Phishing - wszystko co powinieneś wiedzieć o wyłudzaniu danych

Najprostsza definicja phishingu mówi, że jest to **metoda oszustwa**, w której przestępcy, podszywając się pod osoby lub zaufane instytucje **wyłudzają dane** (do logowania do serwisów bankowości elektronicznej, wewnętrznych sieci firmowych, ale także numery kart płatniczych i adresy e-mail), **infekują komputery złośliwym oprogramowaniem** lub **próbują nakłonić ofiary do wykonania konkretnych działań.**

Jak rozpoznać wiadomość phishingową?

Przejrzenie działań oszustów nie zawsze jest łatwe, ale jeśli nie damy ponieść się emocjom i **do każdej, a zwłaszcza podejrzanej wiadomości podejdziemy spokojnie oraz jeśli sprawdzimy kilka jej elementów, to mamy sporą szansę, żeby nie paść ofiarą phishingu**.

PZPN

1) Zwróć uwagę na adresata wiadomości:

Od: ING Bank <suppinf@ingbank.pl>
Data: 21 listopada 2011 10:01:47 CET
Do:
Temat: UWAGA : Masz 1 nowa wiadomosc!

ING
DAJEMY CI SIŁĘ LWA

UWAGA : Masz 1 nowa wiadomosc!

Zaloguj : ING BankOnLine

Dziekujemy za korzystanie z ING Bank !

ING BANK SLASKI

Email ID: 469810

Nadchodzące zmiany w PayPal

Do: PayPal Services, — Brak Twojego adresu, jest ukryty
Odpowiedź do: Services@PayPal.cc — Błędna domena za znakiem "@"
pt., 27 mar, 19:42 (5 dni temu)

PayPal — Niskiej jakości obrazki

OSTRZEŻENIE — Agresywne słownictwo

Witaj, — Bezosobowy zwrot, brak imienia

W zwiazku z wprowadzeniem nowej polityki bezpieczeństwa PayPal, niektóre dane na Twoim koncie PayPal wymagają potwierdzenia.

W celu dalszego użytkowania swojego konta PayPal oraz wszystkich powiązanych benefitów, prosimy o potwierdzenie danych w przeciągu 24 godzin.

Jeśli dane nie zostaną w tym czasie potwierdzone - konto zostanie zawieszone, a środki na Twoim koncie staną się tymczasowo niedostępne. — Ponaglanie, pogróżki

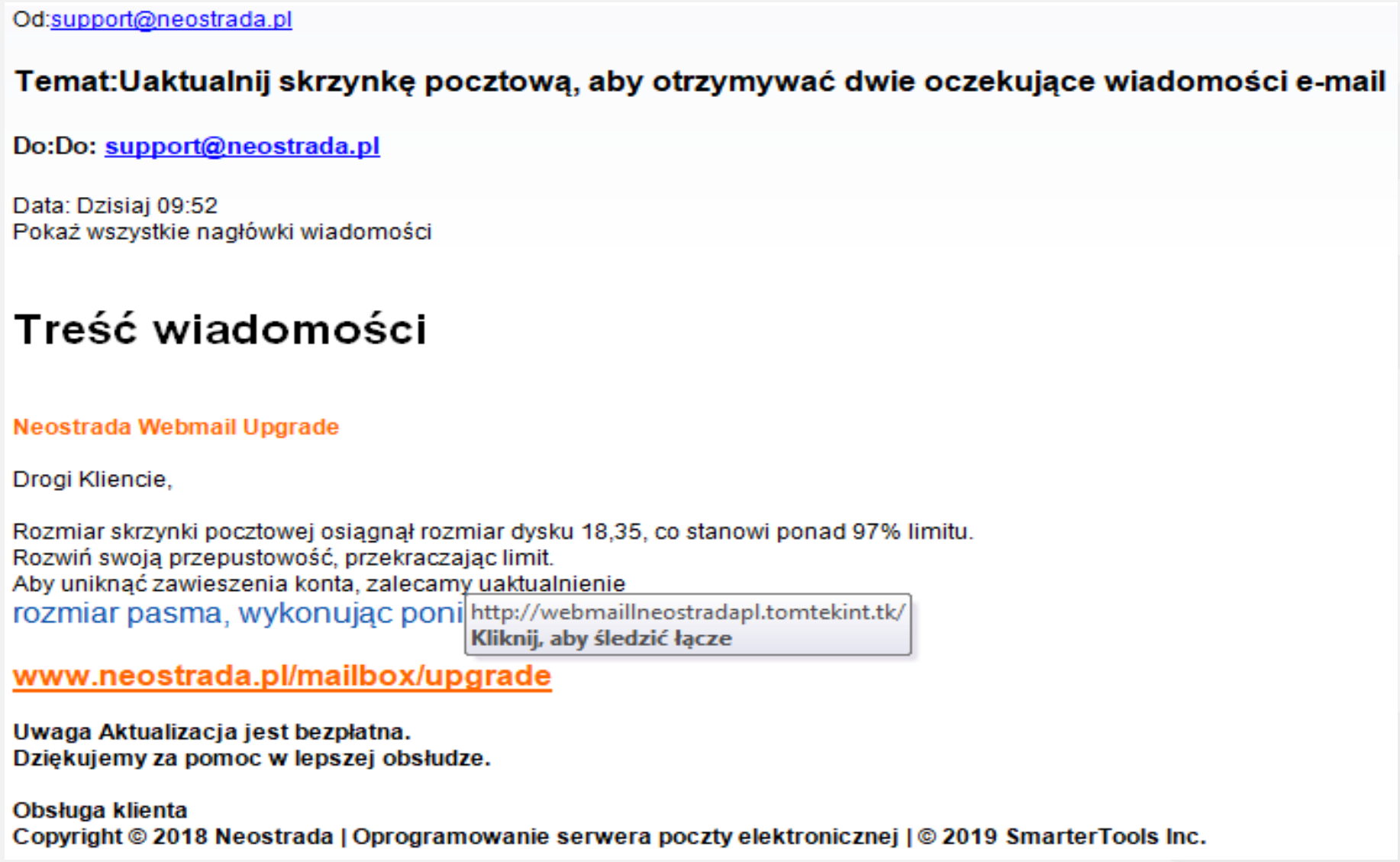
Poniżej link do Twojego konta PayPal

Potwierdź poprawność danych. — Najedź myszką na link i zobacz gdzie prowadzi

Dziękujemy za korzystanie z naszych usług.

Z poważaniem
PayPal

2) Sprawdź adres strony, do której prowadzi link



Od:support@neostrada.pl

Temat:Uaktualnij skrzynkę pocztową, aby otrzymywać dwie oczekujące wiadomości e-mail

Do:Do: support@neostrada.pl

Data: Dzisiaj 09:52
Pokaż wszystkie nagłówki wiadomości

Treść wiadomości

Neostrada Webmail Upgrade

Drogi Kliencie,

Rozmiar skrzynki pocztowej osiągnął rozmiar dysku 18,35, co stanowi ponad 97% limitu.
Rozwiń swoją przepustowość, przekraczając limit.
Aby uniknąć zawieszenia konta, zalecamy uaktualnienie
rozmiar pasma, wykonując poni

http://webmaillneostradapl.tomtekint.tk/
Kliknij, aby śledzić łącze

www.neostrada.pl/mailbox/upgrade

Uwaga Aktualizacja jest bezpłatna.
Dziękujemy za pomoc w lepszej obsłudze.

Obsługa klienta
Copyright © 2018 Neostrada | Oprogramowanie serwera poczty elektronicznej | © 2019 SmarterTools Inc.

3) Nie daj ponieść się emocjom

SMS →

Twoj numer zostanie wkrotce zablokowany z powodu braku splaty zadluzenia. Prosimy o szybka wplate 2,53 zl https://wezwanienr911.83619.eu/91XF7EamS42/hKolKnv

4) Prośba o dezaktywację haseł jest oszustwem

-----Original Message-----
From: Administrator systemu <postmaster@cupid.or.jp>
Sent: Wednesday, February 20, 2019 7:16 AM
To: Recipients <postmaster@cupid.or.jp>
Subject: Twoja skrzynka**
Sensitivity: Personal

Twoja skrzynka pocztowa przekroczyla limit przestrzeni dyskowej ustalony przez administratora, mozesz nie byc w stanie wysylac ani odbierac nowej poczty, dopóki nie zweryfikujesz ponownie skrzynki pocztowej. Aby ponownie zweryfikowac swoja skrzynke pocztowa, wyslij nastepujace informacje ponizej:

Nazwa:
Nazwa Uzytkownika:
Haslo:
Wpisz ponownie haslo:
Adres e-mail:
Numer telefonu:

Jesli nie uda sie ponownie zweryfikowac skrzynki pocztowej, twoja skrzynka zostanie dezaktywowana !!!

Dzieki
Administrator systemu

PZPN

5) Polski język, trudna język.....

Santander

Od: powiadomienia-santander@wp.pl

Ważna informacja: Informujemy o ważnych zmianach z dnia 14.09.2019 z powodu wprowadzenia dodatkowych zabezpieczeń PSD2 prosimy o zaaktualizowanie swojej karty na stronie banku w przeciwnym razie karta zostanie zablokowana co uniemożliwia dalsze korzystanie i wypłacanie środków z konta.

Należy zaaktualizować swoją kartę pod adresem strony banku
https://www.centrum24.pl/centrum24-web/login?/aktualizacje

PZPN

6) Uważajcie na załączniki

Od: Bank Zachodni WBK <contact@indywidualni.bzwbk.pl>
Temat: **[!! SPAM] Dezaktywacja konta**
Data: 6 kwietnia 2011 19:30:18 GMT+02:00
Do: Bank Zachodni WBK <contact@indywidualni.bzwbk.pl>
1 załącznik, 3,0 KB Zachowaj Szybki przegląd

konto.htm (3,0 KB)

Zdezaktywowales(as) swoje konto na Visa/MasterCard.

Wylaczyles(as) swoje konto na Visa/MasterCard. W kazdym momencie mozesz przywrocic swoje konto, uzywajac swojego Visa/MasterCard.

Bedziesz mogl korzystac ze strony jak dawniej.

Pobierz "Bank Zachodni WBK Visa-MasterCard"

Dziekujemy
Zespol Bank Zachodni WBK

PZPN

Jak chronić się przed phishingiem?

Niestety nie ma narzędzia, które gwarantowałoby wysoki stopień ochrony przed takimi oszustwami. Żeby się przed nimi ustrzec, trzeba korzystać z kilku elementów:

1) zdrowy rozsądek i ograniczone zaufanie do każdej wiadomości.

2) korzystanie z programów antywirusowych i choć nie będą one w stanie wskazać, że przeglądany e-mail to phishing, to **mogą zablokować niektóre niebezpieczne witryny oraz załączniki**.

VISHING (czyli phishing telefoniczny)

Wyłudzanie danych, ale w wersji głosowej, a dokładnie rzecz biorąc w trakcie rozmowy telefonicznej. Zręczni rozmówcy podający się za bankowców, doradców inwestycyjnych czy instytucje zaufania publicznego, są w stanie tak zmanipulować rozmówcę, że ten ujawni swoje szczegółowe dane. Chwilę później giną środki z jego konta bankowego.

Jak chronić się przed vishingiem?

Niestety nie ma narzędzia, które gwarantowałoby wysoki stopień ochrony przed takimi oszustwami. Żeby się przed nimi ustrzec, trzeba korzystać z kilku elementów:

1) pamiętajmy, że numer dzwoniącego **można podrobić,**
2) należy uważać jeśli ktoś w rozmowie telefonicznej **podaje się** za policjanta, szefa,
3) należy wzmóc czujność, jeśli ktoś **informuje nas o ataku** hackerskim/utracie pieniędzy,
4) **nie należy wchodzić na linki** podane przez konsultanta w trakcie rozmowy telefonicznej.