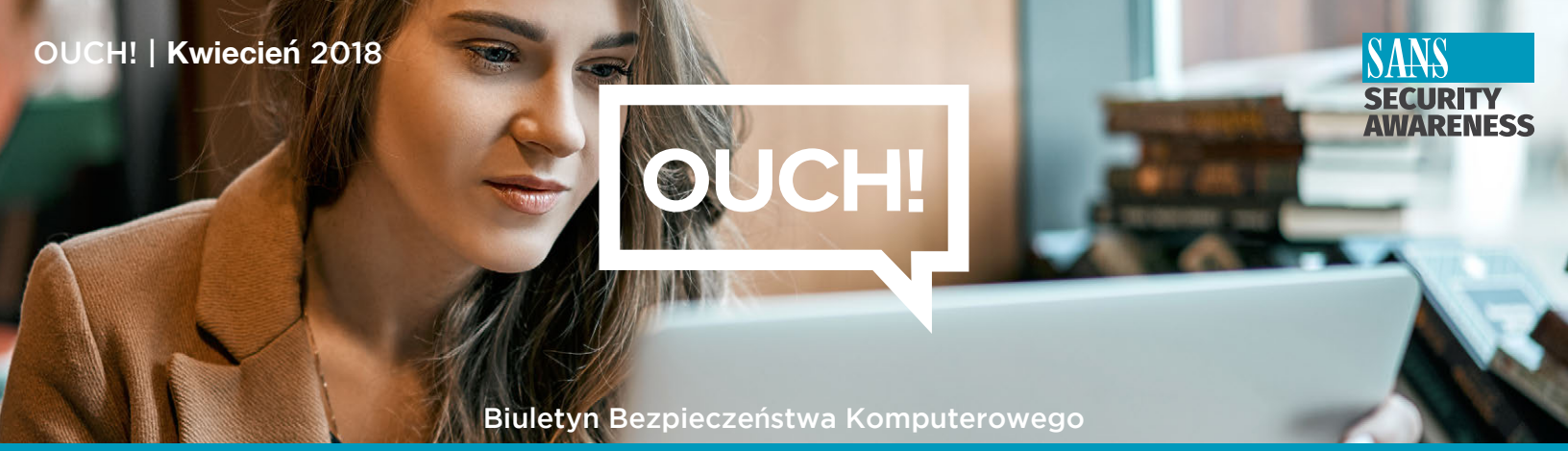

SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Powstrzymać phishing

Wstęp

Email oraz serwisy takie jak Skype, Twitter czy Snapchat stanowią obecnie jeden z podstawowych sposobów komunikacji zarówno w pracy jak i w życiu prywatnym. Ponieważ społeczeństwo w dużej mierze opiera swoją komunikację na wiadomościach elektronicznych, stały się one jednym z wiodących wektorów ataku wykorzystywanym przez przestępców. Zazwyczaj wykorzystywaną tu metodą ataku jest phishing. W bieżącym wydaniu opiszemy, w jaki sposób zorientować się, że jesteśmy atakowani oraz powstrzymać złośliwe działania.

Czym jest phishing

Phishing to typ ataku, w którym przestępcy używając specjalnie spreparowanych wiadomości chcą wprowadzić ofiarę w błąd i nakłonić do wykonania czynności, której nie powinna wykonać, jak na przykład kliknięcie w złośliwy link, podanie hasła na niezaufanej stronie czy otwarcie zainfekowanego załącznika. Atakujący starają się wykorzystywać fałszywe informacje w taki sposób by wzbudzić w Tobie pożądane emocje, poczucie zaciekawienia, lub potrzebę podjęcia natychmiastowego działania. W wiadomościach mogą podszywać się pod znajomego, którego dobrze znasz czy firmę, z której usług regularnie korzystasz. Przestępcy potrafią podrobić logo instytucji (np. Twojego banku) oraz wysłać wiadomość z adresu o łudząco podobnej nazwie (co dodatkowo zwiększa ich wiarygodność). Tego typu kampanie wysyłane są zazwyczaj na masową skalę. Im większa liczba adresatów, tym większe prawdopodobieństwo, że ktoś “połknie haczyk”.

Sposoby zabezpieczania się

W większości przypadków, otwarcie oraz odczytanie wiadomości nie prowadzi jeszcze do niczego złego. Aby phishing był skuteczny, atakujący muszą nakłonić ofiarę do wykonania pewnej czynności. Na szczęście istnieją przesłanki mogące pomóc w odpowiednio wczesnym wykryciu ataku. Poniżej prezentujemy kilka z nich:

- Wiadomość wywołuje u odbiorcy potrzebę podjęcia natychmiastowego działania, gdyż w innym wypadku wydarzy się coś złego. Korzystając z tej metody, atakujący próbuje sprowokować ofiarę do wykonania nieprzemyślanych działań.
- Atakujący próbuje nakłonić odbiorcę do ominięcia lub zignorowania procedur panujących w firmie.
- Treść wiadomości sprawia wrażenie czegoś zbyt pięknego, aby było prawdziwe (przykładem może być informacja o wysokiej wygranej).

- Bądź podejrzliwy w stosunku do wiadomości adresowanych w sposób ogólny, jak na przykład “Szanowny Kliencie”.
- Wiadomość zawiera pytanie o informacje, które nadawca powinien już znać lub zapytanie dotyczące danych wrażliwych (takich jak numer karty płatniczej, czy hasło).
- Nadawca twierdzi, że jest z dużej organizacji, ale mail zawiera dużo błędów językowych lub jest wysłany z ogólnodostępnych adresów @gmail.com, @wp.pl, lub @hotmail.com.
- Otrzymana wiadomość jest od znajomego, ale jej ton lub zastosowane zwroty nie pasują do tej osoby. Jeśli masz podejrzenia, zadzwoń do nadawcy i zweryfikuj czy kontaktował się z Tobą. Przestępcy mogą bardzo łatwo podrobić e-mail od przyjaciela bądź kolegi z pracy.

Zdrowy rozsądek to podstawowa linia obrony. Jeśli mail lub wiadomość wydają się być podejrzane, lub ich treści wskazują na coś nieprawdopodobnego - może to wskazywać na atak phishingowy.

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

Edytor gościnny

Tonia Dudley od 2011 roku opracowuje oraz prowadzi szkolenia w dziedzinie zwiększania świadomości dotyczącej bezpieczeństwa. Wśród nich m.in. nagradzany program w zakresie ochrony przed phishingiem. W mediach społecznościowych można ją znaleźć pod adresem www.linkedin.com/in/toniadudley.

Przydatne linki

Inżynieria Społeczna:	https://www.sans.org/u/Cb1
O tym, jak pomóc innym zabezpieczyć się:	https://www.sans.org/u/Cb6
Email – kilka prostych porad:	https://www.sans.org/u/Cbg
CEO Fraud:	https://www.sans.org/u/Cbl
Archiwum biuletynów OUCH!:	https://www.sans.org/u/Cbq

Licencja

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski