Phishing - rozpoznawanie i reagowanie na próby wyłudzeń

Prezentacja ta pomoże Ci rozpoznawać próby phishingu i skutecznie na nie reagować. Poznasz praktyczne wskazówki, które zwiększą Twoje bezpieczeństwo w sieci.

Na co zwracać uwagę przy korzystaniu ze stron internetowych?

Protokół HTTPS

Sprawdź, czy adres URL rozpoczyna się od https://, a nie tylko http://. Brak litery „s" oznacza brak szyfrowania.

Ikona kłódki

Upewnij się, że na pasku przeglądarki widoczna jest zamknięta kłódka. To znak, że połączenie jest szyfrowane.

Dokładny adres

Przyjrzyj się, czy adres strony nie zawiera podejrzanych znaków lub nieznacznych zmian w pisowni.

Czego należy się wystrzegać?

Niezabezpieczone strony

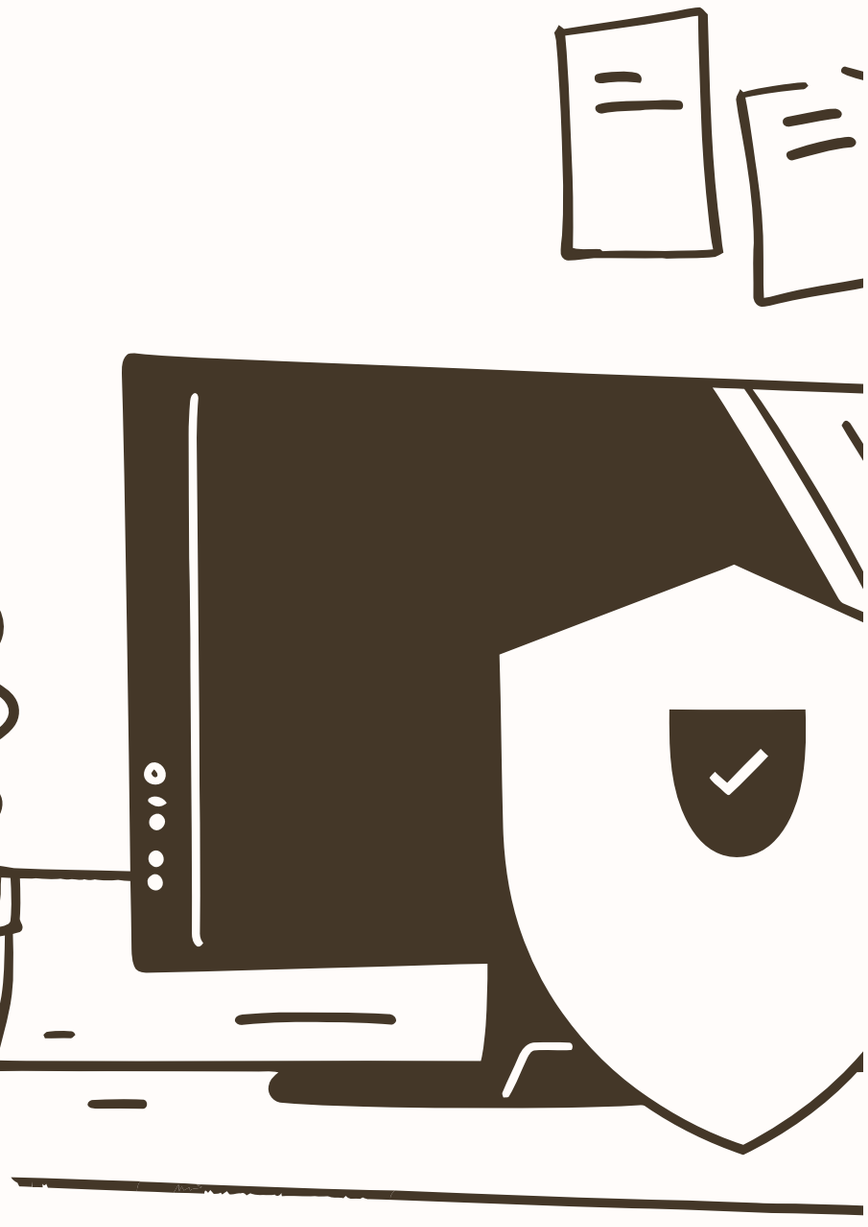
Nigdy nie podawaj ważnych danych na stronach korzystających z niezabezpieczonego protokołu http://.

Linki w e-mailach

Unikaj logowania się do serwisów przez odnośniki w e-mailach. Lepiej samodzielnie wpisać adres.

Podejrzane załączniki

Nie klikaj w linki i nie otwieraj załączników z niespodziewanych wiadomości.



Jak zwiększyć poziom bezpieczeństwa?

Oprogramowanie ochronne

Zainstaluj i korzystaj z oprogramowania antywirusowego oraz chroniącego przed phishingiem.

Regularne aktualizacje

Regularnie aktualizuj system operacyjny, przeglądarki, wtyczki i inne aplikacje.

Ograniczone zaufanie

Każda podejrzana wiadomość lub element strony powinien wzbudzić Twoją czujność.

Unikalne hasła

Nie używaj tego samego lub bardzo podobnego hasła w różnych usługach internetowych.

O czym pamiętać w kontekście phishingu?

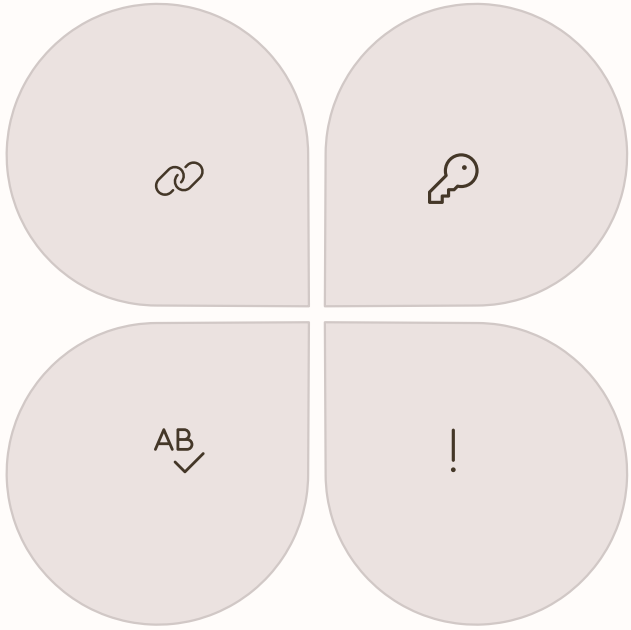
⚠ Skuteczność ataku nie zależy od siły Twojego hasła. Jeśli wpiszesz je na fałszywej stronie, przestępca i tak je pozna.

Fałszywe adresy stron mogą wyglądać bardzo podobnie do prawdziwych, z drobnymi zmianami, np. cyfra „0" zamiast litery „o".

Jak rozpoznać podejrzaną wiadomość?

Podejrzane odnośniki

Zawiera prośbę o zalogowanie się przez podany odnośnik.



Prośba o dane

Zachęca do podania hasła, np. rzekomo w celu sprawdzenia wycieku danych.

Błędy językowe

Błędy ortograficzne, dziwna składnia lub nieprofesjonalny styl.

Wywołanie emocji

Treść ma wywołać strach, presję lub poczucie winy.

Jak rozpoznać fałszywą stronę?

Adres URL

Adres zaczyna się od Http:// zamiast Https://. Może zawierać literówki lub manipulacje.

Nietypowe formularze

Wymagane są nietypowe elementy weryfikacji, jak kilka kodów jednorazowych.

Podejrzane okna

Logowanie odbywa się w małym, osobnym okienku (pop-up).

Wygląd strony

Strona jest niekompletna graficznie, brakuje elementów lub wygląda przestarzale.

Co zrobić, jeśli padniesz ofiarą ataku?

Natychmiastowe zgłoszenie

Zgłoś incydent do odpowiedniego podmiotu – banku, operatora serwisu, portalu.

Blokada dostępu

Zastrzeż karty i zablokuj dostęp do konta do czasu wyjaśnienia sytuacji.

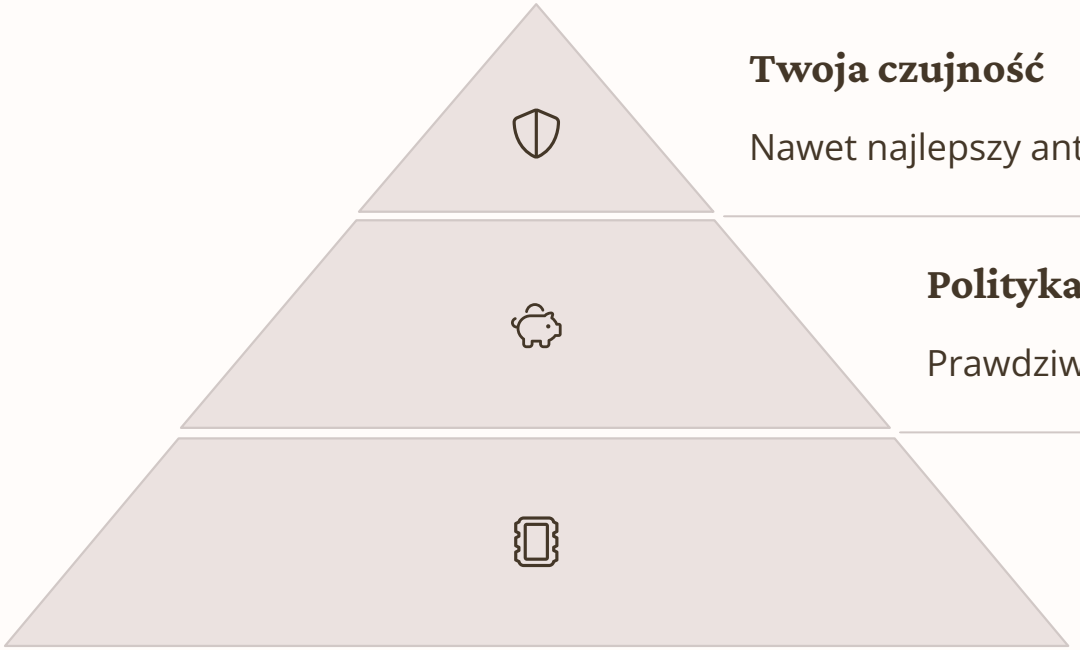
Zmiana haseł

Użyj zaufanego urządzenia, aby zmienić wszystkie hasła – do banków, portali, poczty.

Zachowanie dowodów

Nie kasuj e-maili, historii przeglądarki czy zrzutów ekranu.

Pamiętaj dodatkowo:



Twoja czujność

Nawet najlepszy antywirus nie zastąpi ostrożności użytkownika.

Polityka instytucji

Prawdziwe banki nie proszą o dane przez e-mail.

Różne urządzenia

Ataki mogą dotyczyć komputerów, telefonów, tabletów.

Celem phishingu jest stworzenie iluzji rutynowej czynności, byś nie zauważył zagrożenia. Zachowaj czujność wobec wszystkich nietypowych sytuacji.