ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# PHISHING – CO TO JEST I JAK SIĘ PRZED NIM BRONIĆ

**MATERIAŁ SZKOLENIOWY PRZYGOTOWANY PRZEZ CZŁONKÓW**
**KOMISJI DS. OCHRONY DANYCH OSOBOWYCH DZIAŁAJĄCEJ PRZY ŚZGiP (8/15)**

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – co to jest ?

To metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.
Jest to rodzaj ataku opartego na inżynierii społecznej

*(Wikipedia)*

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – co to jest ?

**Celem ataku phishingowego nie jest sprzęt czy oprogramowanie, ale sam człowiek**

Działaniami, do których ma skłaniać wiadomość phishingowa są często na przykład:

- podanie danych logowania do banku na spreparowanej stronie WWW
- podanie danych karty płatniczej / kredytowej
- wpisanie loginu i hasła logowania do skrzynki pocztowej czy innego serwisu internetowego po kliknięciu w link z wiadomości
- podanie danych osobowych (np. PESEL, nazwisko panieńskie matki, data urodzenia, miejsce urodzenia, numer dowodu) potrzebnych do uzyskania dostępu do niektórych kont lub np. zaciągnięcia kredytu
- pobranie pliku ze złośliwym oprogramowaniem (np. faktury, wezwania do zapłaty, pisma od kancelarii prawnej)
- instalacja złośliwego oprogramowania (np. ransomware, trojana, wirusa)

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – jakimi kanałami komunikacji możesz zostać zaatakowany

- E-mail
- SMS
- Messenger, WhatsApp
- platformy sprzedażowe (Vinted, OLX, Allegro, itp.)
- poprzez media społecznościowe (prywatne wiadomości)
- w czasie rozmowy telefonicznej (tzw. ***Vishing*** – głosowy phishing - metoda na wnuczka, urzędnika, policjanta czy pracownika banku lub innej instytucji finansowej).

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – czego nie powinieneś robić

- wchodzić na podejrzane, nieznane strony www (strony zawierające niebezpieczne treści)
- klikać w linki z nieznanego lub niezaufanego źródła
- pobierać aplikacje oraz załączniki e-mail, z nieznanych/ podejrzanych źródeł, których pochodzenie lub zawartość budzą wątpliwości (w szczególności pliki z rozszerzeniami: *.exe, *.com, *.pif, *.scr, *.bat, .vbs)
- bez konsultacji z pionem IT lub bezpieczeństwa Urzędu – testować podatności systemów informatycznych
- podłączać laptopów, telefonów komórkowych (klasycznych i smartfonów) oraz tabletów do:
  - ☞ nieznanych sieci bezprzewodowych i publicznie dostępnych (np. darmowy Hotspot)
  - ☞ stacji roboczych, za pomocą kabla USB, np. w celu naładowania urządzenia

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – czego nie powinieneś robić

- ujawniać danych osobowych (w szczególności PESEL czy nazwisko rodowe matki), numery kart bankowych, PIN'y, hasła czy loginy w trakcie rozmów telefonicznych lub w korespondencji (e-mail, sms, komunikatorami itp.)
- przekazywać pieniędzy wnuczkom, policjantom, pracownikom banku itp.  na rzekome leczenie, odszkodowanie, mandat lub aby uniknąć kary
- przekazywać kodu blik na prośbę przez komunikator

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – na co powinieneś zwrócić uwagę

- wyłączaj połączenia bezprzewodowe typu Wi-Fi, Bluetooth, IrDa w czasie bezczynności
- zawsze sprawdzaj poziom uprawnień jakiego żądają od Ciebie aplikacje – zwracaj uwagę na uprawnienia, które nie przystają do przeznaczenia aplikacji
- blokuj niechciane reklamy
- każdorazowo wylogowuj się z serwisów WWW
- zawsze weryfikuj dzwoniących do Ciebie, próbujących wymusić wypłatę odszkodowania, kaucji mandatu/grzywny, a podających się za członków rodziny, urzędników, pracowników dostawców energii elektrycznej  lub gazu, policjantów, służby ratunkowe czy pracowników banku
- powiadamiaj odpowiednie służby o możliwych wyłudzeniach

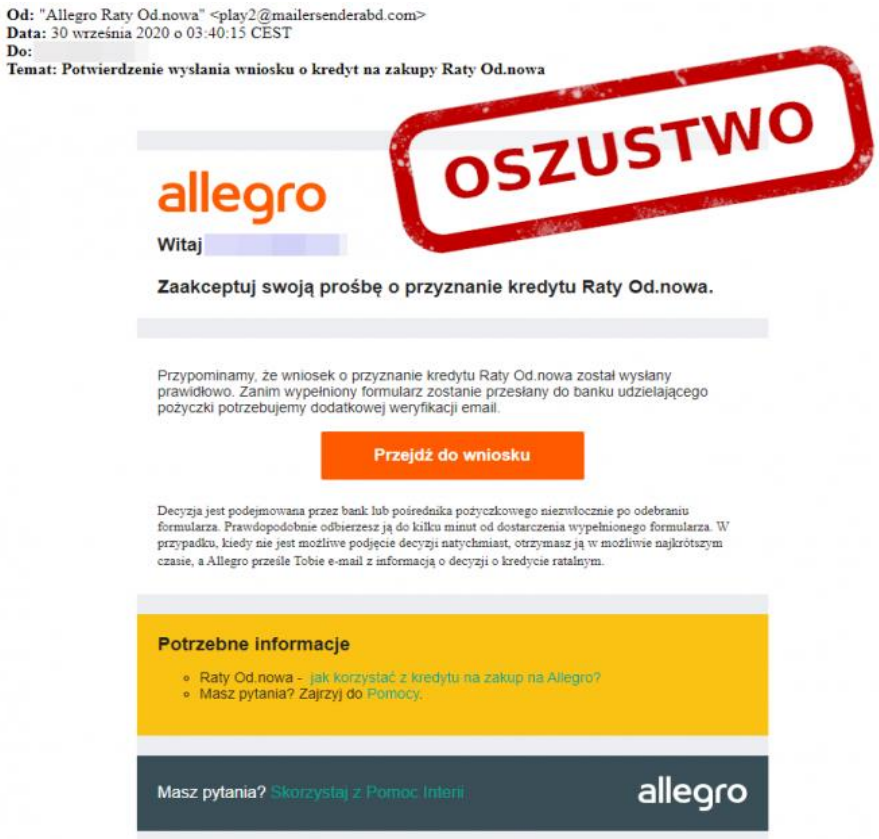
ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – na co powinieneś zwrócić uwagę

- nie ufaj wyświetlanej nazwie nadawcy
- sprawdź poprawność pisowni, gramatykę i stylistykę wiadomości
- sprawdź jak nadawca zwraca się do Ciebie
- uważaj, gdy w wiadomości jest presja czasu
- zweryfikuj podpis nadawcy
- uważaj na załączniki i linki, nie klikaj zanim nie zweryfikujesz nazwy

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – przykłady



**Od:** "Allegro Raty Od.nowa" <play2@mailersenderabd.com>
**Data:** 30 września 2020 o 03:40:15 CEST
**Do:**
**Temat: Potwierdzenie wysłania wniosku o kredyt na zakupy Raty Od.nowa**

OSZUSTWO

allegro

Witaj

**Zaakceptuj swoją prośbę o przyznanie kredytu Raty Od.nowa.**

Przypominamy, że wniosek o przyznanie kredytu Raty Od.nowa został wysłany prawidłowo. Zanim wypełniony formularz zostanie przesłany do banku udzielającego pożyczki potrzebujemy dodatkowej weryfikacji email.

Przejdź do wniosku

Decyzja jest podejmowana przez bank lub pośrednika pożyczkowego niezwłocznie po odebraniu formularza. Prawdopodobnie odbierzesz ją do kilku minut od dostarczenia wypełnionego formularza. W przypadku, kiedy nie jest możliwe podjęcie decyzji natychmiast, otrzymasz ją w możliwie najkrótszym czasie, a Allegro prześle Tobie e-mail z informacją o decyzji o kredycie ratalnym.

**Potrzebne informacje**

- Raty Od.nowa - jak korzystać z kredytu na zakup na Allegro?
- Masz pytania? Zajrzyj do Pomocy.

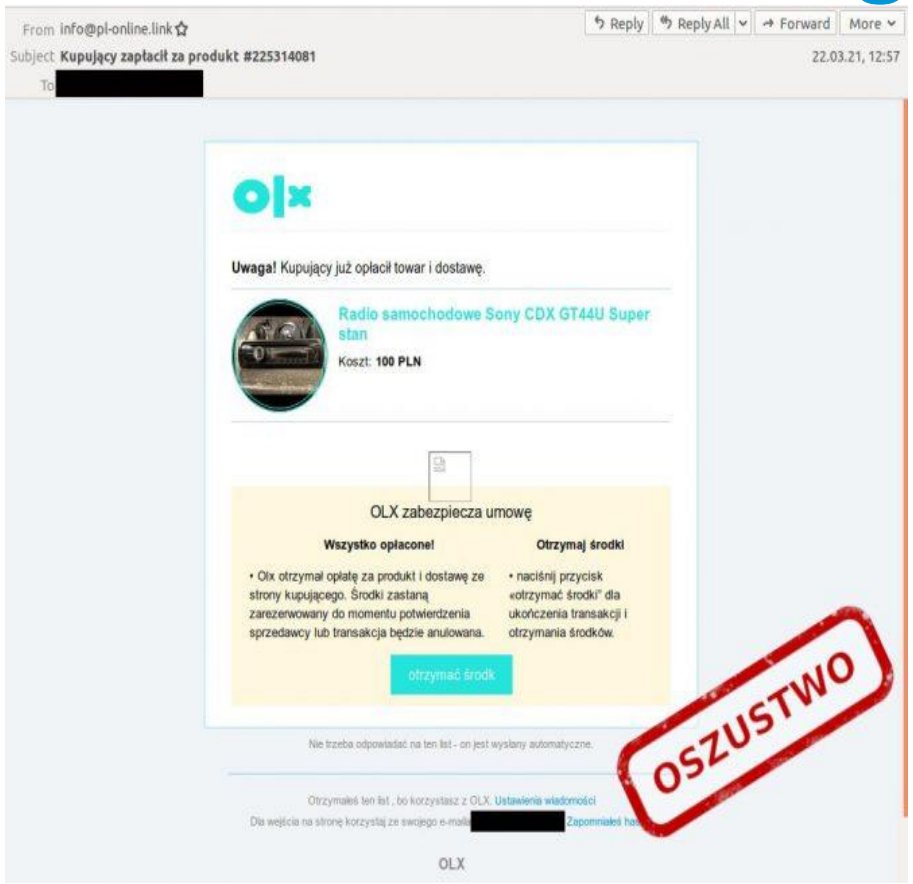
Masz pytania? Skorzystaj z Pomoc Interii

allegro

Źródło: https://kwestiabezpieczenstwa.pl

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

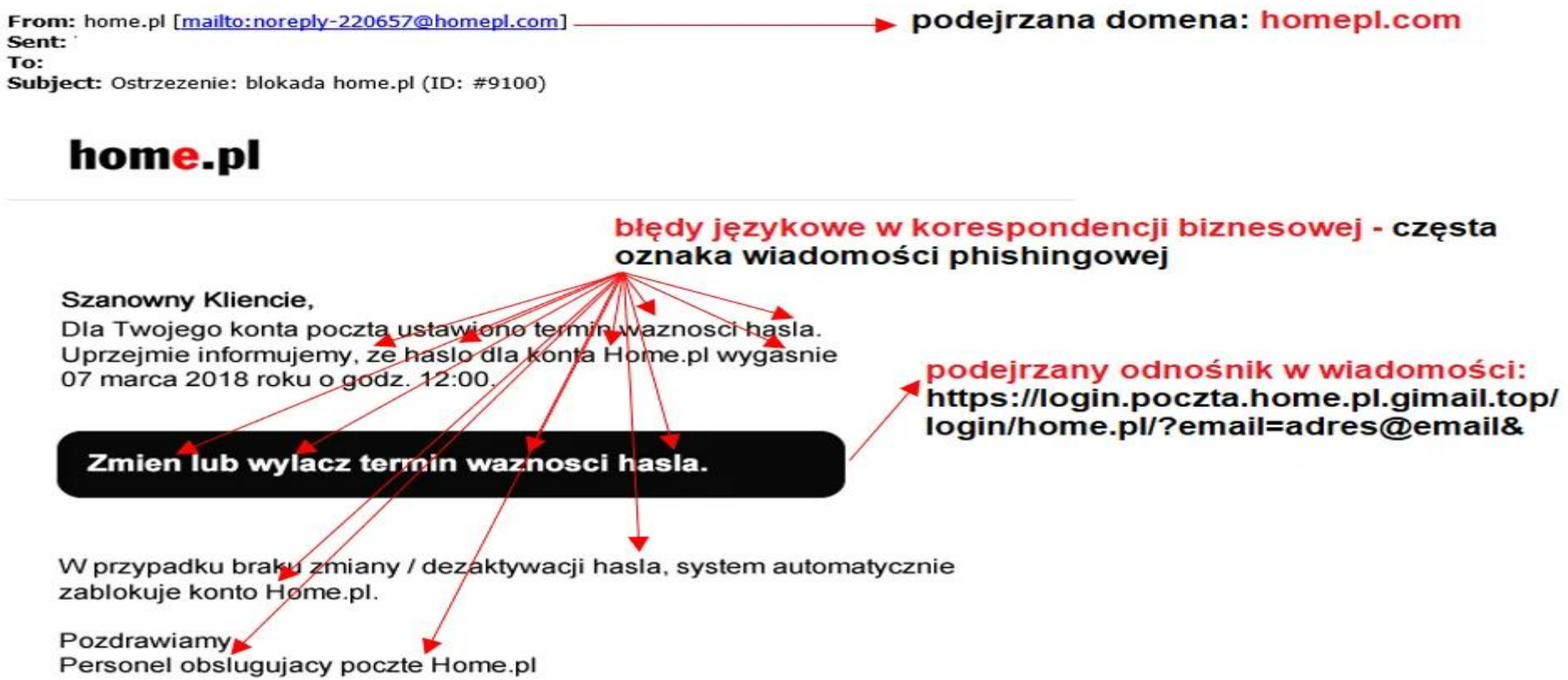
# Phishing – przykłady




Źródło: https://kwestiabezpieczenstwa.pl

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

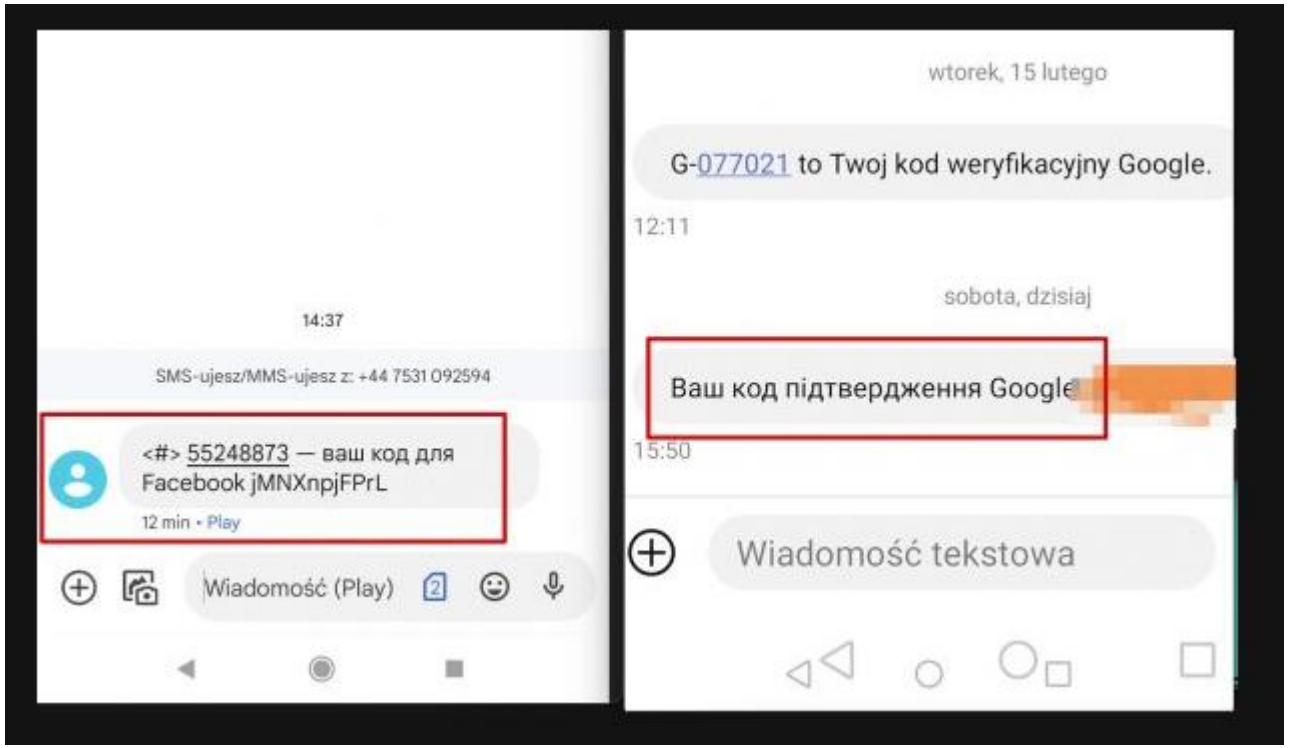
# Phishing – przykłady




Źródło: https://blog.home.pl

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

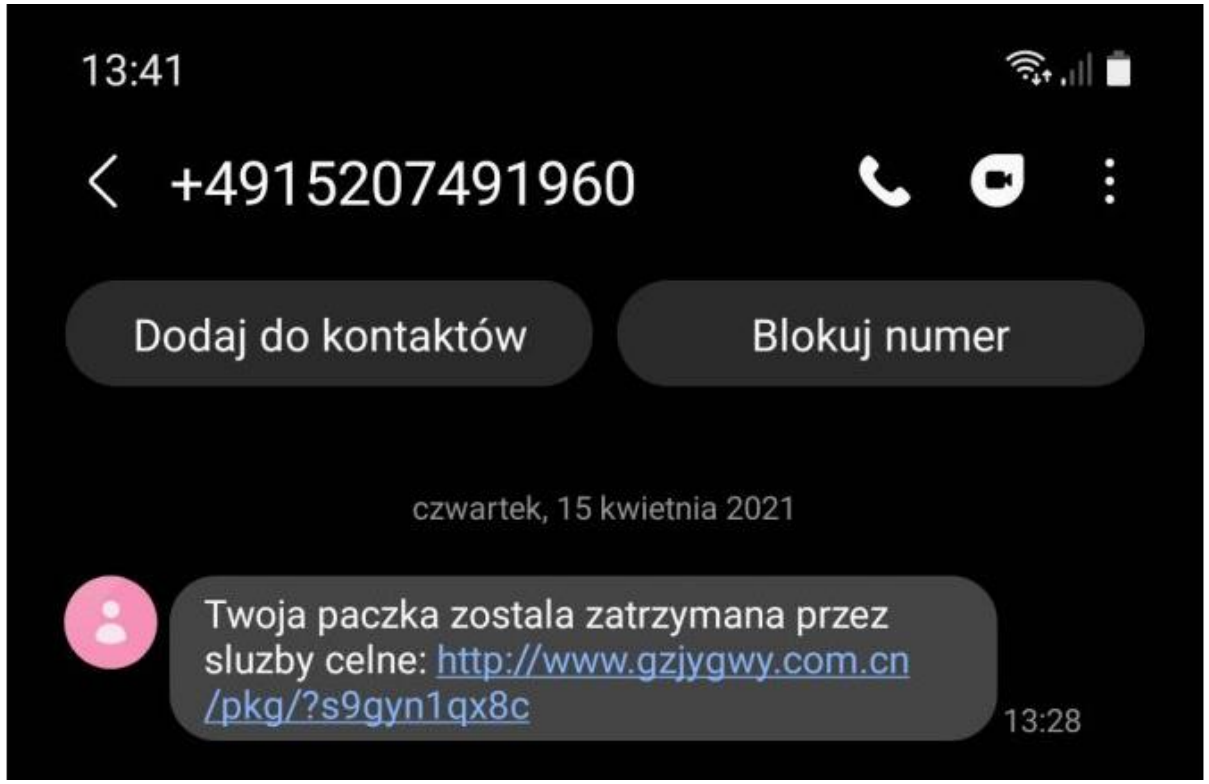
# Phishing – przykłady




Źródło: https://niebezpiecznik.pl

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – przykłady




Źródło: https://kwestiabezpieczenstwa.pl/phishing/

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Phishing – przykłady

07:45

PGE: Na dzien 21.03 zaplanowano odlaczenie energii elektrycznej! Prosimy o uregulowanie naleznosci: https://pgeobrot.click/3w4

Teraz

Payment Detail.xlsx (723,9 KB) Pobierz | Aktówka | Usuń

**Od:** "Eva-Maria Marquardt" <eva-maria.marquardt@Wabtec.com>
**Wysłane:** poniedziałek, 7 lutego, 2022 16:59:08
**Temat:** Transfer confirmation

Hello,

In accordance with agreement, please find in attachment the next Bank Confirmation concerning prepayment by Wabtec.

Many thanks in advance

Mit freundlichen Grüßen / Kind regards

**Eva-Maria Marquardt**
Commodity Buyer Steel Constructions, Raw Material, Coatings

**STEMMANN-TECHNIK GmbH**
Niedersachsenstr. 2 ▪ 48465 Schüttorf ▪ Germany

Tel.: +49 5923 81 148 eva-maria.marquardt@Wabtec.com
Fax: www.stemmann.de
Mobil: +49 ---------- www.wabtec.com

Stemmann-Technik
A Wabtec Company

Źródło: wlasne autora prezentacji

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Co zrobić gdy padliśmy ofiarą ataku

- **Powiadom dział IT/Bezpieczeństwa Informacji/IOD.** Nie wstydź się i nie bój się mówić o ataku. Ostrzeż współpracowników.

- **Zmień hasła.** W przypadku portali internetowych należy zmienić hasło lub zamknąć konto, zanim zrobią to hakerzy;

- **Poinformuj dział obsługi klienta**. Jeśli konto zostało przejęte i nie ma już możliwości zalogowania się poprzednimi danymi, należy skontaktować się z działem obsługi klienta w celu ręcznego przywrócenia danych dostępowych;

Źródło: CERT Polska

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Co zrobić gdy padliśmy ofiarą ataku

- **Skontaktuj się z bankiem w przypadku kradzieży danych bankowych**. Należy niezwłocznie skontaktować się z przedstawicielem banku, aby zablokować karty kredytowe, konta oraz wszystko, co może paść ofiarą cyberprzestępców

- **Ostrzeż instytucję, której dotyczy atak**. Oprócz odzyskiwania danych osobowych warto przekazać wszelkie informacje o ataku instytucji, która została wykorzystana. Pozwoli to podjąć środki zaradcze i ograniczyć potencjalne straty innych użytkowników.

Źródło: CERT Polska

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Jak i gdzie w Twoim Urzędzie zgłaszać phishing

**Każdy incydent powinien zostać zgłoszony zgodnie z obowiązującymi w danej instytucji politykami RODO lub procedurami Systemu Zarządzania Bezpieczeństwem Informacji (KRI, ISO27001)**

**Instytucje realizujące zadania publiczne są zobowiązane do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[1)]**

Źródło: CERT Polska

*1) USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

# Dziękujemy za uwagę.

**Komisja ds. Ochrony Danych Osobowych**

**https://silesia.org.pl/struktura/komisje/komisja-ds-ochrony-danych-osobowych/**