

Pamiętaj!



4 zasady bezpiecznych zakupów w sieci

- ⚠️ **Strzeż danych, które należą tylko do Ciebie**
– nigdy nie przekazuj ani nie przesyłaj wszystkimi dostępnymi komunikatorami haseł dostępowych, numeru karty, numeru BLIK.
- ⚠️ **Nigdy nie podawaj swoich danych obcym**
– szczególnie tych dotyczących konta bankowego czy karty płatniczej.
- ⚠️ **Nie korzystaj z publicznych sieci Wi-Fi**, robiąc zakupy internetowe. To bardzo ryzykowne – ktoś może przechwycić Twoje dane!
- ⚠️ **Zawsze czytaj regulamin sklepu** i upewnij się, czy dane są przetwarzane tylko w celu realizacji zakupu.



Pamiętaj!



incydenty naruszające bezpieczeństwo w sieci zgłasza się do Cert Polska:



na stronie: **incydent.cert.pl**



podjęte SMSy: **pod numer 8080**



*Bądź mistrzem
cyberbezpiecznych
finansów.
Twoich finansów!*

EDUKACJA NBP
NBP.PL/EDUKACJA



NARODOWY
BANK POLSKI

BEZPIECZNE ZAKUPY
|
INTERNETOWE

Zabezpiecz
swoje
pieniądze

Sprawdź!

*Czy umiesz bezpiecznie
kupować w sieci?*



**Zakupy internetowe są wygodne,
ale rób je z głową. Zachowaj
czujność!**

Zakupy w sieci to czysta przyjemność: oferty można wygodnie przeglądać na smartfonie, dostępne są opinie, łatwo porównać ceny. No, a potem – tylko klik i zakupy zrobione. Ten „jeden klik” to marketingowa zachęta do internetowego świata zakupów... i jednocześnie za każdym razem sprawdzian, czy umiesz chronić swoje dane i pieniądze.

To musisz wiedzieć!

01 Nie daj się nabrać fałszywym reklamom



Zakupy często zaczynają się od kliknięcia w reklamę w mediach społecznościowych. Jednak wtedy można trafić na specjalnie spreparowane strony za pomocą fałszywych reklam. Złośliwe reklamy często używają wabika: „Niewiarygodna okazja!” lub „Ostatnia sztuka w magazynie!”. Takie reklamy nazywają się „malvertising”. Jest to połączenie angielskich słów: „malware” (wszelkiego rodzaju szkodliwe aplikacje) oraz „advertising” (reklama). Na złośliwych stronach hakerzy próbują nakłonić osoby do pobrania złośliwego oprogramowania zbierającego prywatne dane użytkownika. W otrzymanej wiadomości np. z okazijną ofertą – fałszywe strony zwykle różnią się od tych prawdziwych zaledwie jedną literą lub znakiem, trzeba być więc bardzo uważnym i unikać klikania w mało wiarygodne reklamy.

Malvertising – to złośliwa reklama wyłudzająca wrażliwe dane

02 Sprawdzaj, czy na pewno jesteś na stronie sklepu



W mediach społecznościowych reklamy posługują się często skróconym adresem strony. Po kliknięciu w reklamę należy sprawdzić, czy strona sklepu jest autentyczna. Adres internetowy należy uważnie weryfikować, ponieważ naciągacze mogą użyć alternatywnego alfabetu w celu ukrycia fałszywego adresu. Aby mieć pewność, czy korzystamy z właściwej strony, należy kliknąć w kłódkę znajdującą się w lewej części paska adresu, a następnie wybrać opcję: „Wyświetl certyfikat”, który pokazuje, czy certyfikat jest poprawny.

Adresy phishingowe – to adresy internetowe, których celem jest wyłudzenie poufnych danych

03 Nie otwieraj wiadomości e-mail od nieznanych nadawców



Nigdy nie wchodź w wiadomości e-mail, jeśli nadawca nie jest Ci znany. A co najważniejsze – nigdy nie otwieraj zawartych w nich załączników oraz nie klikaj w dołączone linki.

04 Zweryfikuj sklep internetowy



Sprawdź, czy na stronie sklepu są dane sprzedawcy i numer telefonu – obowiązkiem każdej firmy jest podanie takich informacji. Przed ewentualnym zawarciem umowy w sklepie internetowym, po otrzymaniu oferty pocztą tradycyjną lub elektroniczną, należy dokładnie zapoznać się z regulaminem portalu lub sklepu internetowego, a w nim z warunkami płatności, dostaw i zwrotów.

Program antywirusowy to absolutna konieczność – zainstaluj go na urządzeniach, na których robisz zakupy w sieci i regularnie aktualizuj

Chcesz płacić bezpiecznie w sieci? Na to uważaj!

- ⚠ Sklepy internetowe używają specjalnych stron do płatności za zakupy. Zanim wprowadzisz na stronie internetowej płatności jakiegokolwiek wrażliwe informacje, takie jak login czy hasło, **uważnie przyjrzyj się paskowi adresu sklepu**. Jeśli adres wzbudza podejrzenia (zawiera literówki, nie wygląda poprawnie lub zamiast liter użyto specjalnych symboli), nie wprowadzaj na takiej stronie żadnych danych!
- ⚠ Jeśli nie korzystałeś dotąd z aplikacji do płatności, którą proponuje sklep, **zobacz liczbę pobrań aplikacji** w sklepie z aplikacjami np. Google Play czy AppStore. Jeśli jest ich tylko kilkadziesiąt – raczej jest to oszustwo!
- ⚠ Omijaj transakcje, które wymagają wyłącznie płatności BLIKiem, **autentyczne sklepy dysponują wieloma opcjami płatności**.
- ⚠ Oszuści mogą podszywać się pod witryny banków lub popularnych portali aukcyjnych i społecznościowych. Dlatego korzystaj tylko ze stron internetowych zaufanych dostawców, na których najlepiej **wprowadź ręcznie adres strony w pasku adresowym przeglądarki**. Pamiętaj, aby w przypadku jakichkolwiek wątpliwości nie wpisywać swojego loginu oraz hasła!
- ⚠ Podczas zakupów, np. w portalach z używanymi rzeczami, korzystaj z takiego modelu płatności, który pozwoli Ci **dokonać płatności za ogłoszenie dopiero wtedy, gdy transakcja dojdzie do skutku** i przedmiot zostanie sprzedany. Kupujący wpłaca ustaloną zapłatę na konto portalu, gdy przedmiot jest dostarczony – a portal przekazuje płatność sprzedającemu. Uważaj też na zakupy na portalach aukcyjnych lub społecznościowych. Często metodą wyłudzenia środków jest sprzedaż fałszywych biletów na imprezę lub koncert.
- ⚠ Zawsze sprawdzaj SMSy typu: „BLIKnij kod, zabrakło mi 10 zł do zakupu”, dzwoniąc do znajomego czy kolegi, od którego otrzymałeś SMS. **Weryfikuj zawsze, czy wysłana prośba dotycząca płatności jest prawdziwa**.
- ⚠ Gdy kupujący przesyła Ci wiadomość: „Już zapłaciłem, kliknij w link, aby zaakceptować płatność. Brat podjedzie jutro po przesyłkę”, jest to niemal zawsze próba oszustwa!
- ⚠ Po zakończeniu zakupów i płatności, za każdym razem **wyloguj się z aplikacji sklepu, płatności czy portalu aukcyjnego**.