



# Phishing



## jak się przed nim bronić?



### Czym dokładnie jest phishing?

Jest to bardzo popularna i prosta metoda ataku hakerskiego, w której cyberprzestępcy podszywają się pod inne osoby lub firmy w celu wyłudzenia poufnych informacji, zainfekowania sprzętu bądź nakłonienia do wykonania określonych działań.

## Na co zwrócić uwagę weryfikując podejrzaną wiadomość?



Ostrożnie traktuj załączniki, które otrzymujesz. Jeśli nie masz co do nich pewności – lepiej ich nie otwieraj.



Nie rozpoznajesz nadawcy wiadomości? Rozważ jej usunięcie. Jeśli zdecydujesz się ją przeczytać, uważaj, aby nie klikać linków i nie pobierać plików. Masz kontakt z nadawcą? Zadzwoń do niego i zweryfikuj czy wysłał do Ciebie wiadomość.



W przypadku linków przesłanych w wiadomości bardzo dokładnie sprawdzaj domeny, na które zostaniesz przekierowany po ich kliknięciu. Najedź na link kursorem, aby wyświetlić adres, do którego zostaniesz przekierowany.



Sprawdź czy przesłana wiadomość nie zawiera błędów językowych. Często atakujący nie przywiązują wagi do jakości.



Jeśli nie masz pewności czy otrzymana wiadomość jest prawdziwa – nie wykonuj żadnej akcji. Prześlij ją do działu IT, celem weryfikacji.

### Podstawa: edukacja pracowników

**Regularne przeprowadzaj zaplanowane kampanie phishingowe i szkolenia awarenessowe dla Twoich pracowników.**



**Potrzebujesz wsparcia w tym zakresie?**  
Napisz od nas: [kontakt@resilia.pl](mailto:kontakt@resilia.pl)