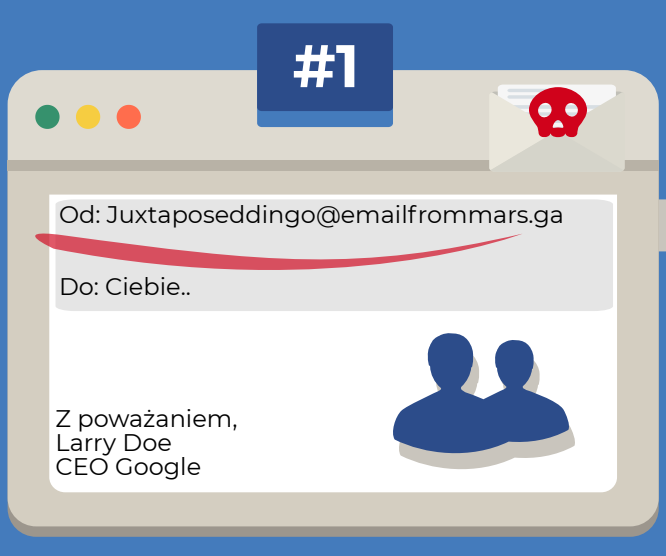
10 Kroków do ochrony przed Phishingiem

Przestrzegając kilku prostych zasad, skutecznie uchronisz się przed kradzieżą haseł, numerów kart kredytowych, danych kont bankowych, pieniędzy i innych poufnych informacji.

Co to jest Phishing?

To praktyka wysyłania wiadomości e-mail, które wydają się pochodzić z renomowanych źródeł w celu wywarcia wpływu lub pozyskania danych osobowych.

#1



Nie ufaj nadawcy wiadomości!

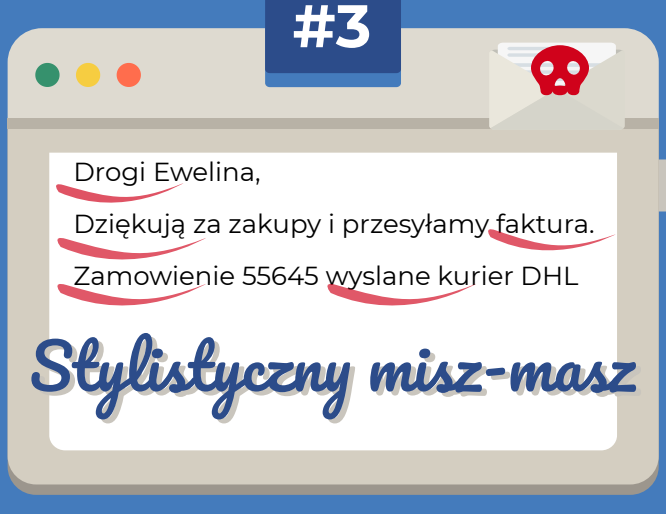
Nie zawsze osoba, której podpis znajdziesz w wiadomości mailowej, to ta za którą się podaje. Dokładnie sprawdź adres mailowy i zweryfikuj nadawcę wiadomości.

#2

Nie klikaj nieznanych linków!

Jeżeli wiadomość zawiera link, najedź na niego kursorem i sprawdź, gdzie faktycznie prowadzi. Nigdy nie klikaj linku, jeśli opis strony wzbudza podejrzenie.

#3



Dokładnie sprawdzaj pisownię!

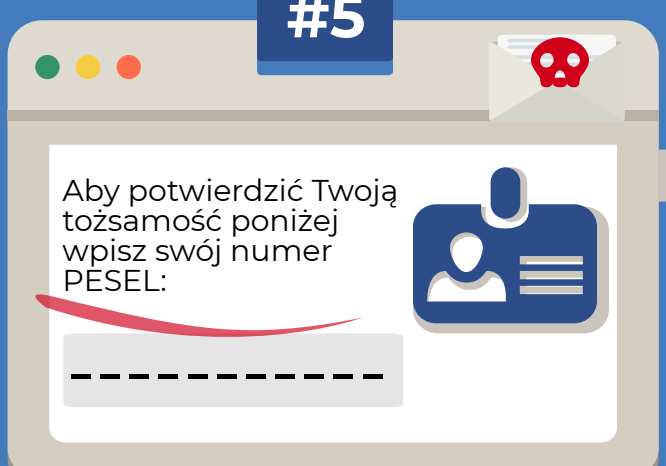
Jeśli wiadomość zawiera dużo błędów stylistycznych, literówek oraz błędów ortograficznych, powinna wzbudzić Twoją czujność.

#4

Zwróć uwagę na zwrot grzecznościowy!

Forma grzecznościowa "Drogi kliencie" lub "Drogi <automatycznie wypełnione imię>" może wskazywać na phishing. Ktoś kto będzie się chciał z Tobą skontaktować uczciwie, użyje poprawnych form imiennych.

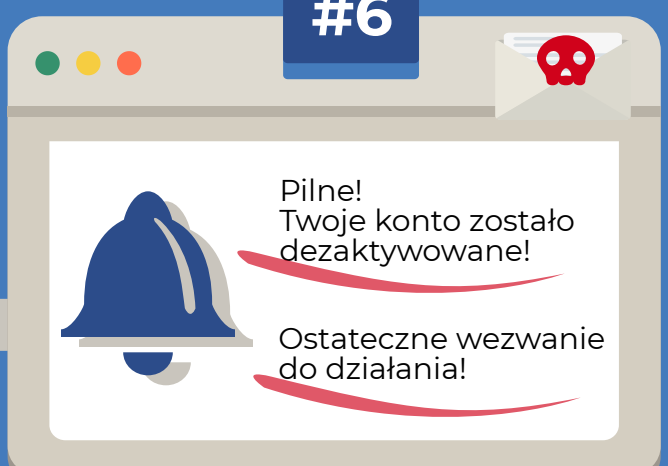
#5



Czy wiadomość zawiera prośbę o podanie danych osobowych?

Wiarygodni nadawcy nigdy nie proszą o podanie prywatnych danych w niezaszyfrowanej wiadomości mailowej.

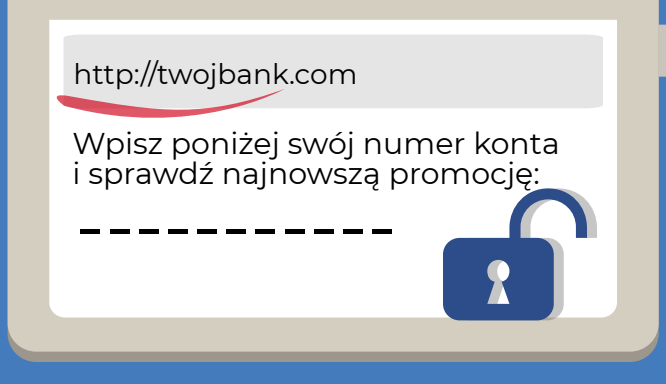
#6



Nie działaj pochopnie!

Nigdy dobrowolnie nie odpowiadaj na wiadomości, które próbują na Tobie wywrzeć presję działania! Większość wiadomości phishingowych zachęca np. do ponownego wpisania hasła.

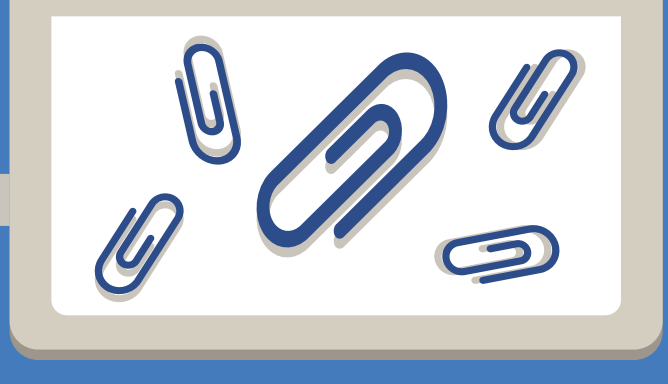
#7



Zwróć uwagę bezpieczeństwo strony!

Bądź pewny, że każda odwiedzana strona ma ważny certyfikat SSL lub przed adresem strony pojawia się symbol zamkniętej kłódki.

#8



Uważaj na załączniki!

Cyberprzestępcy uwielbiają wykorzystywanie załączników do przesyłania szkodliwych plików. Nie otwieraj nieznanych plików.

#9

Bądź podejrzliwy!

Jeśli jakiś element wiadomości wygląda podejrzanie to ją zignoruj. Zgłaszaj wszelkie nieprawidłowości.

#10

Aktualizuj wiedzę o zagrożeniach!

Twój dział IT powinien na bieżąco informować Cię o najnowszych zagrożeniach. Zgłaszaj wszystkie naruszenia bezpieczeństwa.

Zapamiętaj!

Jeśli jesteś pewien, że Twój system operacyjny jest regularnie aktualizowany przy pomocy łatek i uaktualnień pobranych ze strony producenta oraz zabezpieczony programem antywirusowym, zastosuj dodatkowo dobre praktyki i ustrzeż się przed podstępnym cyberatakiem.

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

www.forsafe.pl