eauditor

PORADNIK DLA PRACOWNIKÓW

Black Friday – 6 zasad bezpiecznych zakupów online

Zanim otworzysz link, podasz dane lub zatwierdzisz płatność, sprawdź, skąd pochodzi prośba.

01

Sprawdź adres i sprzedawcę

Zwróć uwagę na literówki i dodatkowe słowa w adresie. Sprawdź dane firmy oraz opinie poza jej sklepem. Sama kłódka nie potwierdza uczciwości sprzedawcy.

02

Zweryfikuj ofertę poza reklamą

Otwórz oficjalną stronę marki samodzielnie i poszukaj tej samej promocji. Reklama sponsorowana również może prowadzić do fałszywego sklepu.

03

Paczkę sprawdź w aplikacji kuriera

SMS o dopłacie lub zmianie adresu? Sprawdź przesyłkę w aplikacji przewoźnika albo w historii zamówienia.

04

Chroń hasła i potwierdzenia logowania

Używaj różnych haseł i włącz dodatkową weryfikację logowania, jeśli jest dostępna. Odrzucaj prośby o potwierdzenie logowania, którego nie zaczynałeś.

05

Czytaj potwierdzenie płatności

Sprawdź kwotę, odbiorcę i rodzaj operacji. Przerwij, jeśli komunikat dotyczy czegoś innego niż planowany zakup.

06

Zgłaszaj podejrzane zdarzenia

Po otwarciu podejrzanego linku na służbowym sprzęcie poinformuj IT. Powiedz, czy wpisałeś dane, pobrałeś lub uruchomiłeś plik albo zatwierdziłeś operację.

Kliknąłeś podejrzany link? Zgłoś to do działu IT.
Nawet jeśli nic się nie stało.

Podałeś dane lub podejrzewasz wyciek?

Hasło

Z zaufanego urządzenia otwórz oficjalny serwis, zmień hasło i zakończ pozostałe sesje, jeśli serwis na to pozwala. Zmień je też tam, gdzie było takie samo. Przy koncie firmowym od razu skontaktuj się z IT.

Karta lub płatność

Pilnie skontaktuj się z bankiem przez aplikację lub oficjalny numer. Zastrzeż ujawnioną kartę i zgłoś podejrzane transakcje.

Dane firmowe lub pobrany plik

Zgłoś sprawę do IT. Zachowaj wiadomość zanotuj czas i podane dane. Nie kasuj historii, ani plików i nie instaluj narzędzi naprawczych na własną rękę.

→ https://www.eauditor.eu/blog/co-zrobic-po-incydencie-bezpieczenstwa

Materiał edukacyjno-marketingowy BTC. Zawiera ogólne wskazówki i nie zastępuje firmowej procedury reagowania, indywidualnej oceny incydentu ani porady specjalisty. Dalsze działania uzgodnij z IT lub bankiem.