



#BH

PORADNIK

CYBERHIGIENA DLA PERSONELU OCHRONY



BH
BezpiecznyHandel.pl
blog o kradzieżach w handlu

Cyberhigiena dla personelu ochrony - najważniejsze zasady.

Chroń organizację przed incydemem wycieku i utraty danych oraz paraliżem systemów.

1 Nie rób zdjęć na służbie

👉 Nie wykonuj i nie upubliczniaj zdjęć z pomieszczeń służbowych. W tle mogą znajdować się grafiki, plany obiektu, widoki z kamer, dane kontaktowe. Takie materiały mogą ułatwić atak socjotechniczny.

2 Uważaj na pocztę elektroniczną

- 👉 Nie klikaj w podejrzaną linki, obrazki i nie pobieraj załączników od nieznanych nadawców.
- 👉 Zawsze sprawdzaj dokładny adres e-mail nadawcy (często różni się od prawdziwego jednym znakiem).
- 👉 Zachowaj szczególną ostrożność wobec nietypowych żądań, np. prośby o dane logowania, hasła czy dokumenty.

3 Nie daj się złapać na SMS-y

- 👉 Traktuj z rezerwą wiadomości zawierające linki i żądania szybkiej reakcji.
- 👉 Nie klikaj w linki z SMS-ów od nieznanych numerów.
- 👉 W razie wątpliwości skontaktuj się z przełożonym, zanim podejmiesz jakiegokolwiek działanie.

4 Obce nośniki to ryzyko

- 👉 Jeśli znalazłeś pendrive, dysk czy inny nośnik danych, nie podłączaj go do służbowych urządzeń.
- 👉 Zgłoś ten fakt przełożonemu.
- 👉 Traktuj każdy obcy nośnik jako potencjalne źródło zagrożenia.

5 Nie podłączaj prywatnych sprzętów

- 👉 Nie podłączaj prywatnych sprzętów do urządzeń i sieci firmowej.
- 👉 To może narazić firmową sieć na zainfekowanie wirusem lub wyciek danych.

6 Korzystaj bezpiecznie komputera i internetu

- 👉 Używaj służbowego komputera i przeglądarki wyłącznie do zadań związanych z pracą.
- 👉 Stosuj silne hasła logowania (tj. odpowiednio długie, ze znakami specjalnymi, unikaj powtarzania haseł) i zachowuj je wyłącznie dla siebie.
- 👉 Nie pobieraj plików ani nie próbuj instalować oprogramowania z nieznanych źródeł.
- 👉 Każde działanie wykraczające poza obowiązki służbowe traktuj jako potencjalne zagrożenie.

7 Czujność wobec nieautoryzowanych wizyt i telefonów

- 👉 Zwracaj szczególną uwagę na osoby podające się za serwisantów, które żądają dostępu do urządzeń lub sieci, a ich wizyta nie wynika z awizacji ani z rzeczywistych potrzeb serwisowych.
- 👉 Jeśli ktoś dzwoni z nieznanego numeru i przedstawia się jako przełożony lub „dział IT”, oczekując szybkich działań (np. podania haseł, zmian w systemie), zachowaj ostrożność.
- 👉 Każde nietypowe żądanie weryfikuj u przełożonego.

Ważne ! Powyższe zagadnienia nie wyczerpują wszystkich możliwych scenariuszy dobrych praktyk. Należy traktować je jako dobry punkt wyjścia do opracowania własnych, dostosowanych do potrzeb organizacji instrukcji.