Quiz wiedzy

O BEZPIECZEŃSTWIE W SIECI

wyniki

7 pytań dotyczących bezpieczeństwa w sieci
24 dni na udział w quizie
17 punktów do zdobycia

Zobacz, jak poradzili sobie uczestnicy Quziu!
4566 osób odpowiedziało na wszystkie pytania
13 to średnia liczba zdobytych punktów

Jak odpowiadali użytkownicy

97% uczestników quizu potrafiło rozpoznać SMS-y, które mogą być próbą oszustwa, nieco mniej, bo 90% wie, jak zachować się w przypadku otrzymania takiej wiadomości

Przypominamy!
Jeśli podejrzewasz, że SMS, który otrzymałeś może być próbą oszustwa – nie klikaj w linki w nim zawarte, nie otwieraj załączników. Najlepiej skontaktuj się z potencjalnym nadawcą (np. sklepem internetowym, kurierem czy sprzedawcą prądu), aby sprawdzić autentyczność wiadomości.

90% uczestników quizu poprawnie wskazało, że nie można otwierać linków czy załączników w podejrzanych wiadomościach mailowych.

10% błędnie wskazało, że to dobra praktyka.

Przypominamy!
Gdy nie masz pewności, że wiadomość jest prawdziwa nie odpowiadaj na wiadomości, nie otwieraj załączników i nie klikaj w linki w niej zawarte.

Tylko **75%** badanych zna zasady postępowania w przypadku podejrzenia phishingu

Przypominamy!
Każde podejrzenie próby oszustwa powinno zgłosić się do firmy/instytucji, pod którą podszywa się oszust. Dobrą praktyką jest również zgłoszenie do CERT Polska – instytucji, która prowadzi rejestr takich incydentów.

67% badanych poprawnie wskazało, że hasła maskujące są narzędziem stosowanym w celu zwiększenia bezpieczeństwa użytkowników internetu

Przypominamy!
Banki i inne instytucje stosują szereg zabezpieczeń do systemów logowania. Najbardziej popularne z nich to m.in. podwójne uwierzytelnianie.

Wśród działań, które służą zwiększeniu bezpieczeństwa w sieci, uczestnicy quziu najczęściej wskazywali:

1265
Korzystanie z mendżera haseł

3221
Włączanie podwójnego uwierzytelniania

2812
Unikanie publicznie dostępnych, niezabezpieczonych sieci WiFi

2946
Regularnie aktualizuję programy antywirusowe na sprzęcie komputerowym

Najmniej znanym narzędziem, które służy zwiększaniu bezpieczeństwa użytkowników internetu są klucze U2F. Taką odpowiedź wskazało tylko
730 osób

Przypominamy!
Klucze U2F wyglądem przypominają pendrive. To urządzenia, które są jednym z najskuteczniejszych sposobów ochrony przed phishingiem. Zasada ich działania jest prosta – możliwość zalogowania się do wybranych systemów będziesz miał tylko po włożeniu klucza do portu USB Twojego komputera.

Więcej informacji o bezpieczeństwie w sieci znajdziesz na **tauron.pl/bezpieczenstwo**