Szkoła Sieci Społecznościowych

Rozpoznaj oszustwo

Prywatność i bezpieczeństwo

Zachowania potencjalnie krzywdzące i szkodliwe

Rozpoznaj oszustwo

Prywatność i Bezpieczeństwo

Zachowania potencjalnie krzywdzące i szkodliwe

Czas trwania: 25 minut **Materiały:** Slajdy, Załącznik 1 (do wydrukowania)

Instrukcje:

- Porozmawiaj z dzieckiem o tym, co wie o oszustwach internetowych - jak do nich dochodzi? Dlaczego ktoś próbuje oszukiwać innych w sieci?
- Wyjaśnij, że rozpoznanie internetowego oszustwa może być czasem trudne - nabiera się na nie wielu dorosłych! Czasem pojawiają się jednak wskazówki, dzięki którym można rozpoznać oszustwo i uniknąć go.
- Przeczytajcie z dzieckiem slajdy i omówcie wskazówki, które mogą zdradzić internetowe oszustwo. Zachęć dziecko do podzielenia się znanymi mu opowieściami o osobach, które dostały oszukańcze wiadomości lub e-maile. Możesz również opowiedzieć o własnych doświadczeniach związanych z dostawaniem oszukańczych wiadomości w sieci, o tym jak rozpoznałeś/-aś, że nie były prawdziwe i co zrobiłeś/-aś, by ochronić swoje dane osobowe lub uniknąć podobnych oszukańczych wiadomości w przyszłości.
- Spytaj dziecko, co poradziłoby komuś, kto chce unikać internetowych oszustw i zapewnić, że jego konta internetowe są zabezpieczone. Możesz przypomnieć mu, że najbezpieczniejszy sposób logowania się do konta internetowego wiąże się zawsze z wejściem na oficjalną stronę/korzystaniem z oficjalnej aplikacji, a nie kliknięciem w link w wiadomości lub e-mailu.
- Jeżeli masz czas, możesz opracować z dzieckiem jego własny przykład oszukańczej wiadomości/oszukańczego e-maila przy pomocy nowo poznanych wskazówek. W Załączniku 1 znajdziesz wzór, w który dziecko może wpisać własny fałszywy e-mail lub wiadomość.

Rozpoznaj oszustwo

Prywatność i bezpieczeństwo

Zachowania potencjalnie krzywdzące i szkodliwe

Kwestie do omówienia:

- Czym są internetowe oszustwa?
- W jaki sposób użytkownicy internetu padają ofiarą oszustw?
- Dlaczego ktoś może próbować oszukać Cię w sieci?
- Jak rozpoznać, że coś jest oszustwem/podstępem?
- Co poradził(a)byś komuś, kto chce chronić się przed internetowymi oszustwami?
- Co zrobić, jeśli podejrzewasz, że ktoś oszukał Cię w internecie?

Rozpoznaj oszustwo

Naucz się rozpoznawać internetowe oszustwa dzięki poniższym wskazówkom:

1. Wiadomość oczekiwana?
2. PILNE!
3. Ortografia i poprawność gramatyczna
4. Co zawiera wiadomość?
5. Dokąd prowadzi link?
6. Sprawdź adres
7. Strona zabezpieczona czy niezabezpieczona?

Szkoła Sieci Społecznościowych

1. Wiadomość oczekiwana?

Zawsze podejrzliwie podchodź do e-maili i wiadomości, których nie oczekiwałeś/-aś, zwłaszcza jeżeli zawierają prośbę o zresetowanie hasła.

Może być to podstęp mający na celu ujawnienie przez Ciebie hasła lub znak, że ktoś próbował wejść na Twoje konto.

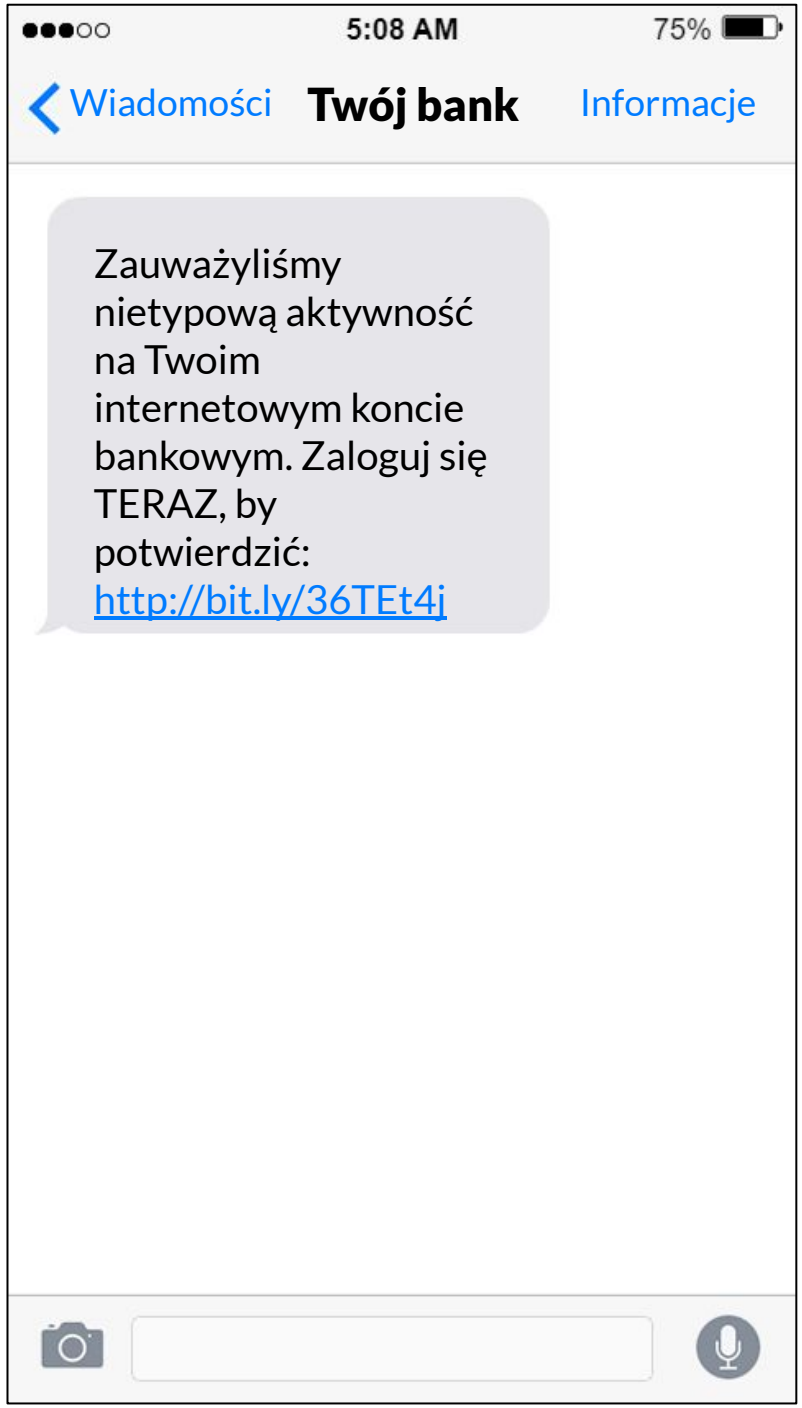
Pamiętaj: Jeżeli nie brałeś/-aś udziału w konkursie, niemożliwe jest, abyś wygrał/-a w nim nagrodę!

2. PILNE!

Oszukańcze wiadomości często zapraszają do podjęcia natychmiastowego działania lub grożą dezaktywacją lub zamknięciem konta.

Mogą również zawierać WIELKIE LITERY, by sytuacja wydawała się jeszcze pilniejsza.

Tekst wiadomości może być napisany w innym stylu niż prawdziwa wiadomość od firmy.

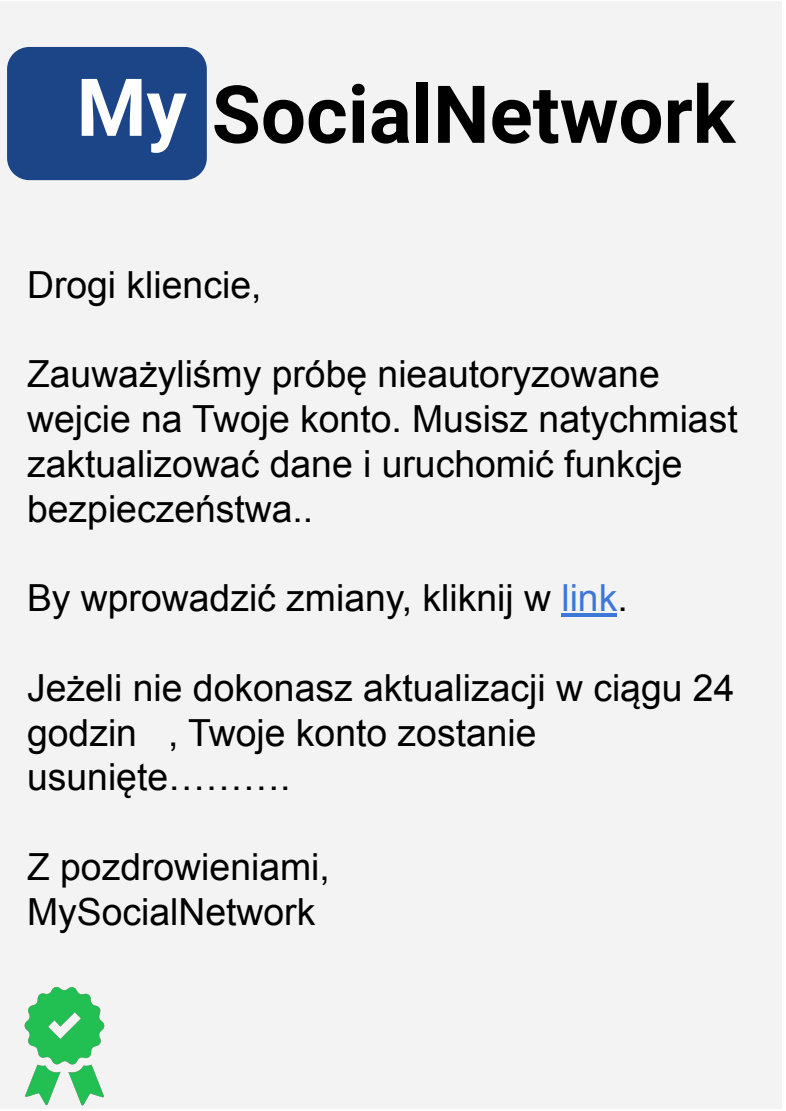


3. Ortografia i poprawność gramatyczna

Nawet jeśli wiadomość posiada wszystkie właściwe logo, błędy ortograficzne i gramatyczne mogą wskazywać, że jest fałszywa.

Wiadomości, które nie zawierają Twojego imienia ani nazwiska należy również traktować jako podejrzane.

Jeżeli masz wątpliwości, najbezpieczniejszym rozwiązaniem jest wejście na oficjalną stronę firmy/serwisu, zalogowanie się do konta i wprowadzenie zmian.



4. Co zawiera wiadomość?

Podejrzliwie podchodź do wszystkich nieoczekiwanych wiadomości zapraszających do otwarcia załączników. Pliki te mogą w rzeczywistości zawierać wirusy lub inne złośliwe oprogramowanie, które może uszkodzić Twoje urządzenie lub ukraść Twoje dane osobowe.

Jeżeli masz wątpliwości, lepiej nie otwierać ani nie pobierać załącznika na Twoje urządzenie.

faktura-klienta.docx

danekonta.pdf

WAŻNE - PRZECZYTAJ.zip

5. Dokąd prowadzi link?

Zawsze podejrzliwie podchodź do e-maili i wiadomości, w których jesteś proszony/-a o kliknięcie w link.

W e-mailu możesz sprawdzić, dokąd prowadzi link bez klikania w niego.
Na ekranie komputera umieść kursor myszki nad linkiem, by go wyświetlić. Na urządzeniu z ekranem dotykowym przytrzymaj link, by go wyświetlić.

By potwierdzić hasło

Kliknij w link TERAZ!

http://monreseaus0clal.com/confirmationmotdepasse

6. Sprawdź adres

Niektóre fałszywe strony internetowe posiadają adresy, które na pierwszy rzut oka wydają się autentyczne, ale używają innych znaków, by zamaskować fałszywy charakter strony.

Autorem e-maila może wydawać się prawdziwa osoba lub firma, podczas gdy w rzeczywistości jest nim oszust.

Potwierdź „Hasło do My Social Network TERAZ!

hasło@mysocialnetwork.com <mysn@mysn-genuine.ru>

do mnie

7. Strona zabezpieczona czy niezabezpieczona?

Strona niezabezpieczona

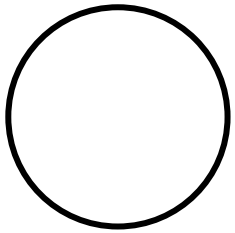
Strona zabezpieczona

Gdy wchodzisz na stronę, zawsze sprawdzaj adres strony u góry przeglądarki.

Logowanie i wpisywanie danych osobowych na niezabezpieczonej stronie nie jest bezpieczne (ale strona zabezpieczona nie gwarantuje autentyczności)

Załącznik 1: Rozpoznaj oszustwo

Odpowiedz | Odpowiedz wszystkim | Przekaż dalej



Data:

Od:

Temat:

Do:

Szkoła Sieci Społecznościowych