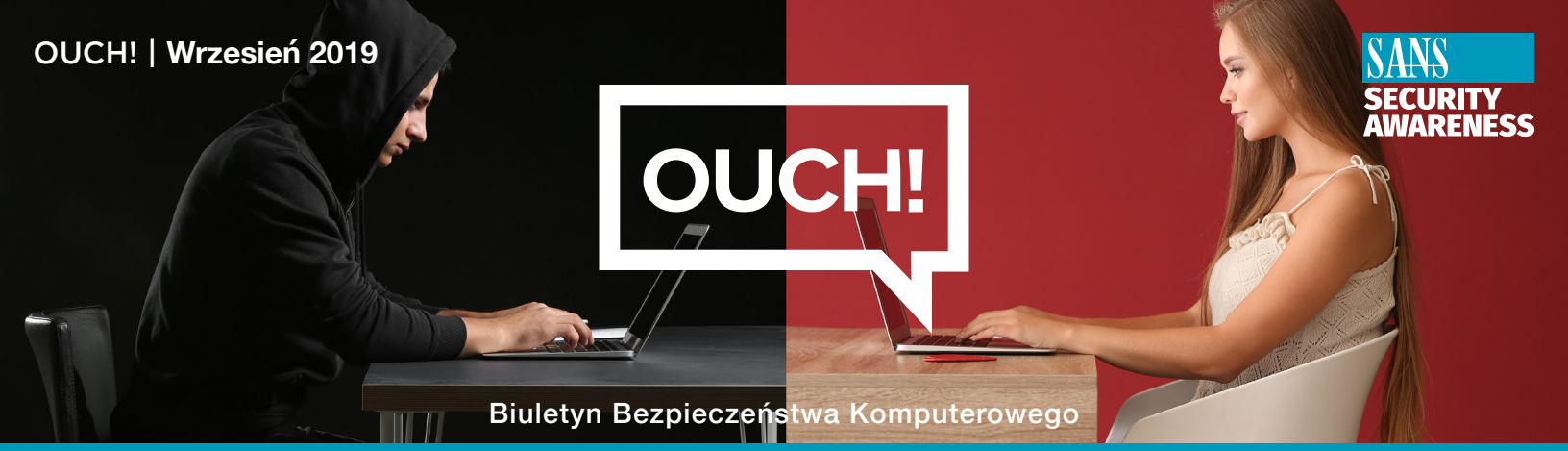

Biuletyn Bezpieczeństwa Komputerowego

Oszustwa za pośrednictwem mediów społecznościowych

Wstęp

Wielu z nas otrzymuje w domu bądź w pracy maile, które wyglądają na godne zaufania, gdzie jako nadawca widnieje bank, szef lub ulubiony sklep internetowy. W rzeczywistości mogą to być maile phishingowe, w których atakujący próbują wykorzystać naszą naiwność i skłonić nas do działań których powinniśmy unikać jak np. otwieranie zainfekowanych załączników, podawanie hasła bezpieczeństwa lub przelewanie pieniędzy. Im bardziej jednak udaje się zwalczać tego rodzaju ataki tym więcej nowych sposobów oszustw wynajdują przestępcy.

Próby oszustw odbywają się najróżniejszymi kanałami komunikacji: Skype, WhatsApp, Slack, Twitter, Facebook, Snapchat, Instagram a nawet gry aplikacyjne. Komunikacja za pośrednictwem tych platform wydaje się bardziej nieformalna i godna zaufania, co jest właśnie czynnikiem ułatwiającym wykorzystanie ich do oszukiwania ofiar. Ponadto obecnie powszechna dostępność zaawansowanej technologii umożliwia z łatwością każdemu przestępcy na świecie podszywanie się pod kogokolwiek zechce. Pamiętajmy o tym, że nie każda osoba która się z nami kontaktuje jest tym kim za kogo się podaje.

Kluczowe elementy

Poniżej zostały przedstawione podstawowe wskazówki, które umożliwią zidentyfikowanie maila który jest próbą ataku phishingowego.

"Pilne": Wiadomości która bazuje na wrażeniu pilności, wymaga "natychmiastowego działania" aby zapobiec negatywnym skutkom takim jak: zamknięcie konta czy pójście do więzienia. Atakujący liczy na twoje potknięcie pod wypływem pośpiechu

Presja: nakłanianie do tego aby ominąć lub zignorować procedury i politykę bezpieczeństwa w miejscu pracy

Ciekawość: Jeśli wygraliśmy w loterii jako milionowy klient to zbyt piękne aby mogło być prawdziwe, jednak atakujący wykorzystują naturalną ciekawość ofiar.

Wrażliwe informacje: Żądanie podania wyjątkowo wrażliwych danych takich jak numer karty kredytowej, hasło lub innych informacji których nie jesteśmy skłonni ujawniać w normalnych okolicznościach

Pisma urzędowe: Wiadomość, która pochodzi rzekomo od oficjalnej instytucji ale napisana jest łamaną polszczyzną. Większość organizacji publicznych nie komunikuje się za pośrednictwem mediów społecznościowych. Jeśli nie jesteśmy pewni, potwierdźmy otrzymanie wiadomości, kontaktując się pośrednictwem rozmowy telefonicznej na numer umieszczony na oficjalnej stronie urzędu

Podszywanie się: Wiadomość od współpracownika, którego styl lub dobór słów nie pasuje do niego. Jeśli coś podejrzewamy zadzwońmy do znajomego aby potwierdzić czy ktoś się pod niego nie podszywa. Cyberprzestępcy z łatwością mogą stworzyć wiadomość która wygląda jakby przyszła od znajomego np. poprzez przejęcie jednego z jego kont pocztowych i wysyłanie z niego wiadomości. Zwracajmy szczególną uwagę na wiadomości na Twitterze i inne krótkie formy w których trudno rozróżnić tożsamość nadawcy

Nasza czujność jest najlepszą linią obrony przed atakami i oszustwami. Jeśli wiadomość bądź poczta wygląda podejrzanie, po prostu zignorujmy ją lub usuńmy. Ewentualnie jeśli pochodzi od osoby którą znamy, zadzwońmy do niej aby potwierdzić, że ją wysłała.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK, powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.

WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor wydania

Dr Jessica Barker *(@drjessicabarker) to wiodący specjalista z zakresu czynnika ludzkiego w cyberbezpieczeństwie. Znana wykładowczyni i przewodnicząca ClubCISO, a jako wiceprezes Cygenta promuje na całym świecie: świadomość, etykietę i kulturę cyberbezpieczeństwa.*

Źródła

Socjotechnika:	https://www.sans.org/u/Uz6
Oszustwa telefoniczne oraz scam:	https://www.sans.org/u/Uzb
Powstrzymać phishing:	https://www.sans.org/u/Uzg
Spersonalizowane oszutwa:	https://www.sans.org/u/Uzl

Biuletyn OUCH! powstaje w ramach programu „Security Awareness" Instytutu SANS i jest wydawany na licencji Creative Commons BY-NC-ND 4.0 license. Powielanie treści biuletynu jest dozwolne jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści oraz nienaruszania zawartości samego biuletynu. Informacje kontaktowe: www.sans.org/security-awareness/ouch-newsletter. Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Polski przekład (NASK/CERT Polska): Bartłomiej Wnuk, Konrad Purzycki, Janusz Urbanowicz