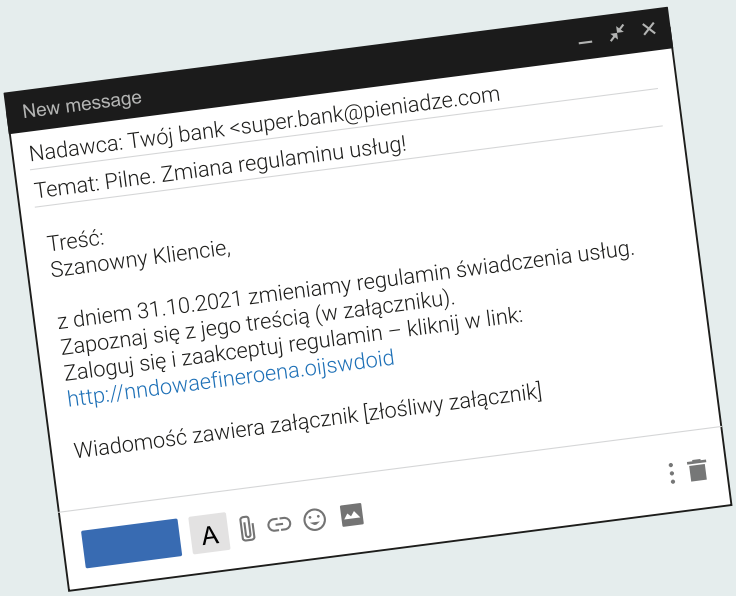
CYBER lekcje
Phishing

Phishing to metoda oszustwa polegająca na tym, że przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

Jak poznać, że wiadomość może być phisihingiem? Co zrobić, by nie dać się złowić w sieci przestępców?

- Zwróć uwagę na nadawcę wiadomości.
- Sprawdź, jak wygląda jego e-mail.
- Oceń, czy np. Twój bank w ten sposób komunikuje się z klientami?
- Porównaj poprzednie wiadomości od zaufanego nadawcy.



TEMAT:
Jeżeli już sam temat maila zawiera w sobie element presji i zmusza do szybkiego działania – **uważaj**.

TREŚĆ:
Zwróć uwagę na ogólnikowe stwierdzenia (Kliencie, Użytkowniku). Literówki czy brak polskich znaków to również sygnały ostrzegawcze. Upewnij się, że szata graficzna maila jest podobna do innych materiałów przesyłanych przez dobrze znanego Ci nadawcę. Czy grafika jest dobrej jakości?

LINKI:
Sprawdź treść linku. Najedź na niego kursorem (**nie klikaj!**) i przyjrzyj się dokładnie, dokąd kieruje Cię link.

ZAŁĄCZNIKI:
Uważaj na załączniki. Może kryć się w nich złośliwe oprogramowanie. Sprawdź rozszerzenie pliku. Najbardziej podejrzane są: .exe, .com, .scr, .vbs, .js – załączniki są często spakowane do formatów .zip i .rar. Najlepiej w ogóle nie otwierać załączników w mailach, których się nie spodziewasz. Zanim otworzysz plik, przeskanuj go programem antywirusowym.

Jeżeli masz jakiekolwiek wątpliwości odnośnie do maila, skontaktuj się z prawdziwym nadawcą – np. za pośrednictwem oficjalnego adresu e-mail banku czy platformy handlowej itp. Warto też skorzystać z infolinii.

Wszelkie podejrzane wiadomości możesz zgłosić na https://incydent.cert.pl/.

NASK NASK akademia KPRM GOV.pl CYFRYZACJA