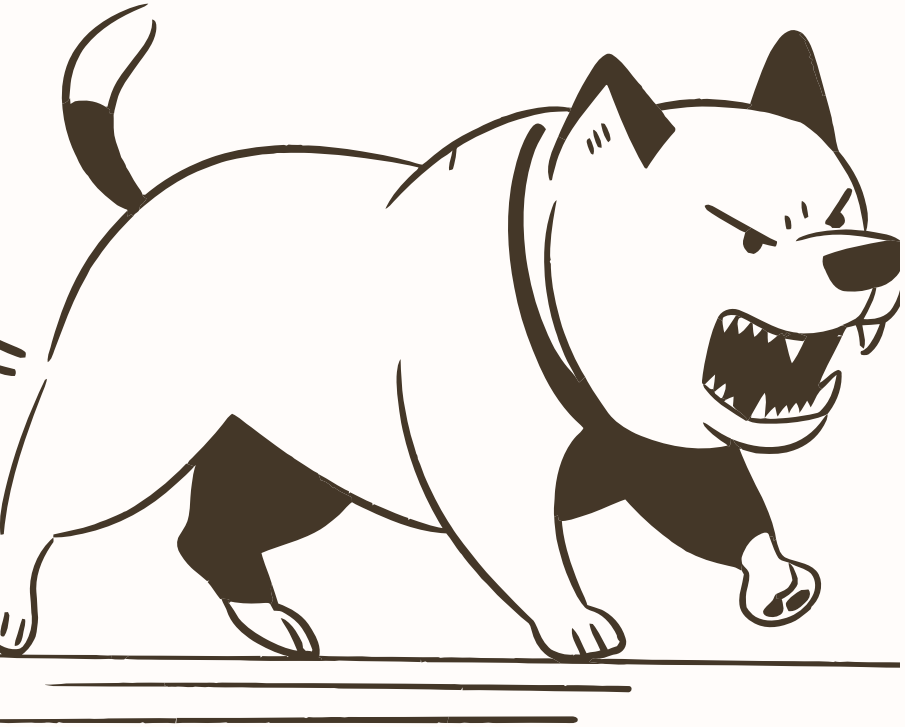


Scenariusze ataków phishingowych

Phishing to jedna z najpopularniejszych metod cyberataków, wykorzystująca socjotechnikę do wyłudzania poufnych informacji. Przestępcy podszywają się pod zaufane osoby lub instytucje, aby nakłonić ofiary do określonych działań. Prezentacja omawia trzy popularne scenariusze ataków: wakacyjny phishing, phishing na prezesa oraz phishing przez komunikatory.

Wakacyjny phishing - oszustwa w sezonie urlopowym

Podszywanie się

Atakujący udają współpracownika, klienta lub przełożonego, wiedząc, że wiele osób jest na urlopie.

Wykorzystanie nieobecności

Wykorzystują brak osoby decyzyjnej do wymuszenia działania (np. przelewu).

Podszywanie się pod działy

Często podszywają się pod osoby z działu księgowości, HR lub kadr.

Przykład: „Szef jest na urlopie, więc pilnie prosimy o uregulowanie zaległej faktury" – mail trafia do zastępcy, który nie zna wszystkich procedur.

Na co uważać przy wakacyjnym phishingu

Pilne prośby o przelew

Zwracaj uwagę na nagłe, pilne prośby o przelew w nietypowej sytuacji, szczególnie gdy pojawiają się w okresie urlopowym.

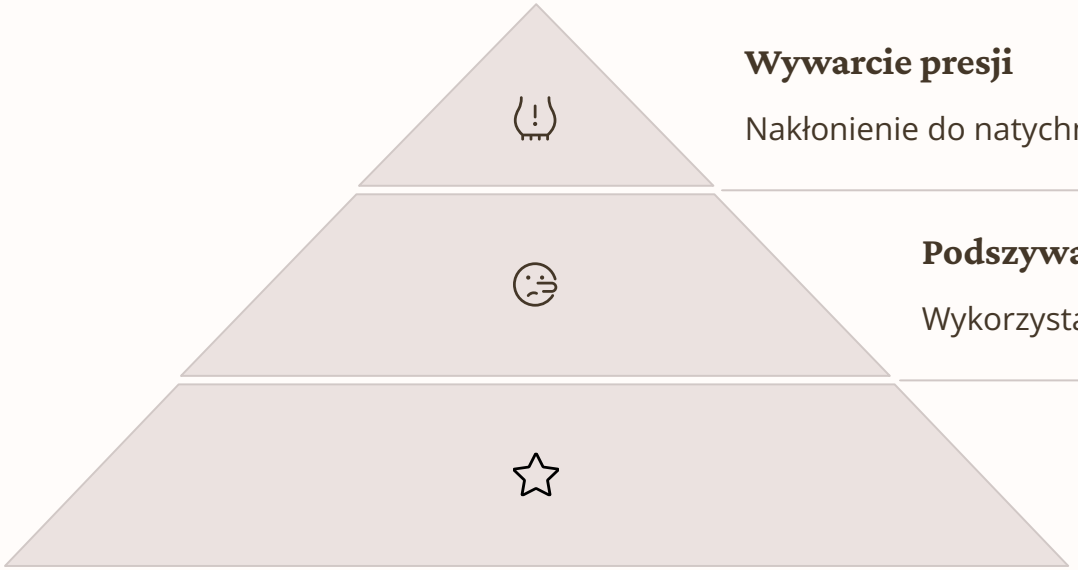
Zmiany w danych odbiorcy

Bądź czujny na wszelkie zmiany w danych odbiorcy, takie jak nowy numer konta bankowego czy inne dane kontaktowe.

Brak osoby zatwierdzającej

Zachowaj szczególną ostrożność, gdy osoba zwykle zatwierdzająca płatności jest nieobecna lub niedostępna.

Phishing na prezesa (CEO fraud)



Wywarcie presji

Nakłonienie do natychmiastowego działania

Podszywanie się

Wykorzystanie podobnych domen lub prywatnych adresów

Autorytet

Wykorzystanie pozycji osoby na wysokim stanowisku

Przykład: „Potrzebuję, byś niezwłocznie wykonał przelew na poufny projekt. Nie zadawaj pytań – sprawa strategiczna. Zrób to jeszcze dziś." – wiadomość podpisana „Prezes Marek Z.", wysłana z adresu łudząco podobnego do firmowego.

Na co uważać przy phishingu na prezesa

Presja czasu

Polecenia typu „zrób to natychmiast" lub „bez informowania nikogo" powinny wzbudzić Twoją czujność. Przestępcy często wykorzystują pośpiech, aby ofiara nie miała czasu na weryfikację.

Błędy językowe

Zwracaj uwagę na błędy językowe lub nienaturalne sformułowania w wiadomościach. Często są one wynikiem automatycznego tłumaczenia lub pisania przez osobę, dla której polski nie jest językiem ojczystym.

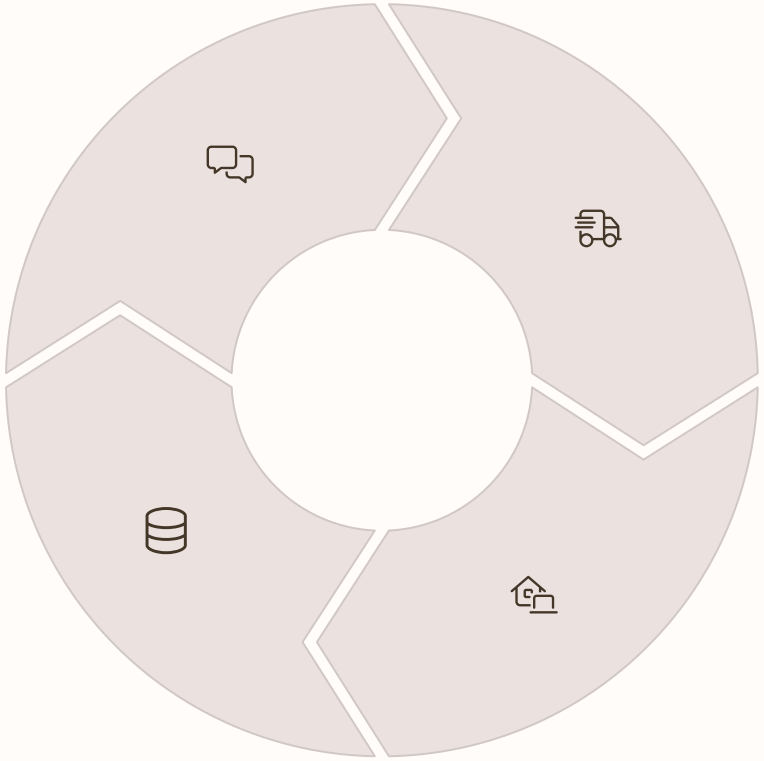
Nietypowe prośby

Bądź szczególnie ostrożny wobec próśb niezgodnych z polityką firmy lub wykraczających poza standardowe procedury, nawet jeśli wydają się pochodzić od przełożonego.

Phishing przez komunikatory

Wysłanie wiadomości

Atakujący wysyła wiadomość przez popularny komunikator, podszywając się pod współpracownika



Pilna prośba

Celem jest szybka reakcja odbiorcy – np. podanie kodu autoryzacyjnego

Kradzież danych

Finalnym celem jest uzyskanie dostępu do systemów lub wyłudzenie pieniędzy

Wykorzystanie pracy zdalnej

Popularny wektor ataku przy pracy zdalnej i w dynamicznych zespołach

Przykład: „Cześć, zapomniałem hasła do systemu. Możesz mi przesłać SMS z kodem logowania, który zaraz przyjdzie na Twój numer? Dzięki!"

Cechy wspólne wszystkich ataków phishingowych

Presja czasu

Atakujący zawsze podkreślają pilność sprawy używając słów: „pilne", „dzisiaj", „teraz". Ma to na celu wywołanie stresu i skłonienie do szybkiego, nieprzemyślanego działania.

Przestępcy wiedzą, że pod presją czasu ludzie częściej popełniają błędy i rzadziej weryfikują informacje.

Brak możliwości potwierdzenia

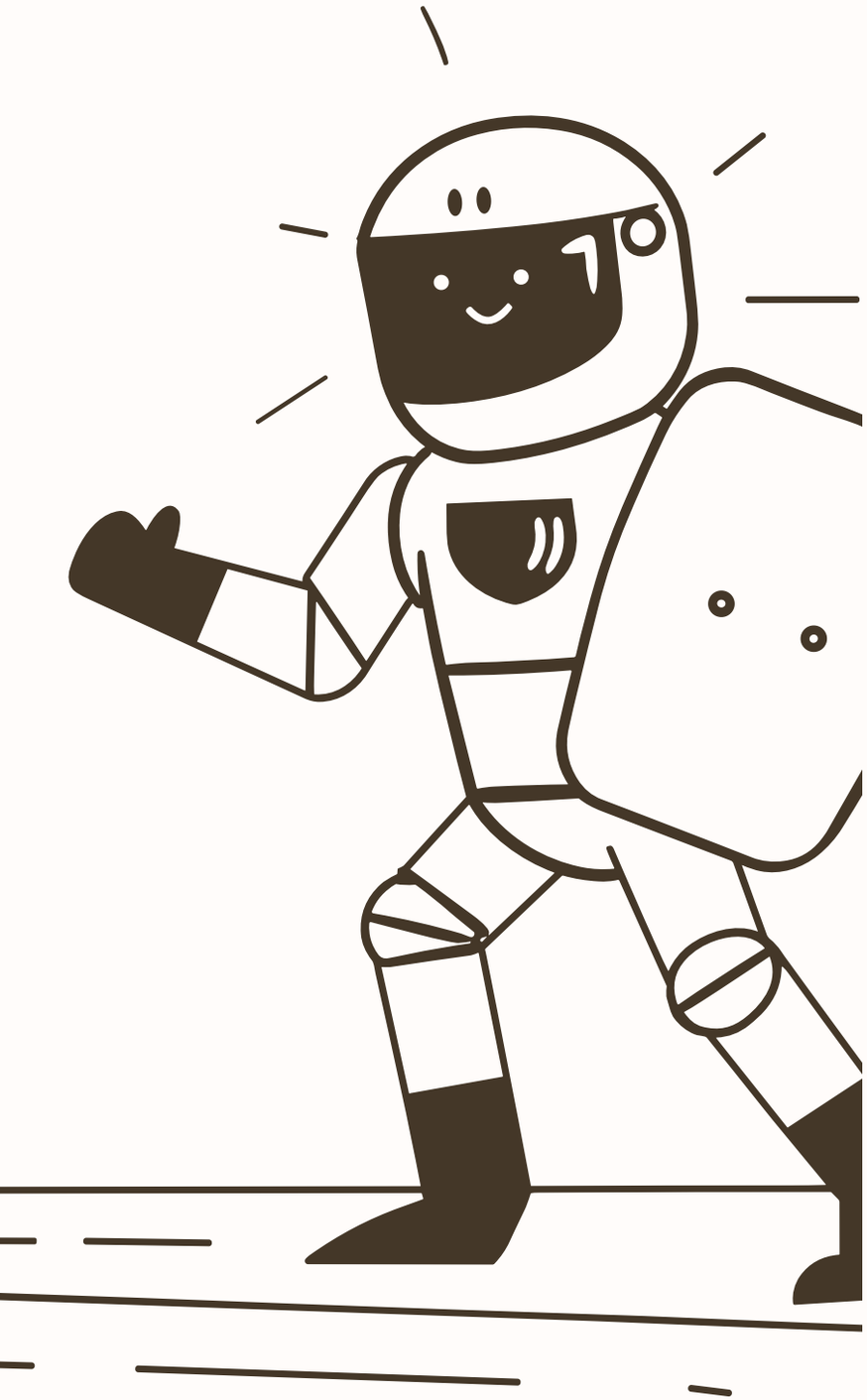
Typowe wymówki to: „nie dzwoń, jestem na spotkaniu", „pisz tylko tutaj". Atakujący za wszelką cenę chcą uniknąć weryfikacji przez inny kanał komunikacji.

Jeśli ktoś utrudnia Ci potwierdzenie informacji inną drogą, powinna zapalić się czerwona lampka ostrzegawcza.

Wzbudzanie zaufania

Przestępcy podpisują się imieniem i nazwiskiem, wykazują znajomość struktury firmy i relacji między pracownikami, aby wzbudzić zaufanie.

Często wykorzystują informacje dostępne publicznie, np. z mediów społecznościowych, aby ich wiadomości brzmiały wiarygodnie.



Jak się chronić przed atakami phishingowymi

Weryfikuj nadawcę

Zawsze weryfikuj nadawcę przez telefon lub innym kanałem niż otrzymana wiadomość. Szczególnie w przypadku próśb o przelew lub udostępnienie danych.

Nie podejmuj pochopnych decyzji

Nie podejmuj decyzji finansowych na podstawie wiadomości „na szybko". Sprawdzaj dokładnie adres e-mail i numer telefonu – nawet drobne różnice mogą oznaczać fałszerstwo.

Chroń dane dostępowe

Nie podawaj żadnych danych dostępowych (loginów, kodów SMS) przez komunikatory. Wprowadź zasadę podwójnego potwierdzenia przelewów i zmian danych kontrahentów.

Szkol zespół

Pamiętaj, że to nie technologia jest najsłabszym ogniwem, lecz człowiek. Cyberprzestępcy bazują na emocjach: stresie, pośpiechu, lojalności wobec przełożonego.