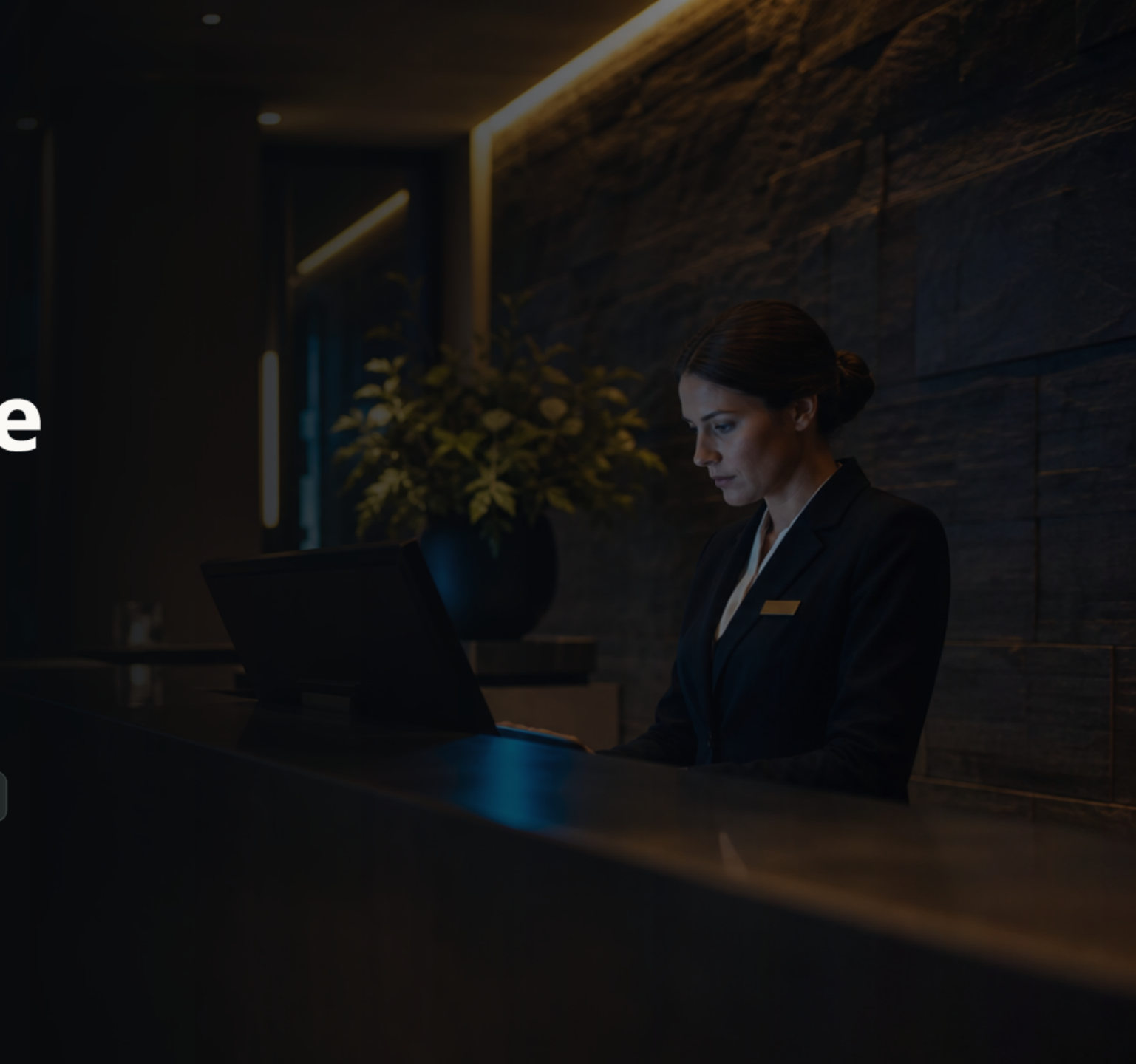


Phishing w hotelarstwie

Kiedy wiadomość zna rezerwację,
pośpiech staje się podatnością.

90 MIN

RECEPCJA • REZERWACJE • FINANSE



„Płatność gościa została odrzucona.”

Wiadomość zawiera nazwisko, numer rezerwacji i datę przyjazdu.

Prosi o ponowne logowanie w ciągu 30 minut.

Co robisz najpierw?

A • KLIKAM

B • DZWONIĘ DO GOŚCIA

C • WERYFIKUJĘ OSOBNO

Po 90 minutach wykonasz trzy ruchy bez zgadywania

01

Zatrzymasz

akcję, zanim presja przejmie decyzję.

02

Zweryfikujesz

prośbę poza kanałem, który ją przyniósł.

03

Zgłosisz

incydent szybko — także po kliknięciu.

Nie musisz zostać analitykiem. Masz umieć zatrzymać ryzykowną akcję.

DLACZEGO HOTELARSTWO?

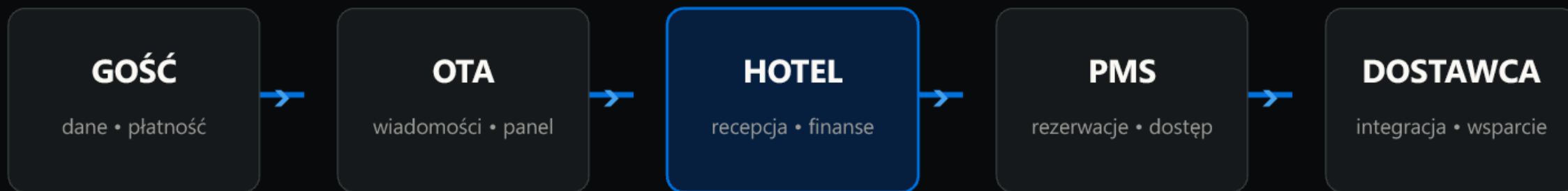
Hotel pracuje w wielu kanałach. Atakujący też.

Rezerwacje, poczta, OTA, PMS, telefon, komunikatory, płatności, dostawcy i zmiany pracowników — wszystko spotyka się przy jednej decyzji.

SZYBKOŚĆ OBSŁUGI

ROZPROSZONE ZAUFANIE

Jedna rezerwacja przechodzi przez łańcuch zaufania



E-MAIL

SMS / WHATSAPP

TELEFON

PANEL PARTNERA

Każdy węzeł może być prawdziwy. Każdy kanał może zostać podszyty.

Atakujący nie chce tylko hasła

- | | | |
|----|------------------------|--|
| 01 | DOSTĘP | skrzynka • panel OTA • PMS |
| 02 | PIENIĄDZE | dopłata • faktura • zmiana rachunku |
| 03 | ZAUFANIE GOŚCIA | wiadomość z prawdziwym kontekstem |
| 04 | CZAS | ukryta reguła • sesja • dalsze podszycie |

Najcenniejsze jest konto, które wygląda zwyczajnie i zna codzienny proces.

Jedno logowanie może uruchomić phishing do gości



Prawdziwe dane tworzą fałszywe poczucie pewności.

Kanał i dostawca realnie zmieniają ryzyko

40%

wyższy medianowy poziom skutecznych kliknięć w symulacjach zaczynających się od telefonu lub SMS-a niż od e-maila

48%

naruszeń w DBIR 2026 obejmowało udział strony trzeciej — partnera, dostawcy lub innego elementu łańcucha

Dane globalne nie opisują każdego hotelu. Pokazują, gdzie warto ćwiczyć decyzje.

Nie szukaj literówek. Szukaj ryzykownej prośby.

Dzień dobry Pani Marto,

w rezerwacji 48172 wykryliśmy niezgodność płatności. Aby utrzymać dostępność pokoju, prosimy o ponowne potwierdzenie konta przed 18:15.

Z poważaniem,
Zespół Partner Support

BRZMI POPRAWNIE

ale prosi o:

- pilne logowanie
- działanie z wiadomości
- zaufanie do numeru rezerwacji

Treść ma przekonać. Kontekst ma ją uwierzytelnić.

02

Najpierw kontekst. Dopiero potem treść.

Cztery sygnały, które zatrzymują działanie.

Cztery miejsca ujawniają więcej niż cała treść



Partner Support

alert@hotel-panel.example

Pilna weryfikacja rezerwacji 48172

Nie udało się zsynchronizować płatności gościa. Aby uniknąć anulowania, zaloguj się ponownie i potwierdź konto do 18:15.

POTWIERDŹ KONTO

1

Pełny adres i domena

2

Presja czasu lub straty

3

Czynność: login, plik, płatność

4

Czy można sprawdzić to osobno?

Nazwa nadawcy jest etykietą. Domena jest wskazówką.

Partner Support

TA SAMA NAZWA MOŻE STAĆ NAD DWOMA ADRESAMI

support@panel.hotel.example

adres znany z procedury hotelu

support@hotel-panel.example

podobny wygląd ≠ znana domena

Domena nie dowodzi bezpieczeństwa. Rozbieżność wystarcza jednak, by zatrzymać akcję.

Link i kod QR skracają drogę — także do błędnej decyzji

secure-ota.example/verify

**Zaloguj się ponownie,
aby zachować rezerwacje**

KONTYNUUJ

NA TELEFONIE CEL BYWA UKRYTY

1

Nie loguj się z linku w wiadomości

2

Otwórz portal z zapisanej zakładki

3

Kod QR traktuj jak niewidoczny link

Zmiana rachunku nie jest informacją. Jest procesem ryzyka.

1

WSTRZYMAJ

nie zlecaj przelewu

2

ODDZWOŃ

na zapisany numer

3

POTWIERDŹ

z drugą osobą

Ten sam kanał, który przyniósł zmianę, nie może jej sam potwierdzić.

ĆWICZENIE 1

Trzy wiadomości. Jedna zasada.

Masz 20 sekund na decyzję:

OBSŁUŻ

SPRAWDŹ

ESKALUJ

Nie pytamy „czy to na pewno phishing?”. Pytamy „czy ta akcja jest bezpieczna teraz?”.

A • Gość wysyła „dokument rezerwacji”



Anna Kowalska

anna.kowalska@example.com

Późny przyjazd — rezerwacja 48172

Dzień dobry, przesyłam dokument potrzebny do późnego zameldowania. Plik jest zabezpieczony hasłem: 2026. Proszę potwierdzić odbiór.

reservation_details.html

DECYZJA

Otwierasz załącznik?

OBSŁUŻ

SPRAWDŹ

ESKALUJ

Nie musisz wiedzieć, czy gość jest prawdziwy

1 Nie otwieraj pliku HTML ani pliku chronionego hasłem z niespodziewanej wiadomości

2 Sprawdź rezerwację bezpośrednio w PMS

3 Skontaktuj się z gościem przez dane zapisane w rezerwacji

BEZPIECZNA DECYZJA: ZWERYFIKUJ • ESKALUJ, JEŚLI ZAŁĄCZNIK ZOSTAŁ OTWARTY

B • „Partner Support” pisze na WhatsAppie

PS

Partner Support

WhatsApp • nowy numer

Dzień dobry. 7 rezerwacji nie zsynchronizowało się z Państwa obiektem. Konto zostanie ograniczone za 30 minut. Proszę zeskanować kod i potwierdzić dane logowania.



DECYZJA

Skanujesz kod?

OBSŁUŻ

SPRAWDŹ

ESKALUJ

Prawdziwy numer rezerwacji nie uwierzytelnia nadawcy

DANE

**„7 rezerwacji”
„konto obiektu”**

mogą być prawdziwe



TOŻSAMOŚĆ

**„to naprawdę
Partner Support”**

wymaga osobnej weryfikacji

OTWÓRZ PANEL Z ZAKŁADKI • SPRAWDŹ ALERTY • ZGŁOŚ WIADOMOŚĆ

C • Dostawca zmienia rachunek na fakturze



Anna Nowak • LinenPro

anna.nowak@linenpro.example

Nowy rachunek od sierpnia

Ze względu na zmianę banku proszę opłacać wszystkie kolejne faktury na nowy IBAN. Dzisiejsza płatność może już zostać wysłana na nowe konto.

FAKTURA_07_2026.PDF

DECYZJA

Zmieniasz dane?

OBSŁUŻ

SPRAWDŹ

ESKALUJ

Najdroższa wiadomość może być całkowicie poprawna językowo

01

WSTRZYMAJ

płatność i zmianę danych

02

ODDZWOŃ

na numer zapisany wcześniej

03

ZATWIERDŹ

z drugą uprawnioną osobą

BEZPIECZNA DECYZJA: ZWERYFIKUJ • NIE UŻYWAJ NUMERU Z TEJ WIADOMOŚCI

Jedna procedura na e-mail, SMS, WhatsApp i telefon

S**Stój**

Nie klikaj, nie odpowiadaj, nie zatwierdzaj.

T**Tożsamość**

Sprawdź pełny adres, domenę, kanał i kontekst.

O**Otwórz osobno**

Wejdź z zakładki lub zadzwoń na znany numer.

P**Powiadom**

Zgłoś szybko — również po kliknięciu.

STOP

**Nie udowadniaj,
że wiadomość jest fałszywa.**

Zatrzymaj ryzykowną akcję.

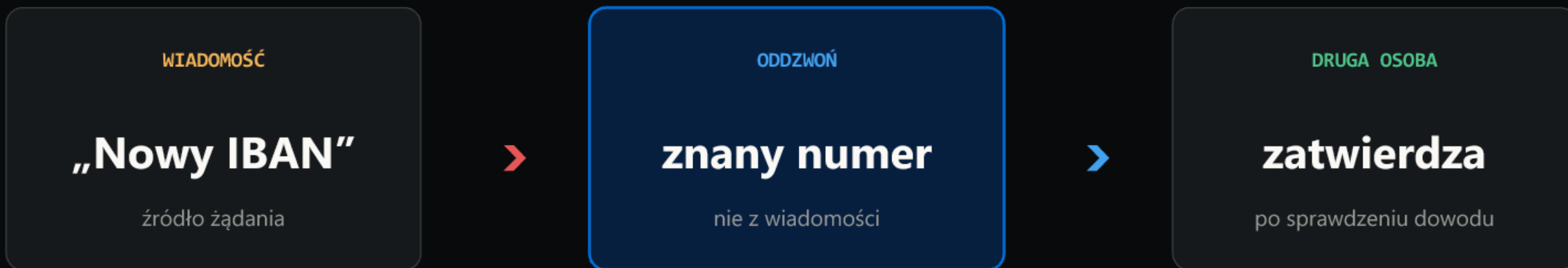
Recepcja chroni gościa, zanim chroni skrzynkę

GDY WIADOMOŚĆ DOTYCZY REZERWACJI

- 1 Sprawdź rezerwację w PMS**
nie przez link z wiadomości
- 2 Nie ujawniaj nowych danych**
nadawcy, który już zna część informacji
- 3 Użyj kontaktu z rezerwacji**
nie numeru dostanego w wiadomości
- 4 Zgłoś próbę podszycia**
zanim podobna wiadomość trafi do kolejnej zmiany

PROFESJONALNA ODPOWIEDŹ: „SPRAWDZĘ TO W SYSTEMIE I WRÓCĘ DO PAŃSTWA ZNANYM KANAŁEM.”

Zmiana rachunku wymaga drugiego kanału i drugiej osoby



Dwie osoby w tym samym e-mailu to nadal jeden kanał.

Nieoczekiwana prośba o MFA nie jest formalnością

**Czy zatwierdzasz
logowanie?**

Warszawa • nowe urządzenie
Kod dopasowania: 73

ODRZUĆ

ZATWIERDŹ

1

Odrzuć, jeśli nie rozpoczęłeś logowania

2

Nie podawaj kodu rozmówcy ani „wsparciu”

3

Zgłoś próbę i sprawdź aktywne sesje

**Dla kont kluczowych: passkeys / FIDO zamiast kodów
możliwych do wyłudzenia.**

PO KLIKNIĘCIU

Liczy się szybkość. Nie wstyd.

Szybkie zgłoszenie ogranicza zasięg,
chroni gości i daje zespołowi
technicznemu czas.

ZGŁOŚ TERAZ — NIE PO ZMIANIE

Pierwsze minuty zależą od tego, co już się stało

TYLKO KLIK

Zamknij stronę
Zapisz wiadomość / adres
Zgłoś próbę

DANE LOGOWANIA

Skontaktuj IT
Zmień hasło z zaufanej
ścieżki
Unieważnij sesje i MFA

PLIK / PŁATNOŚĆ

Zgłoś natychmiast
Wstrzymaj pracę na
urządzeniu
Bank + finanse przy
przelewie

W KAŻDYM WARIANCIE: NIE KASUJ WIADOMOŚCI • NIE UKRYWAJ ZDARZENIA • PODAJ CZAS I URZĄDZENIE

Trzy odruchy, które powiększają incydent

- 01 NIE KASUJ** wiadomości, pliku ani historii
- 02 NIE NAPRAWIAJ PO CICHU** bez zgłoszenia i unieważnienia sesji
- 03 NIE CZEKAJ** do końca zmiany lub powrotu managera

Najlepszy raport zaczyna się od: „To wydarzyło się przed chwilą. Oto co zrobiłem.”

17:46 przed weekendem weselnym

120

zameldowań do 20:00

2

osoby na recepcji

7rzekomo
„niesynchronizowanych”
rezerwacji**30 min**do blokady konta —
według wiadomości

Pracujecie jako jedna zmiana. Decyzje muszą być konkretne: kto, co, którym kanałem.

Runda 1 • Wiadomość trafia do recepcji

**Partner Support**

WhatsApp • nowy numer

7 rezerwacji nie zsynchronizowało się. Konto obiektu zostanie ograniczone o 18:15. Proszę potwierdzić login przez kod QR.

90 SEKUND

Ustalcie:

1. Kto zatrzymuje akcję?
2. Gdzie sprawdzacie rezerwacje?
3. Jak kontaktujecie partnera?
4. Komu zgłaszacie próbę?

ODPOWIEDŹ = OSOBA + CZYNNOŚĆ + KANAŁ

Runda 2 • Kolega już wpisał login i kod MFA

17:51

**„Myślałem, że to prawdziwy panel.
Wpisałem hasło i kod. Strona się
zamknęła.”**

Laptop nadal działa normalnie.

90 SEKUND

Pierwsze trzy działania:

- kto kontaktuje IT?
- jak zmieniacie poświadczenia?
- kto unieważnia sesje?
- co zapisujecie jako dowód?

Runda 3 • Gość dzwoni o „pilną dopłatę”



Gość • rezerwacja 48172

**„Dostałam SMS z nazwą hotelu,
terminem pobytu i linkiem do dopłaty
240 zł. Czy rezerwacja jest zagrożona?”**

Gość jeszcze nie zapłacił.

90 SEKUND

Ustalcie:

1. Co mówicie gościowi?
2. Jak chronić pozostałych?
3. Kto zabezpiecza konto?
4. Co zachować do analizy?

Dobra reakcja biegnie dwoma torami jednocześnie

TOR 1 • OBSŁUGA

Potwierdź rezerwację
Zatrzymaj fałszywą płatność
Daj gościowi znany kanał

TOR 2 • INCYDENT

Zabezpiecz konto i sesje
Sprawdź zasięg wiadomości
Zachowaj ślady i eskaluj

GOŚCINNOŚĆ NIE WYMAGA ZAUFANIA DO WIADOMOŚCI. WYMAGA BEZPIECZNEJ DROGI OBSŁUGI.

Pracownik nie może być jedyną zaporą

01	MFA odporne na phishing	dla kont kluczowych i partnerów
02	Przycisk / kanał zgłoszeń	widoczny na każdej zmianie
03	Proces zmian płatniczych	drugi kanał + druga osoba
04	Dostęp według roli	bez wspólnych kont i nadmiarowych uprawnień
05	Ćwiczenia branżowe	e-mail, telefon, WhatsApp, OTA

SZKOLENIE DZIAŁA NAJLEPIEJ, GDY PROCEDURA POZWALA WYKONAĆ DOBRĄ DECYZJĘ.

ZASADA NA NASTĘPNĄ ZMIANĘ

Nie musisz udowodnić, że wiadomość jest fałszywa.

Musisz zatrzymać ryzykowną akcję.

STÓJ • TOŻSAMOŚĆ • OTWÓRZ OSOBNO • POWIADOM

Szkolenia i ćwiczenia phishingowe dla organizacji

breachroad.com

