MyFiz.io

Zabezpiecz się przed wyłudzeniem danych pocztą elektroniczną

Nie podawaj danych w odpowiedzi na maila

Żadna firma ani instytucja nie wyśle prośby o zmianę/podanie określonych danych drogą mailową. Organizacja rządowa nie prosiłaby o wysyłanie danych medycznych pacjentów poprzez maila. Jeśli otrzymamy takiego maila, warto najpierw sprawdzić adres z jakiego przyszła wiadomość. Najczęściej taki mail składa się z ciągu znaków, lub posiada nazwę niezwiązaną z daną instytucją. Dodatkowo często w treści maila pojawiają się błędy składniowe, lub inne sygnały, iż wiadomość wygenerowana została automatycznie.

Nie klikaj w linki znajdujące się w treści maila

Czasami zdarza się, iż atak jest tak dobrze przygotowany, iż wygląda jakby rzeczywiście został wysłany przez konkretną instytucję. W takim jednak przypadku linki prowadzą do strony, która przygotowana została na wzór strony firmy, pod którą podszywają się cyberprzestępcy. Ma ona jednak na celu wyłudzić dane. Zawsze więc wyszukuj stronę firmy bezpośrednio w przeglądarce, oraz sprawdzaj szyfrowanie https, które znajdują się w lewym górnym roku przy adresie strony internetowej. Każda strona, na której wymagane jest logowanie powinna posiadać https. Brak takiego certyfikatu powinien wzbudzić naszą czujność.

Dostajesz maila z prośbą o pilną reakcję? Ignoruj

Jest to jedna z socjotechnik mających na celu przykucie naszej uwagi, oraz zareagowanie zanim moglibyśmy zrobić się podejrzliwi. Zawsze jednak warto się upewnić, że taki mail nie jest próbą ataku.
PS. Nie odpowiadamy za skutki uboczne nieustannego ignorowania wiadomości od szefa z prośbą o pilną odpowiedź :)

Zachowaj nieustanną czujność

Cyberprzestępcy nie śpią. Jeśli jakaś technika przestaje być skuteczna, obmyślają nowy sposób na wyłudzenie danych. Dlatego też zawsze bądź podejrzliwy i upewnij się kilka razy, zanim wykonasz jakieś działanie. Bo lepiej stracić w życiu sekundę na sprawdzenie informacji, niż stracić dane w sekundę.

Masz pytania? Skontaktuj się z nami!

info@myfiz.io