

Trzeci numer Cyber Poradnika poświęcamy najpopularniejszej formie oszustw w Internecie, których cyberprzestępcy dopuszczali się w 2019 roku, a mianowicie phishingowi.

E-mail to podstawowa forma komunikacji w Internecie. Używana jest praktycznie codziennie. Za jej pośrednictwem pozostajemy w kontakcie z bliskimi czy przekazujemy informacje pomiędzy współpracownikami. Firmy w ten sposób mogą kontaktować się z klientami informując ich o swojej ofercie, promocjach, realizacji zamówień czy zmianach w regulaminie. Dlatego też poczta elektroniczna stała się głównym wektorem ataku dla cyberprzestępców. W dzisiejszym wydaniu **Cyber Poradnika** chcemy przedstawić Wam na jakie zagrożenia możecie być narażeni używając komunikacji e-mailowej oraz jak bronić się przed potencjalnymi atakami ze strony cyberprzestępców.

Czym jest phishing?



Najbardziej rozpowszechnioną formą ataku, która jest wykorzystywana podczas komunikacji e-mailowej jest phishing. Phishing jest metodą oszustwa polegającą na podszyciu się przestępca pod inną osobę/instytucję w celu oszukania użytkownika. Napastnikowi zależy na zdobyciu Twojego zaufania, aby w ten sposób uzyskać interesujące go dane. Cyberprzestępcy masowo wysyłają tysiące podejrzanych wiadomości do milionów



Jak nie dać się „złowić”, czyli czym jest phishing i jak się przed nim bronić?

użytkowników Internetu. Ten sposób działania gwarantuje, że uda się im „złowić” jak najczęściej nieuważnych lub nieświadomych ofiar.

Obecnie phishing przybiera coraz bardziej wyrafinowane formy, a cyberprzestępcy coraz częściej przygotowują spersonalizowany atak pod danego użytkownika bądź instytucję, na początku zbierając dane z dostępnych źródeł na ich temat (tzw. **spear phishing**, czyli najbardziej skuteczna obecnie odmiana phishingu). Możemy wyróżnić również **clone phishing** (wiadomość przygotowywana jest przez cyberprzestępcę na podstawie autentycznego e-maila) oraz **whaling** (phishing skierowany do kierownictwa wyższego szczebla). W tym miejscu warto zauważyć, że obecnie phishing nie dotyczy jedynie poczty elektronicznej. Coraz częściej ataki tego typu przeprowadzane są za pośrednictwem wiadomości prywatnych w mediach społecznościowych.

Obecnie można wyróżnić kilka głównych celów ataków wykonywanych metodą phishingu:

- **Wyłudzenie danych.** Podstawowy cel przyświecający cyberprzestępcom podczas przeprowadzania ataku phishingowego jest wyłudzenie Twoich informacji wrażliwych. Uzyskanie Twojego numeru karty płatniczej czy też danych logowania do Twojego konta w banku umożliwi atakującemu na dostęp do Twoich pieniędzy.
- **Zainfekowany plik.** Przesłanie za pośrednictwem e-maila zainfekowanego pliku w załączniku to również popularny wektor ataku. Cyberprzestępca przesyłając Ci fałszywą fakturę, list przewozowy lub link do pobrania jakiegoś pliku chce nakłonić Cię do jego otworzenia na Twoim urządzeniu. W ten sposób ma nadzieję zainfekować Twój komputer oprogramowaniem złośliwym (więcej na temat oprogramowania złośliwego opowiemy Ci w kolejnych wydaniach Cyber Poradnika). To z kolei może doprowadzić do zaszyfrowania Twoich plików, wycieku informacji przechowywanych na komputerze lub całkowitej blokady Twojego urządzenia.
- **Nakłonienie ofiary do określonego działania.** Poprzez przesłanie do Ciebie fałszywej wiadomości atakujący chce Cię nakłonić do konkretnego, zaplanowanego przez siebie działania. W tym celu ucieka się do zastosowania socjotechnik (o których napiszemy jeszcze w tym miesiącu), aby wymóc na Tobie zachowanie na jakim mu zależy.

Jak go rozpoznać?



Aby z powodzeniem bronić się przed atakami phishingowymi musisz wiedzieć jak je rozpoznać. Poniżej kilka rad, dzięki którym poznasz proste metody identyfikacji podejrzanych wiadomości.

- **Nakłanianie do działań.** Jeśli czujesz, że jesteś przymuszany do jakiś konkretnych działań/zachowań lub nadawca wiadomości nadaje jej charakteru pilności powinieneś nabrać podejrzeń co do takiego e-maila. To znane socjotechniki wykorzystywane przy phishingu.
- **Błędy.** Błędy ortograficzne lub interpunkcyjne, literówki, niepoprawna składnia, zdanie brzmiące jak przetłumaczone przez translator online to niektóre ze znaków alarmowych, że wiadomość może by fałszywa.
- **Nie klikaj w link.** Jeśli masz wątpliwości co do prawdziwości wiadomości pod żadnym pozorem nie klikaj w zawarte w niej linki. Natomiast w przypadku, gdy wiadomość wydaje się prawdziwa, a nie masz pewności co zawartego w niej linku możesz w prosty sposób sprawdzić dokąd Cię skieruje. Nie klikając w hiperłącze najedź kursorem na podejrzany link. W ten sposób zobaczysz jego prawdziwe źródło.
- **Zbyt dużo informacji.** W przypadku, jeśli nadawca wymaga od Ciebie podania wrażliwych informacji jak dane karty czy konta w bankowości elektronicznej zdecydowanie nabierz podejrzeń i nie odpowiadaj na takiego e-maila.
- **Styl.** Wiadomość pochodzi od znanej Ci osoby, ale jej styl, charakter bądź treść kompletnie do niej nie pasują? Może to być oznaka, że ktoś wykorzystuje jej wizerunek w celu przeprowadzenia na Tobie ataku phishingowego.
- **Adres e-mail nadawcy.** Nadawca podaje się za ważną osobę z branży a jej mail



Jak nie dać się „złować”, czyli czym jest phishing i jak się przed nim bronić?

pochodzi z adresu e-mail zarejestrowanego u jednego z popularnych dostawców poczty (jak np. Gmail lub Yahoo)? Jest to przesłanka co do tego, że mail może mieć charakter phishingu.

Podczas korzystania z poczty elektronicznej zachowaj ostrożność oraz ograniczone zaufanie do nadawcy wiadomości. Jeśli masz wątpliwości co do wiarygodności e-maila dla własnego bezpieczeństwa usuń taką wiadomość. Zachęcamy Cię do odwiedzenia naszych profili w mediach społecznościowych ([Facebook](#) oraz [Twitter](#)), gdzie możemy podyskutować na temat bezpieczeństwa w sieci.

Czytałeś już nasze wcześniejsze numery **Cyber Poradnika**? Jeśli nie to serdecznie zachęcamy Cię do ich lektury i podnoszenia świadomości nt. cyberbezpieczeństwa.

[Cyber Poradnik nr 1 - Bezpieczne zakupy](#)

[Cyber Poradnik nr 2 - Co zrobić, gdy padniesz ofiarą cyberprzestępcy?](#)