NARODOWY BANK POLSKI

Bezpieczeństwo płatności w sieci

Podstawowe zasady bezpieczeństwa w Internecie, których przestrzeganie uchroni nas przed stratami finansowymi:

- **Zawsze dokładnie sprawdzajmy pasek adresu otrzymanej wiadomości** – fałszywe strony zwykle różnią się od tych prawdziwych zaledwie jedną literą lub kilkoma znakami, trzeba być więc bardzo uważnym. Nigdy nie warto też ufać skróconym adresom, a po kliknięciu zawsze należy sprawdzać, czy trafiliśmy na właściwą stronę.
- Zanim wprowadzimy na stronie internetowej jakiekolwiek wrażliwe informacje, takie jak login czy hasło, **należy zawsze uważnie przyjrzeć się paskowi adresu**. Jeśli adres wzbudza podejrzenia (zawiera literówki, nie wygląda poprawnie lub zamiast liter używa specjalnych symboli), nie wprowadzajmy na takiej stronie żadnych danych.
- **Adres internetowy trzeba sprawdzać bardzo uważnie**, gdyż naciągacze uwielbiają używać alternatywnych alfabetów w celu ukrywania phishingowych adresów internetowych. 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" — dzięki temu dowiemy się, kto jest prawdziwym właścicielem strony.
- **Oszuści często podszywają się pod witryny banków lub popularnych portali aukcyjnych i społecznościowych**. Dlatego należy korzystać tylko ze stron internetowych zaufanych dostawców, najlepiej wprowadzając adres strony ręcznie w pasku adresu przeglądarki. Pamiętajmy, aby w przypadku jakichkolwiek wątpliwości nie wpisywać swojego loginu oraz hasła.
- Przed ewentualnym zawarciem umowy w sklepie internetowym, po otrzymaniu oferty pocztą tradycyjną lub elektroniczną, **należy dokładnie zapoznać się z regulaminem danego portalu**.
- **Nie należy klikać w linki otrzymane z nieznanych źródeł** (w e-mailach, komunikatorach i sieciach społecznościowych).
- **Nigdy nie należy otwierać wiadomości e-mail od nieznanych nadawców**, a co najważniejsze – nie należy otwierać zawartych w nich załączników.
- **Nie można przesyłać e-mailem ważnych informacji**, haseł dostępu ani numerów kart płatności.
- **Pilnujmy swoich haseł dostępowych** i pamiętajmy, aby wprowadzone hasła nie były możliwe do odszyfrowania przez osoby nieupoważnione. Dla bezpieczeństwa zmieniajmy je co kilka miesięcy.
- **Pamiętajmy o wylogowywaniu się z aplikacji** za każdym razem po zakończeniu ich użytkowania.
- **Nie należy podawać danych dotyczących kont bankowych** czy posiadanych kart płatniczych osobom postronnym.
- **Trzeba systematycznie uaktualniać system i oprogramowanie urządzeń**, z których korzystamy, stosować silne hasła oraz dobrej jakości programy antywirusowe i antyszpiegowskie. W szczególności warto używać narzędzi antywirusowych, które zapewnią ochronę przed spamem i phishingiem.
- **Unikajmy korzystania z publicznych sieci Wi-Fi**. Zachowajmy też ostrożność, gdy zamierzamy skorzystać z publicznie dostępnych komputerów.

Sprawdźmy ważność certyfikatu strony, klikając w ikonę kłódki znajdującej się po lewej stronie paska adresu. Zwróćmy uwagę, czy kłódka jest zamknięta, a pasek adresu witryny zawiera literkę „s" (https), co oznacza bezpieczne połączenie.

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

Dopiero wtedy, gdy jesteśmy pewni dobrych zamiarów firmy, możemy podjąć z nią współpracę. W przeciwnym wypadku możemy narazić się na nieprzyjemności.

Spam – niechciane lub niepotrzebne wiadomości elektroniczne, wysyłane zwykle masowo, za pośrednictwem poczty elektronicznej, w komunikatorach, a także SMS-ach.