Socjotechnika

SOCJOTECHNIKA, czyli inżynieria społeczna, to działania z wykorzystaniem różnych technik manipulacji. W odniesieniu do cyberataków mają na celu nakłonienie ofiary do podjęcia niekorzystnych dla niej działań, ale intratnych dla przestępcy.

Na co zwracać uwagę?

Wyjątkowość sytuacji

Spadek, nagroda lub specjalne warunki tylko dla Ciebie.

Angażowanie emocji

Wiadomości i powiadomienia wywołują u Ciebie lęk, strach, radość lub zaskoczenie.

Presja czasu

Musisz podjąć działania, w krótkim czasie.

Nietypowe zachowanie

Znajomy nagle prosi Cię o szybką pożyczkę, opłatę zakupów, pisze w inny sposób niż zwykle.

Phishing

to najczęstszy typ ataku wykorzystującego m.in. socjotechnikę, w którym oszuści podszywają się pod wiarygodne źródła, aby skłonić ofiarę do podjęcia określonych działań, mogących prowadzić do zainstalowania złośliwego oprogramowania lub kradzieży danych i pieniędzy.

Najczęstsze metody ataku

- **E-mail**
- **SMS**
- **Połączenia telefoniczne**
- **Komunikatory**

Jak się chronić?

1. **BĄDŹ NA BIEŻĄCO** z informacjami o oszustwach i aktualizuj swoją wiedzę o tym, jak się chronić.
2. **ZWRACAJ UWAGĘ** na treść, emocje i presję czasu w otrzymywanych wiadomościach i rozmowach.
3. **STOSUJ** unikalne hasła do każdej usługi.
4. **WŁĄCZ** weryfikację dwuetapową i automatyczne aktualizacje na swoich urządzeniach.
5. **ZGŁASZAJ** nietypowe wiadomości do działu bezpieczeństwa lub IT w Twojej organizacji oraz do zespołu CERT Polska (incydent@cert.pl, SMS na numer 8080).

NASK

EUROPEJSKI MIESIĄC CYBERBEZPIECZEŃSTWA

PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTRA CYFRYZACJI