Warsztaty 7: Deepfake i oszustwa AI
Drill: Czerwona sluchawka

CEL

To nie jest test wiedzy o deepfake.
To jest trening odruchu:

1. koncze rozmowe albo nie odpowiadam w podejrzanym kanale,
2. nie podaje kodu, danych, hasla ani pieniedzy,
3. wybieram drugi kanal, ktory nie pochodzi od rozmowcy,
4. decyzje podejmuje dopiero po sprawdzeniu.

Runda jest zaliczona dopiero wtedy, gdy uczestnik zrobi dwa kroki:

KROK A: przerwanie presji
KROK B: wskazanie bezpiecznego drugiego kanalu

Zdanie drillowe:
Nie musze tego rozstrzygac w tej rozmowie.
Rozlaczam sie i sprawdzam drugim kanalem.

JAK PROWADZIC

1. Prowadzacy czyta role "rozmowcy" albo "wiadomosci".
2. Uczestnik nie tlumaczy sie dlugo.
3. Uczestnik mowi jedno krotkie zdanie przerwania.
4. Uczestnik wskazuje drugi kanal sprawdzenia.
5. Grupa dopowiada, czego nie robimy pod presja.

Nie udajemy prawdziwych osob, marek ani instytucji.
Wszystkie rozmowy sa fikcyjne.

DRILL 1: GLOS BLISKIEJ OSOBY

Rozmowca:
"Hej, to ja. Stoje przy kasie i karta nie dziala.
Wyslij mi szybko kod BLIK, oddam za 10 minut.
Nie oddzwaniaj, telefon mi pada.
Masz tylko chwile, kolejka patrzy."

Oczekiwana reakcja:
"Nie wysylam kodu przez telefon. Rozlaczam sie i oddzwaniam
na znany numer."

Drugi kanal:
Znany numer tej osoby, zapisany wczesniej w kontaktach.

Czego nie robimy:
- nie podajemy kodu,
- nie zostajemy na linii,
- nie dajemy sie popchnac presja czasu.

DRILL 2: TELEFON Z INSTYTUCJI

Rozmowca:
"Dzwonie w sprawie zagrozenia na koncie.
Prosze zostac na linii, system zamknie sprawe za kilka minut.

Wysle link do aplikacji zabezpieczajacej.
Jesli sie rozlaczymy, srodki moga przepasc."

Oczekiwana reakcja:
"Nie zalatwiam tego w tej rozmowie. Rozlaczam sie i samodzielnie
wybieram oficjalny numer instytucji."

Drugi kanal:
Oficjalna strona albo znany numer banku, urzedu lub organizacji,
wpisany samodzielnie.

Czego nie robimy:
- nie instalujemy aplikacji z linku,
- nie podajemy kodow ani danych logowania,
- nie zostajemy na linii dlatego, ze ktos tego wymaga.

DRILL 3: PILNA ZBIORKA

Wiadomosc:
"Pilna pomoc, liczy sie kazda minuta.
Wplac przez ten link, zwykla strona jest przeciazona.
Kto nie udostepnia, ten nie ma serca.
Zbiorka znika dzis o polnocy."

Oczekiwana reakcja:
"Nie klikam linku z wiadomosci. Jesli chce pomoc, wchodze samodzielnie
na oficjalna strone organizacji."

Drugi kanal:
Oficjalna strona organizacji, znana platforma lub niezalezne potwierdzenie.

Czego nie robimy:
- nie klikamy linku z presji,
- nie wplacamy "malej kwoty na probe",
- nie udostepniamy zanim sprawdzimy zrodlo.

DRILL 4: SMS Z DOPLATA

Wiadomosc:
"Doplata 1,49 zl wymagana do realizacji.
Brak platnosci dzisiaj spowoduje anulowanie.
Oplac teraz przez link w wiadomosci.
To ostatnie przypomnienie."

Oczekiwana reakcja:
"Nie klikam linku z SMS-a. Sprawdzam sprawe w oficjalnej aplikacji
albo na stronie wpisanej samodzielnie."

Drugi kanal:
Oficjalna aplikacja, konto klienta albo strona wpisana samodzielnie.
Podejrzany SMS z linkiem mozna przekazac na numer 8080.

Czego nie robimy:
- nie klikamy linku z SMS-a,
- nie placimy malej kwoty "dla spokoju",
- nie odpowiadamy na podejrzany SMS.

DRILL 5: REKLAMA INWESTYCYJNA

Reklama i telefon:
"Znana osoba pokazuje prosty sposob na dodatkowy dochod.
Zostaw numer telefonu, oddzwonimy z dostepem tylko dzis.
Wystarczy mala wplata startowa.
Prosze nie zwlekac, liczba miejsc jest ograniczona."

Oczekiwana reakcja:
"Nie podaje danych i nie wplacam pieniedzy z reklamy.
Sprawdzam ostrzezenia i oficjalne zrodla."

Drugi kanal:
Oficjalne ostrzezenia, rejestry i strony znalezione samodzielnie,
nie przez link z reklamy ani konsultanta.

Czego nie robimy:
- nie zostawiamy telefonu "tylko po informacje",
- nie wplacamy kwoty startowej,
- nie uznajemy znanej twarzy za dowod prawdziwosci.

DRILL 6: WIDEOPOLOCZENIE Z PROSBA

Rozmowca:
"To ja, kamera slabo dziala, jestem w klopocie.
Nie moge mowic dlugo, potrzebuje przelewu albo kodu.
Nie dzwon do nikogo, bo tylko pogorszysz sprawe.
Zaufaj mi, przeciez mnie widzisz."

Oczekiwana reakcja:
"Nie podejmuje decyzji w tym polaczeniu. Koncze rozmowe
i sprawdzam ustalonym kanalem."

Drugi kanal:
Znany numer, ustalone haslo rodzinne albo kontakt z inna zaufana osoba
poza podejrzanym polaczeniem.

Czego nie robimy:
- nie robimy przelewu dlatego, ze widzimy twarz,
- nie zostajemy w rozmowie, zeby "lepiej rozpoznac",
- nie przyjmujemy nowego linku do rozmowy od tej samej osoby.

MINI-SCORE DLA UCZESTNIKA

[ ] zakonczylem/zakonczylam podejrzany kanal
[ ] nie podalem/podalam kodu, danych ani pieniedzy
[ ] wskazalem/wskazalam drugi kanal niezalezny od rozmowcy
[ ] powiedzialem/powiedzialam krotkie zdanie bez tlumaczenia sie
[ ] decyzje odlozylem/odlozylam do czasu sprawdzenia

DEBRIEF PO SZESCIU RUNDACH

Zapytaj:

1. Ktory moment najbardziej zachecal do tlumaczenia sie?
2. Ktory drugi kanal byl najlatwiejszy do wskazania?
3. Gdzie brakowalo gotowego numeru, adresu albo rodzinnego hasla?
4. Ktore zdanie przerwania bylo najlatwiejsze do powiedzenia?
5. Komu warto przekazac zasade czerwonej sluchawki po warsztacie?

ZDANIE NA KONIEC

Nie musze wiedziec od razu, czy to deepfake.
Mam zatrzymac akcje i sprawdzic zrodlo.