OUCH! | Grudzień 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..



# Phishing i oszustwa w e-mailach

## Wstęp

E-mail to jeden z podstawowych sposobów komunikacji. Nie tylko używamy go codziennie w pracy, ale dzięki niemu pozostajemy w kontakcie z przyjaciółmi i rodziną. Ponadto e-mail jest używany przez firmy do kontaktu z klientem w takich sprawach jak potwierdzenie zakupów online czy przesłanie informacji o zmianach na koncie bankowym. Ponieważ ludzie tak bardzo opierają swoją komunikację na poczcie elektronicznej, stała się ona jednym z podstawowych narzędzi do dokonywania ataków. W tym numerze biuletynu zostaną wyjaśnione niebezpieczeństwa związane z wiadomościami e-mail i kroki jakie można podjąć, aby się ochronić.

### Redaktor gościnny

Dr Lance Hayden jest Dyrektorem Zarządzającym w Berkeley Research Group. Jest też ekspertem w dziedzinie zachowań i kultury związanej z bezpieczeństwem IT oraz autorem książki People-Centric Security: Transforming Your Enterprise Security Culture wydanej przez McGraw-Hill. Jego profil zawodowy dostępny jest pod adresem: www.linkedin.com/in/drhayden.

## Phishing

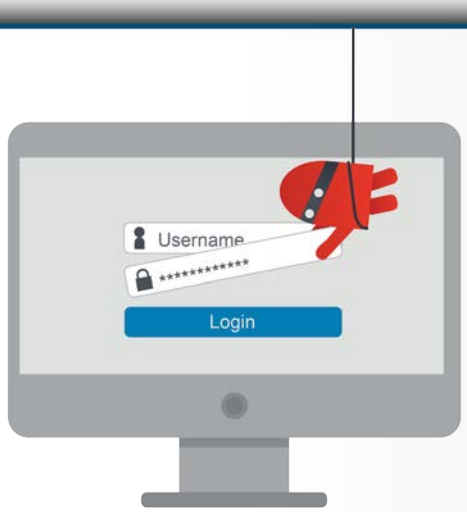
Phishing to jeden z najpopularniejszych ataków opartych o wiadomości e-mail, ale także coraz częściej o wiadomości na portalach społecznościowych. Przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami. Atakujący bardzo skrupulatnie przygotowują treść takich wiadomości. Mogą udać, że mail pochodzi od kogoś kogo znasz, jak na przykład od kolegi lub firmy, której ufasz. Potrafią nawet podrobić logo banku lub wysłać wiadomość z podobnego adresu. Cyberprzestępcy wysyłają takie wiadomości do tysięcy, a nawet milionów odbiorców na całym świecie. Doskonale wiedzą, że im więcej takich wiadomości roześlą, tym więcej osób będą mogli oszukać. Ten sposób jest podobny do sposobu znanego z łowienia ryb: im większą masz sieć, tym więcej złowisz ryb. Ataki typu phishing mają najczęściej następujące cele:

- **Wyłudzanie informacji**: Celem atakującego jest zmanipulowanie Cię tak, abyś kliknął na link, który zabierze Cię na stronę pytającą o login i hasło, Twój ulubiony kolor czy nazwisko panieńskie matki. Takie strony bliźniaczo przypominają na przykład znane strony banku, jednak są zaprojektowane tylko po to, żeby wykraść dane potrzebne do uzyskania dostępu do Twojego konta bankowego czy numer karty kredytowej.
- **Przejęcie kontroli nad komputerem poprzez złośliwy link**: Tym razem celem atakującego jest zainfekowanie Twojego komputera. Aby to osiągnąć wysyłają do Ciebie wiadomość z linkiem. Po kliknięciu

# Phishing i oszustwa w e-mailach

na taki link zostajesz przekierowany na stronę, która w tle przeprowadza atak na Twoją przeglądarkę internetową i kiedy atak ten się powiedzie, przestępca uzyskuje kontrolę na Twoim komputerem.

- **Przejęcie kontroli nad komputerem poprzez złośliwe załączniki**: Złośliwe wiadomości mogą zawierać zainfekowane załączniki, takie jak pliki PDF lub dokumenty Microsoft Office. Jeśli otworzysz taki załącznik, atakuje on Twój komputer i jeśli atak się powiedzie, przestępca uzyskuje nad nim kontrolę.
- **Scam**: Niektóre maile to po prostu próby oszustwa i kradzieży. Klasycznym przykładem są wiadomości informujące o wygranej w loterii, albo że jakaś ważna osobistość potrzebuje przelać miliony dolarów do Twojego kraju i chciałaby Ci zapłacić za pomoc w tym transferze. Następnie zostajesz poinformowany, że musisz zapłacić opłatę manipulacyjną zanim otrzymasz pieniądze. Kiedy zapłacisz, już nigdy się nie odezwie.




*Użyj zdrowego rozsądku. Jeśli treść wiadomości e-mail jest podejrzana lub zbyt obiecująca, najprawdopodobniej jest to atak.*

## Jak się chronić

Zazwyczaj otwieranie wiadomości e-mail jest bezpieczne. W większości przypadków, aby atak się powiódł, to Ty musisz zrobić coś po przeczytaniu takiego e-maila. Poniżej znajduje się kilka wskazówek, jak rozpoznać, że otrzymana wiadomość to atak.

- Bądź podejrzliwy jeśli jakikolwiek e-mail wymaga natychmiastowego działania lub powoduje wrażenie pilności. To znany trik, aby zmusić ludzi do szybkiego działania.
- Zachowaj ostrożność jeśli wiadomość zawiera załącznik, szczególnie jeśli nie spodziewałeś się takiej wiadomości. Przykładami są: lista płac, nieplanowane zwolnienia albo mail od urzędu skarbowego.
- Bądź podejrzliwy w stosunku do e-maili adresowanych podobnie jak „Dear Customer” / ”Drogi Kliencie” lub w inny, bardzo ogólny sposób.
- E-mail wymaga podania szczególnie ważnych informacji jak numeru karty kredytowej czy haseł.
- Nadawca twierdzi, że jest z dużej organizacji, ale mail zawiera dużo błędów i jest wysłany z adresu @gmail.com, @yahoo.com, lub @hotmail.com.
- Jeśli link wydaje Ci się podejrzany, najedź na niego myszką (nie klikając). Wówczas ukaże się prawdziwy adres,

# Phishing i oszustwa w e-mailach

pod który zaprowadziłby Cię ten odnośnik jeśli byś na niego kliknął. Link, który widzisz w wiadomości może być zupełnie inny niż miejsce, do którego rzeczywiście prowadzi.

- Dostajesz wiadomość od znajomego, ale jej ton lub zastosowane zwroty po prostu nie pasują do tej osoby. Jeśli masz podejrzenia, spytaj nadawcy czy się z Tobą kontaktował. Cyberprzestępcy mogą bardzo łatwo podrobić e-mail od znajomego bądź kolegi z pracy.

Aby bezpiecznie korzystać z poczty elektronicznej, należy po prostu użyć zdrowego rozsądku. Jeśli coś wydaje się podejrzane lub zbyt obiecujące, to zapewne jest to atak. Dla zachowania bezpieczeństwa skasuj taką wiadomość.

## Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

## 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

## Linki

| | |
|---|---|
| OnGuard Online – Jak uniknąć SCAMu (EN): | https://www.onguardonline.gov/topics/avoid-scams |
| Anti-Phishing Working Group (EN): | https://www.apwg.org |
| Phishtank (EN): | https://www.phishtank.org |
| Definicje pojęć związanych z bezpieczeństwem (EN): | https://www.securingthehuman.org/resources/security-terms |



Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski