UNIWERSYTET WARSZAWSKI

Dział Organizacji Zasobów Informacyjnych

Warszawa, dnia 15 maja 2025 roku

UWAGA VISHING – ZACHOWAJ OSTROŻNOŚĆ!

Szanowni Państwo,

w związku z rosnącą liczbą zagrożeń związanych z cyberbezpieczeństwem, pragniemy zwrócić Państwa uwagę na zjawisko **vishingu** – jednej z form oszustw socjotechnicznych, które dotykają również środowisko akademickie.

Czym jest vishing?

Vishing (skrót od "voice phishing") to forma ataku, w której oszuści podszywają się pod zaufane osoby lub instytucje, dzwoniąc do ofiary i próbując wyłudzić poufne informacje, takie jak:

- dane logowania do systemów uczelnianych (np. poczta, USOS, platformy e-learningowe),
- numery kont bankowych,
- dane osobowe,
- informacje o studentach lub innych pracownikach.

Celem vishingu może być także skłonienie ofiary do wykonania przelewu lub kliknięcia w przesłany link.

Jak rozpoznać próbę vishingu?

Oszuści często:

- przedstawiają się jako pracownicy działu IT, administracji (np. IOD) lub instytucji publicznych (np. uczelni, policji, banku, ministerstwa);
- wywierają presję czasową ("To bardzo pilne!", "Jeśli nie zareagujesz natychmiast, konto zostanie zablokowane");

ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa
tel.: 22 55 22 042
e-mail: iod@adm.uw.edu.pl

- proszą o przekazanie danych logowania, kodów SMS, danych osobowych lub finansowych, zachęcają do udziału w ankiecie;
- proponują "pomoc" w zainstalowaniu oprogramowania zdalnego dostępu (np. TeamViewer);
- podają fałszywe numery telefonów lub posługują się numerami przypominającymi te należące do uczelni.

Jak się chronić?

1. **Nie podawaj poufnych informacji przez telefon** – uczelnia nigdy nie prosi o takie dane tą drogą.
2. **Nie instaluj oprogramowania zdalnego na prośbę telefoniczną.**
3. **Zachowaj ostrożność** wobec nieznanych lub podejrzanie brzmiących połączeń.
4. **Nie daj się zastraszyć** – presja i pośpiech to taktyki wykorzystywane przez oszustów.
5. **Zawsze weryfikuj tożsamość rozmówcy** – możesz oddzwonić na oficjalny numer instytucji, z którą rzekomo dzwoniący ma związek.
6. **Nie klikaj w linki przesyłane SMS-em lub e-mailem po rozmowie telefonicznej** bez ich wcześniejszej weryfikacji.

Gdzie zgłaszać incydenty?

W przypadku podejrzenia próby vishingu, prosimy o **niezwłoczny kontakt** z:

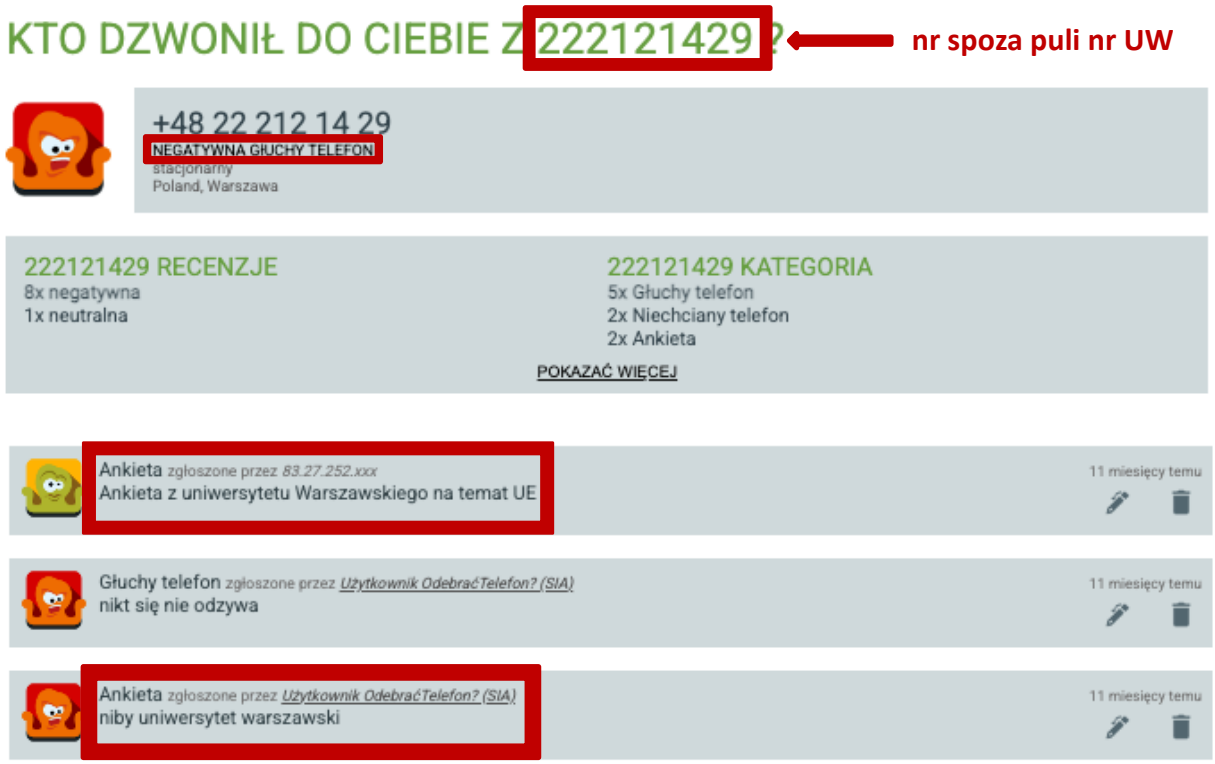
- **Inspektorem Ochrony Danych**: iod@adm.uw.edu.pl
- Można również zgłosić sprawę do **CERT Polska**: https://incydent.cert.pl/

Przykłady prób vishingu:

- telefon rzekomo od "działu IT", z prośbą o pilne potwierdzenie loginu i hasła do konta uczelnianego;
- rozmowa z osobą podającą się za pracownika banku, informującą o "nieautoryzowanym przelewie" i proszącą o dane logowania do bankowości elektronicznej;
- fałszywe telefony od „urzędników”, twierdzących, że potrzebne są dane osobowe pracowników do aktualizacji centralnego rejestru;
- telefon od ankietera podającego się za pracownika uczelni, z prośbą o udział w ankiecie dot. aktualnych wydarzeń i działalności uczelni.

PAMIĘTAJ: Dbajmy wspólnie o bezpieczeństwo naszych danych. W razie wątpliwości – zawsze warto zapytać i upewnić się przed podjęciem działania.

Przykład:


KTO DZWONIŁ DO CIEBIE Z 222121429 ?
nr spoza puli nr UW
+48 22 212 14 29
NEGATYWNA GŁUCHY TELEFON
stacjonarny
Poland, Warszawa
222121429 RECENZJE
8x negatywna
1x neutralna
222121429 KATEGORIA
5x Głuchy telefon
2x Niechciany telefon
2x Ankieta
POKAZAĆ WIĘCEJ
Ankieta zgłoszone przez 83.27.252.xxx
Ankieta z uniwersytetu Warszawskiego na temat UE
11 miesięcy temu
Głuchy telefon zgłoszone przez Użytkownik OdebraćTelefon? (SIA)
nikt się nie odzywa
11 miesięcy temu
Ankieta zgłoszone przez Użytkownik OdebraćTelefon? (SIA)
niby uniwersytet warszawski
11 miesięcy temu