**Bezpieczni nie tylko w Święta**

**Rozpoczął się okres przedświątecznej gorączki, świadczą o tym nie tylko ozdobione witryny sklepowe, piosenki świąteczne i wszechobecne promocje, ale także wzmożona aktywność oszustów. Aby się im nie dać, warto zachować zdrowy rozsądek wydając pieniądze w sposób odpowiedzialny i dbając o bezpieczeństwo zakupów, przypomina ZBP.**

Przedświąteczne zamieszanie to raj dla cyberprzestępców i oszustów internetowych, ponieważ w ferworze zakupów łatwo stracić czujność i narazić się na utratę pieniędzy. W samym III kwartale 2022 r. odnotowano 2.089 prób wyłudzeń na łączną kwotę 47,7 mln zł.

Warto więc stosować kilka zasad, które zwiększą bezpieczeństwo zakupów - jest ich mniej niż potraw, które tradycyjnie powinny znaleźć się na wigilijnym stole.

**1. Bezpiecznie korzystaj**

Wypłacając pieniądze stań blisko maszyny i zasłoń swoim ciałem ekran i klawisze. Dobrym nawykiem jest też zasłanianie klawiatury ręką. Jeszcze przed włożeniem karty do bankomatu sprawdź, czy wejście na kartę nie posiada żadnych dodatkowych nakładek w postaci np. doklejonej nietypowej listwy z nawierconymi małymi otworami, elementów działających jak magnes, elementów, które można oderwać czy odkleić itp.

Zwróć również uwagę na klawiaturę - nie powinna być wypukła ani zniekształcona. Jeśli wygląd lub funkcjonowanie bankomatu wzbudzi Twoje podejrzenia, nie wykonuj transakcji.

**2. Instaluj programy ze sprawdzonych źródeł**

Szczególnie narażone są osoby, które pobierają aplikacje z nieoficjalnych sklepów i pozwalają im na niczym nieuzasadnione nadawanie uprawnień dostępowych do zawartości urządzenia. Zagrożenie stanowić mogą też phishingowe (czyli wyłudzające dane) e-maile oraz wyskakujące reklamy z atrakcyjnymi, świątecznymi promocjami na stronach, w które możesz kliknąć nawet przez przypadek. Aplikacja antywirusowa może pomóc wykryć fałszywe aplikacje i próby wyłudzeń danych. Pomoże także gdy telefon zostanie zgubiony lub skradziony wiele antywirusów pozwala na zdalne usuwanie danych.

**3. Pomyśl zanim klikniesz**

Większość ataków polega na wykorzystaniu ludzkiej naiwności. Przestępcy tworzą komunikat motywujący odbiorcę do tego, żeby wykonał szybko jakieś działanie. Nikt nie chce stracić dostępu do maili albo mieć zablokowanego konta bankowego, dlatego klikamy w podany link, żeby uchronić się przed taką sytuacją.

Nie powinniśmy tego robić! Banki nigdy nie komunikują się z klientami w tych sprawach w taki sposób. Jak można uchronić się przed takimi kłopotami? Najlepsza rada brzmi: daj sobie czas i nie klikaj od razu w link. Pomyśl, zadzwoń do instytucji lub osoby, od której potencjalnie otrzymałeś e-mail lub SMS-a, z pytaniem czy rzeczywiście chcą żebyś wykonał nietypowe działania.

**4. Chroń swoją tożsamość**

Powinniśmy mieć świadomość, że nie tylko zagubienie dowodu tożsamości, ale również jego czasowa strata może przyczynić się do naszych problemów w przyszłości. Nie należy więc pozostawiać dokumentów bez opieki, czy też jako zastaw np. w wypożyczalni. Przestępcy posiadający nasze dane osobowe mogą przykładowo wyłudzić kredyt na nasze nazwisko, czy też wziąć tzw. chwilówkę w firmie pożyczkowej. Mogą także na nasze nazwisko wypożyczyć i sprzedać samochód lub podpisać kilka umów z operatorem telekomunikacyjnym, dostając w zamian markowe telefony komórkowe.

Problemy związane z wykorzystaniem naszej tożsamości mogą do nas dotrzeć po kilku miesiącach lub nawet latach. Bardzo ważną czynnością po utracie dokumentu tożsamości jest jego zastrzeżenie.

**Gdy zastrzegasz dowód, zgłaszasz go do Systemu DOKUMENTY ZASTRZEŻONE. W kilka minut informacja dotrze do wszystkich banków w Polsce, Poczty Polskiej oraz operatorów telefonii komórkowej. Twoja tożsamość jest bezpieczna i nikt nie będzie mógł już potwierdzić tożsamości na podstawie Twojego dokumentu.**

**5. Zabezpiecz kod PIN**

PIN do karty bankowej nie powinien być nigdzie zapisywany, zwłaszcza na karcie, w portfelu, ani w telefonie. Ułóż PIN, który nie będzie oczywisty (jak data Twoich urodzin czy ciąg takich samych cyfr). Nigdy nie podawaj nikomu swojego PIN-u, ani nie pożyczaj karty. Pamiętaj o zmianie PIN-u co jakiś czas, np. raz na pół roku.
Aby zwiększyć swoje bezpieczeństwo sprawdzaj także wyciąg z konta. W przypadku podejrzanych transakcji zgłoś problem swojemu bankowi.

**6. Straciłeś kartę? Nie ryzykuj**

Co roku Polacy tracą ponad milion kart płatniczych. Głównie dlatego, że je gubią, ale czasem padają także ofiarą kradzieży. Jeżeli Cię to spotka, skorzystaj z wygodnego systemu do zastrzegania kart bankomatowych. Zadzwoń na numer **(+48) 828 828 828**, wypowiedz nazwę banku, a system połączy Cię z jego infolinią. Następnie odpowiedz na kilka pytań weryfikujących i bezpłatnie zastrzeż swoją kartę.

**7. Aktualizuj system i aplikacje**

Aktualizacje systemu operacyjnego oraz kluczowych aplikacji oprócz nowych funkcji i możliwości, zawierają w sobie wiele dodatków poprawiających bezpieczeństwo naszych danych oraz wirtualnego portfela. Warto również rozdzielić kanały komunikacyjne tak, by autoryzujące wiadomości np. SMS przychodziły na inne urządzenie, niż to przez które logujemy się do banku.

**8. Zabezpiecz dostęp**

Tak jak nie zostawiasz otwartych drzwi do domu, tak nie zostawiaj otwartego dostępu do swojego telefonu czy laptopa. W czasach weryfikacji odciskiem palca, twarzą czy kilkucyfrowym kodem nie warto podawać swoich danych na tacy. Stosuj zabezpieczenia jakie umożliwia Ci Twoje urządzenie.

Źródło: Związek Banków Polskich/ZBP

BANKOWCY DLA EDUKACJI
program sektorowy

*Program sektorowy „Bankowcy dla Edukacji" to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.*

*Zapraszamy na stronę **www.bde.wib.org.pl***