Warsztaty 7: Deepfake i oszustwa AI
Plan domowy: drugi kanal, haslo, pierwsze 10 minut

Cel tej karty

Ta karta pomaga ustalic z bliskimi prosta procedure na sytuacje, w ktorej ktos dzwoni, pisze albo wysyla nagranie i prosi o kod, pieniadze, dane, klikniecie w link albo szybka instalacje aplikacji.

Nie musimy od razu wiedziec, czy to deepfake.
Mamy zatrzymac akcje i sprawdzic prosbe drugim kanalem.

1. PLAN 3-2-1

3 sprawy, ktorych nie robimy pod presja:

[ ] nie podajemy kodu BLIK
[ ] nie robimy przelewu
[ ] nie podajemy danych dokumentu, karty, loginu ani hasla

2 kanaly powrotu:

[ ] znany numer telefonu zapisany w kontaktach
[ ] drugi kontakt awaryjny: rodzic, dorosle dziecko, sasiedzi, opiekun, instytucja z oficjalnej strony albo numer z dokumentu/karty

1 haslo albo pytanie kontrolne:

[ ] ustalone offline, zanim zdarzy sie kryzys
[ ] nie jest data urodzin, imieniem zwierzecia ani informacja z Facebooka
[ ] mozna je spokojnie zmienic, gdy ktos je uslyszy albo podejrzy

Przyklad:
Pytanie: Co zawsze kupujemy do herbaty, gdy jedziemy na dzialke?
Odpowiedz: To, co ustalimy miedzy soba offline.

2. ZDANIE, KTORE KAZDY MOZE POWIEDZIEC

Jesli prosisz mnie o kod, pieniadze albo dane, rozlacze sie i oddzwonie na znany numer.

Wazne:
To nie jest brak zaufania do bliskiej osoby.
To jest sposob ochrony bliskiej osoby przed podszyciem.

3. DRUGI KANAL W PRAKTYCE

Gdy prosba przychodzi przez:

telefon:
- rozlaczam sie,
- oddzwaniam na numer zapisany w kontaktach,
- jesli osoba nie odbiera, dzwonie do drugiej zaufanej osoby.

SMS albo komunikator:
- nie klikam linku,
- nie odpowiadam w tym samym watku,
- otwieram aplikacje banku, urzedu albo firmy samodzielnie.

wideopolaczenie:
- nie pokazuje dokumentu ani ekranu,
- koncze rozmowe,
- wracam znanym numerem lub innym ustalonym kontaktem.

reklama albo post:
- nie klikam przycisku z reklamy,
- wpisuje adres samodzielnie,
- sprawdzam oficjalna strone, liste ostrzezen lub niezalezne zrodlo.

4. PIERWSZE 10 MINUT PO KLIKNIECIU

0-2 minuty: przerwij akcje

[ ] koncze rozmowe
[ ] nie instaluje niczego wiecej
[ ] nie podaje kolejnych danych
[ ] jesli ktos mial zdalny dostep, odlaczam urzadzenie od internetu

2-5 minut: zabezpiecz pieniadze i konta

[ ] dzwonie do banku numerem z karty lub oficjalnej strony
[ ] prosze o blokade karty, przelewu, konta albo dostepu
[ ] zmieniam haslo z innego, zaufanego urzadzenia
[ ] wlaczam lub sprawdzam uwierzytelnianie dwuskladnikowe

5-10 minut: zachowaj slady

[ ] robie zrzuty ekranu
[ ] zapisuje numer, link, nazwe profilu i godzine rozmowy
[ ] nie kasuje SMS-a, maila ani historii polaczenia
[ ] przekazuje podejrzany SMS z linkiem na numer 8080
[ ] zglaszam incydent przez https://incydent.cert.pl/

Zasada:
Szybkie zgloszenie jest lepsze niz idealny opis sytuacji.

5. UMOWA RODZINNA DO UZUPELNIENIA

Nasz znany numer do oddzwaniania:

1. .....
2. .....

Druga osoba do sprawdzenia pilnej prosby:

1. .....
2. .....

Nasze pytanie kontrolne albo haslo:

.....

Kiedy haslo nie wystarcza:

[ ] gdy chodzi o przelew, kod, karte, dokument albo instalacje aplikacji
[ ] gdy rozmowca mowi: nikomu nie mow
[ ] gdy rozmowca nie pozwala sie rozlaczyc
[ ] gdy historia jest bardzo emocjonalna i wymaga natychmiastowej decyzji

Wtedy nadal robimy drugi kanal.

6. MINI DRILL DO POWTORZENIA W DOMU

Runda 1:
"Mamo, mialem wypadek, szybko wyslij kod BLIK."

Odpowiedz:
"Rozlaczam sie i oddzwaniam na znany numer."

Drugi kanal:
.....

Runda 2:
"Dzwonie z banku. Na pani koncie jest atak. Prosze zainstalowac aplikacje."

Odpowiedz:
"Nie instaluje niczego z telefonu. Samodzielnie kontaktuje bank."

Drugi kanal:
.....

Runda 3:
"To ostatnia szansa na odbior doplaty. Kliknij link i doplac 1,99 zl."

Odpowiedz:
"Nie klikam linku z SMS-a. Sprawdzam sprawe samodzielnie."

Drugi kanal:
.....

7. GDZIE SPRAWDZAC I ZGLASZAC

- CERT Polska: https://incydent.cert.pl/
- Kontakt CERT Polska i SMS 8080: https://cert.pl/kontakt/
- NASK o rozpoznawaniu deepfake: https://www.nask.pl/aktualnosci/jak-rozpoznac-deepfake-po-bledach-logicznych
- Policja: https://policja.pl/
- CEBRF KNF o falszywych inwestycjach: https://cebrf.knf.gov.pl/falszywe-inwestycje

ZDANIE NA KONIEC

Deepfake moze udawac glos, twarz i emocje.
Nie musi udawac naszych zasad.