedno lub więcej wybranych urządzeń. Kod ten pełni funkcję dodatkowej weryfikacji i zapobiega niechcianym zmianom na stronie Apple ID.

Niestety nawet korzystanie z dwustopniowej weryfikacji nie powstrzyma cyberprzestępców przed użyciem skradzionych danych finansowych, gdy już uda się im do nich dostać. Dlatego bardzo ważne jest, by użytkownicy nie klikali odsyłaczy w podejrzanych wiadomościach e-mail. Dodatkowo, użytkownicy komputerów Mac powinni zaopatrzyć się w dobre rozwiązanie bezpieczeństwa, takie jak [Kaspersky Security for Mac](http://kaspersky.pl/kis), które zabezpieczy sprzęt przed wirusami, trojanami, oprogramowaniem szpiegującym i atakami phishingowymi w czasie rzeczywistym.

Więcej informacji o atakach phishingowych na użytkowników sprzętu i usług firmy Apple znajduje się w raporcie opublikowanym w serwisie SecureList.pl prowadzonym przez Kaspersky Lab: [http://securelist.pl/blog/7232,jablko\_niezgody.html](http://securelist.pl/blog/7232%2Cjablko_niezgody.html).

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>.