European Cyber Security Month

Ochroń firmę przed oszustwami

5 wskazówek dla pracowników

Zachowaj spokój, gdy otrzymasz „pilną” prośbę o płatność od osoby wyższego szczebla w Twojej firmie

1

Oszuści mogą udawać kierownika wyższego szczebla albo dyrektora firmy, aby spróbować przekonać pracownika do dokonania płatności w sposób poufny.
Sprawdź, czy adres e-mail jest poprawny, i zadzwoń, żeby zweryfikować pozostałe informacje - nie używaj do tego numeru telefonu, który pojawia się w podejrzanej wiadomości e-mail.

Zawsze sprawdzaj prośbę dostawcy o zmianę szczegółów płatności

2

Jeśli ktoś do Ciebie zadzwoni lub wyśle e-mail z informacją, że dostawca zmienił sposób płatności, może to być oszustwo.
Skontaktuj się z dostawcą osobiście, aby potwierdzić te informacje.

Uważaj na fałszywe „alerty bezpieczeństwa”

3

Fałszywe alerty są często wykorzystywane przez oszustów, by przekonać pracowników, że doszło do naruszenia bezpieczeństwa systemu firmy lub systemu bankowości internetowej.
Następnie oszuści żądają podania szczegółowych informacji finansowych w celu przywrócenia bezpieczeństwa.
Upewnij się, że alert jest prawdziwy. Zadzwoń do danej osoby, korzystając z numeru z książki adresowej Twojej firmy.

Zastanów się, zanim klikniesz

4

Metody, których używają oszuści, aby przekonać pracowników do pobrania szkodliwych plików są niezliczone.
Jeśli masz jakieś wątpliwości dotyczące wiadomości e-mail, nie otwieraj załącznika, nie klikaj na link, ani nie pobieraj plików.
Poproś swój dział IT, aby sprawdził e-mail i jego zawartość.

I pomyśl, zanim udostępnisz

5

Nie udostępniaj żadnych poufnych informacji o swojej firmie w mediach społecznościowych, może to zwiększyć ryzyko, że staniesz się celem ataku.
Zapoznaj się z polityką swojej firmy dotyczącą mediów społecznościowych i dowiedz się, co możesz udostępniać, a jeśli masz wątpliwości, nie publikuj.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#ThinkB4UClick