



NARODOWY
BANK POLSKI

Światowy
Tydzień
Pieniądza

18-24
marca
2024

Zabezpiecz
swoje
pieniądze
i swoją
przyszłość



TWÓJ PLAN na bezpieczne finanse

Czy pieniądze są nastolatkowi niezbędne? Absolutnie tak!
Do kupna rzeczy, które lubi lub których po prostu potrzebuje. Do wspólnego spędzania czasu – w kawiarni, kinie, na koncercie. Do realizacji swojego hobby i swoich pasji. Do spełniania marzeń.

Portmonetka, portfel – to oczywiście wciąż jest potrzebne.
Ale płacić można też cyfrowo!



CYFROWE PIENIĄDZE to wygoda, ale też cyfrowe zagrożenia

Smartfon, zegarek, BLIK lub przelew w aplikacji. Przygotowaliśmy mapę, z którą łatwiej poruszać się po cyfrowych finansach i cyfrowych zagrożeniach. Zacznijmy od najważniejszego, od tego, że każdy nastolatek, słysząc o konieczności stosowania zasad „cyberhigieny”, powie: „Super, ale to nie o mnie” albo „Ja bym w życiu nie dał się na to nabrać”.

Właśnie na to liczą cyberoszuści – na nieostrożność i nierozwagę.

CO TRZEBA WIEDZIEĆ?

01



Najważniejsze jest zabezpieczenie cyfrowego portfela

czyli **smartfona, laptopa i tabletu**, a także aplikacji znajdujących się na tych urządzeniach. Przede wszystkim pamiętaj, by ustawiać trudne hasło. Łatwe hasło można złamać w 3 sekundy. Dostęp do źle zabezpieczonego smartfona może pozwolić hakerowi ukraść Twoje dane osobiste, umożliwić dostęp do aplikacji bankowej lub innej, zawierającej cenne dane, a nawet zainstalować w smartfonie „kryptogórnika” – cyfrowego agenta działającego na giełdzie kryptowalut.
Unikaj stosowania funkcji „zapamiętaj hasło” w przeglądarce internetowej – to nie jest bezpieczna metoda. Używaj przeznaczonych do tego celu niezależnych aplikacji (managerów haseł), stosujących silne algorytmy szyfrowania.

Pamiętaj

o używaniu oprogramowania antywirusowego i częstych aktualizacjach. Każda zainstalowana aplikacja i przeglądarka musi być na bieżąco aktualizowana – to chroni ją przed lukami w oprogramowaniu.



Nie korzystaj z oprogramowania służącego do „rootowania” telefonu, które omija zabezpieczenia stosowane przez producenta urządzenia. To działanie spowoduje wyłączenie ważnych mechanizmów kontroli i doprowadzi do utraty gwarancji producenta. Bez fabrycznych zabezpieczeń sprzęt jest pozbawiony właściwej ochrony, jest też zaproszeniem do ataku cyberprzestępców.

Na co dzień unikaj korzystania z darmowych punktów ładowania poprzez USB w publicznych miejscach (kawiarnie, galerie handlowe, lotniska). Przestępcy wykorzystują publiczne porty USB do wprowadzenia na urządzenia złośliwego oprogramowania. Korzystaj z własnej ładowarki i przewodu USB.



NARODOWY
BANK POLSKI

Światowy
Tydzień
Pieniądza

18-24
marca
2024

Zabezpiecz
swoje
pieniądze
i swoją
przyszłość

GLOBAL
MONEY
WEEK

02



Stosuj zasadę ograniczonego zaufania

Ta zasada dotyczy całej sfery cyfrowej. W języku angielskim smartfony i tablety oznacza się skrótem PD – Personal Device. Personal (osobisty) jest czymś, co należy tylko do Ciebie. **Nie ujawniaj nikomu swoich danych dostępowych** (loginów, haseł, nazw użytkownika, symboli i kodów odblokowania). **Nie przekazuj również numerów karty płatniczej.**

Pamiętaj!

Bank, platformy handlowe (Allegro, OLX, Vinted itp.) **NIGDY nie żądają haseł!** Jeśli widzisz połączenie telefoniczne lub głosowe (na WhatsApp, Messenger) przychodzące z „egzotycznego” numeru – zignoruj je, to są częste metody na wyłudzenie danych lub kradzież pieniędzy z konta bankowego.

03



Udane internetowe zakupy to przede wszystkim bezpieczne zakupy

Przed potwierdzeniem transakcji BLIK zawsze sprawdź dwa razy, ile wynosi kwota, i czy trafia do właściwego odbiorcy. Podczas zakupów internetowych odwiedzaj tylko bezpieczne strony. Bezpieczna strona to taka, która przed adresem wyświetla ikonkę „kłódki”, a jej adres zaczyna się od **https://**. Sprawdź, czy w adresie strony nie ma błędu lub literówki. Zweryfikuj stronę, wyszukując ją niezależnie w wyszukiwarce.

Nie klikaj w wyskakujące ekrany (pop up). Takie reklamy mogą zawierać wirusy lub złośliwe oprogramowanie, wykradające dane. To zjawisko nosi nazwę *malvertising*. Polega na umieszczeniu szkodliwego kodu w reklamach wyświetlanych na popularnych stronach internetowych. Portale korzystają z automatycznych systemów reklamowych, i nie zawsze są w stanie wyeliminować podejrzane reklamy.

04



W cyfrowym świecie trudniej odróżnić prawdziwe intencje osoby, będącej po drugiej stronie monitora

Pewnie słyszałeś już gdzieś słowa takie jak *phishing* (np. fałszywy link w mailu), *smishing* (SMS z nieuczciwym żądaniem lub przynagleniem do zapłaty, np. za paczkę) i *vishing* (głosowe, telefoniczne podszywanie się pod instytucję publiczną lub osobę, którą znasz). Gdy dostaniesz nietypowy telefon, maila lub smsa – **sprawdź wiarygodność przekazanej informacji, skontaktuj się z zaufaną osobą.**

Przestępcy mogą sfalszować nadawcę w wiadomościach SMS, lub w polu adresu mailowego, by w nieuczciwy sposób pozyskać Twoje dane lub wyłudzić od Ciebie pieniądze. Takie ataki noszą nazwę *spoofingu*, i są podobne do ataków phishingowych, dlatego najlepszą ochroną jest zachowanie dystansu i spokojna weryfikacja rozmówcy.



NARODOWY
BANK POLSKI

Światowy
Tydzień
Pieniądza

**18-24
marca
2024**

*Zabezpiecz
swoje
pieniądze
i swoją
przyszłość*

**GLOBAL
MONEY
WEEK**



Twoje dane osobowe – imię, nazwisko, adres mailowy, numer telefonu, cookies (ciasteczka), mają wartość pieniężną

Twoje dane osobowe, pozyskane przez portale i strony internetowe mogą być wykorzystane w różny sposób. Często są przedmiotem transakcji handlowych z agencjami reklamowymi. Dane służą następnie do profilowania reklam i treści. Dlatego należy je odpowiednio cenić i chronić.

JAK CHRONIĆ DANE?

- Weryfikuj ustawienia prywatności w profilach mediów społecznościowych.
- Naucz się rozpoznawać sposoby wpływu i manipulacji w przestrzeni internetowej.
- Kontroluj własne emocje: strach lub pośpiech. Łatwiej wtedy podejmować błędne decyzje.



PAMIĘTAJ!

incydenty naruszające bezpieczeństwo w sieci zgłasza się do Cert Polska:



SMsem: **na numer 8080**



Mailem: **incydent.cert.pl**



*Bądź mistrzem
cyberbezpiecznych
finansów.*

Twoich finansów!