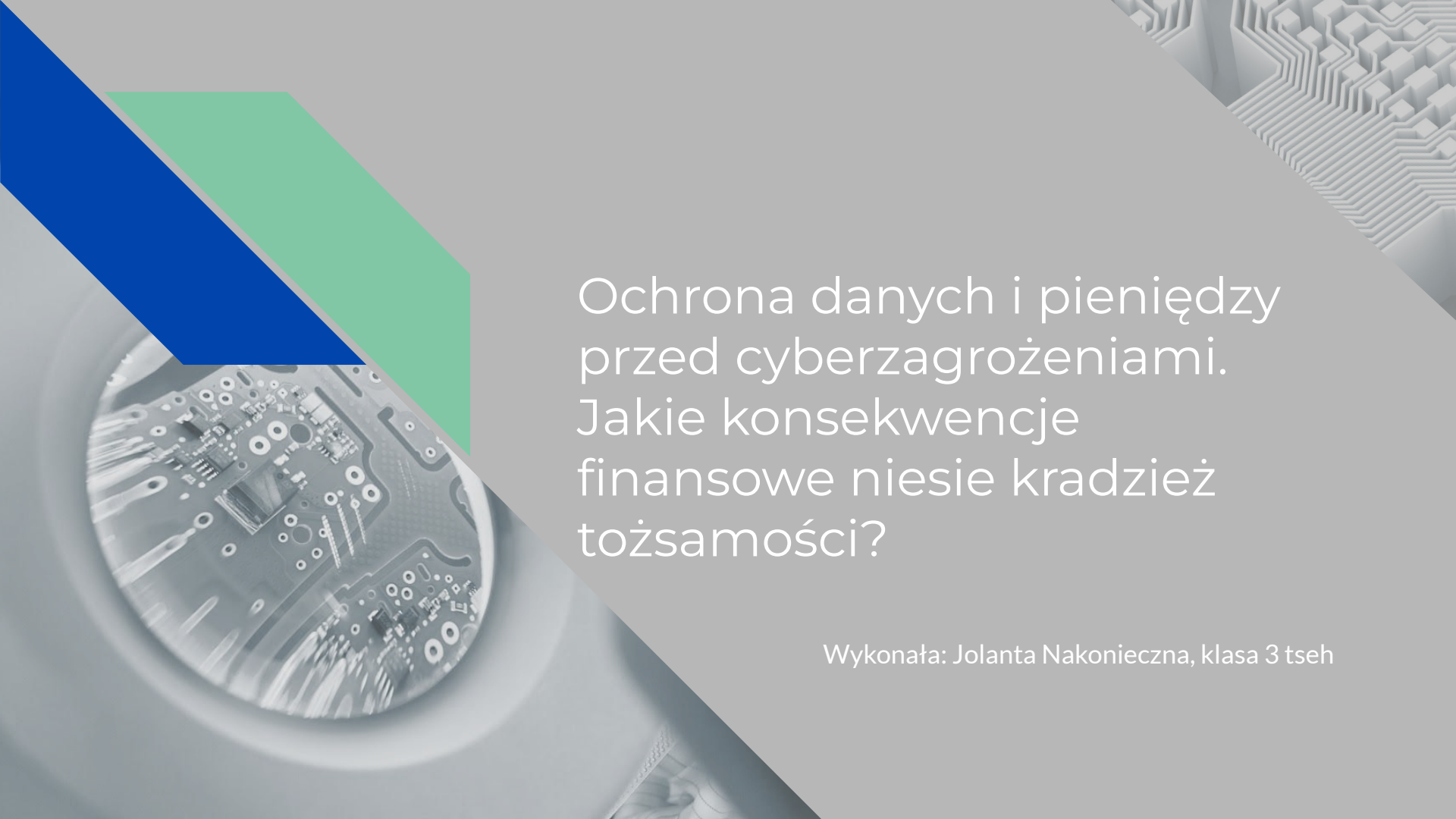


Ochrona danych i pieniędzy przed cyberzagrożeniami. Jakie konsekwencje finansowe niesie kradzież tożsamości?

Wykonała: Jolanta Nakonieczna, klasa 3 tseh

Czym są cyberataki?

Cyberatakami nazywamy przestępstwa przy wykorzystaniu systemów komputerowych i sieci informatycznych lub przy użyciu złośliwego oprogramowania. Ich celem jest przechwycenie danych lub informacji, które umożliwią kradzież, oszustwo czy szantaż.

Najczęstszymi konsekwencjami cyberataków są:

1. utrata środków na koncie osoby lub instytucji, której dane zostały wykradzione, a w konsekwencji nawet bankructwo osoby lub przedsiębiorstwa dotkniętego cyberatakiem

2. utrata reputacji osoby, wiarygodności marki w przypadku firmy

3. utrata własności intelektualnej

Najpopularniejsze rodzaje cyberataków

Do kradzieży tożsamości dochodzi najczęściej, gdy:

• niedostatecznie chronimy własne dane w sieci, np. ustawiamy słabe, zbyt krótkie hasła, powielamy to samo hasło na różnych stronach, udostępniamy dane bez przeczytania polityki prywatności oraz warunków przetwarzania danych osobowych;

• gubimy i nie zastrzegamy utraconych dokumentów, takich jak dowód osobisty czy prawo jazdy;

• padniemy ofiarą oszustwa pod nazwą **phishing;**

• nieświadomie użyjemy złośliwego oprogramowania- **malware;**

• dane z naszej karty płatniczej zostaną nielegalnie skopiowane (**skimming**) lub pozyskane w trakcie rozmowy telefonicznej (**vishing**);

• damy się naciągnąć na **smishing** – wiadomości SMS, które nakłaniają do wykonania konkretnych czynności (umożliwiających kradzież danych).

Czym jest phishing i jak się przed nim bronić?

Pierwszym krokiem może być masowe rozesłanie specjalnej wiadomości, która wygląda prawie jak e-mail z naszego banku. Informacje w niej zawarte mają nas skłonić do określonej czynności, najczęściej do niezwłocznego kliknięcia w podany link lub pobrania załącznika. Link zazwyczaj prowadzi nas do strony, która łudząco przypomina stronę logowania naszego banku.

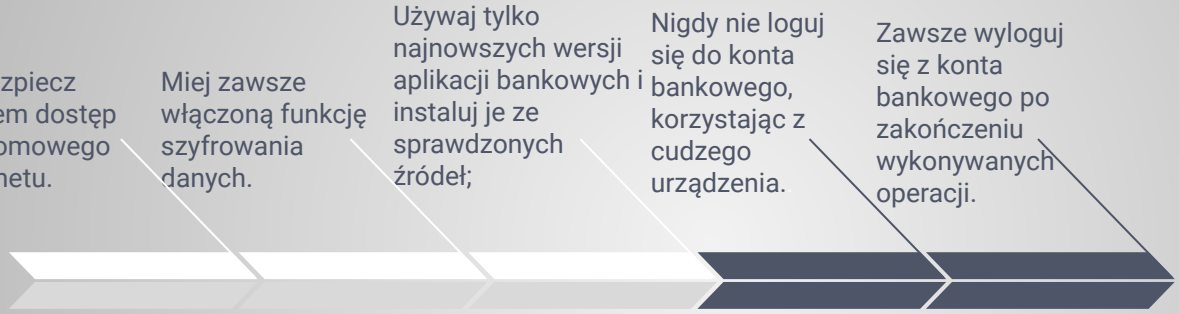
Jeżeli otrzymamy wiadomość przypominającą informację wysłaną przez instytucję finansową, w pierwszej kolejności sprawdźmy, z jakiego adresu e-mail został wysłany. Zwróćmy uwagę na elementy personalizujące e-mail – podejrzane mogą być sformułowania wskazujące na korespondencję masową w rodzaju: „Szanowny Kliencie” zamiast bezpośredniego skierowania wiadomości do nas.

Ochrona przed złośliwym oprogramowaniem

Złośliwe oprogramowanie (malware) jest narzędziem do przejmowania kontroli nad urządzeniem elektronicznym umożliwiającym dostęp do danych na nim zapisanych, takich jak login i hasło do bankowości elektronicznej. Aby chronić się przed złośliwym oprogramowaniem, należy zainstalować zarówno na komputerze, jak i w telefonie komórkowym program antywirusowy od autoryzowanego dostawcy. Ważne, aby program ten był aktualizowany tak często, jak jest to wymagane.

Szczególnie niebezpieczne jest logowanie się do konta lub do aplikacji w miejscu publicznym (np. w szkole czy kawiarni) – przy użyciu publicznej sieci Wi-Fi.

Zapamiętaj zasady bezpiecznego korzystania z internetu



Zabezpiecz hasłem dostęp do domowego internetu.

Stosuj uwierzytelnienie dwuetapowe wszędzie, gdzie to możliwe.

Miej zawsze włączoną funkcję szyfrowania danych.

Utwórz kopię bezpieczeństwa danych, których nie chcesz utracić bezpowrotnie.

Używaj tylko najnowszych wersji aplikacji bankowych i instaluj je ze sprawdzonych źródeł;

Przy instalowaniu aplikacji za pośrednictwem sklepu, zawsze sprawdź, czy to Twój bank jest jej producentem.

Nigdy nie loguj się do konta bankowego, korzystając z cudzego urządzenia.

W komputerze czy telefonie włącz funkcję, która uniemożliwia instalowanie oprogramowania z nieznanych źródeł.

Zawsze wyloguj się z konta bankowego po zakończeniu wykonywanych operacji.

Bądź wyczulony na wiadomości z propozycją aktualizacji systemu operacyjnego, upewnij się, że informacja pochodzi od Twojego operatora.

Bezpieczny w internecie

Bezpieczne używanie karty płatniczej

Użytkownicy kart płatniczych są narażeni na przestępstwo zwane skimmingiem, które polega na kopiowaniu danych z paska magnetycznego karty płatniczej. Kopiowanie danych z paska magnetycznego jest możliwe, gdy w bankomacie zostaje zainstalowany tzw. skimmer (nakładka na slot do wkładania karty do bankomatu) – urządzenie, które służy do sczytywania danych z karty.

Przed włożeniem karty do bankomatu trzeba upewnić się, że wygląd klawiatury czy ekranu nie budzi podejrzeń. Jeżeli widzimy na urządzeniu element, który wydaje się obcy, zrezygnujmy z transakcji i skontaktujmy się ze swoim bankiem. Nasze podejrzenia może budzić m.in. nietypowy kształt klawiatury (np. nadmiernie wypukła), nienaturalnie wystające części, nakładki niepołączone z bankomatem czy obecność dodatkowych wkładek w szczelinie na kartę – wlot na kartę musi być pusty. Ważnym zabezpieczeniem (szczególnie gdy przestępcy udało się zrobić duplikat naszej karty) jest posiadanie dziennego limitu transakcji bezgotówkowych

Zintegrowany System Zastrzegania Kart pozwala na szybkie zastrzeżenie karty płatniczej, nawet jeżeli nie znamy numeru telefonu do infolinii naszego banku. Możemy to zrobić pod numerem telefonu:

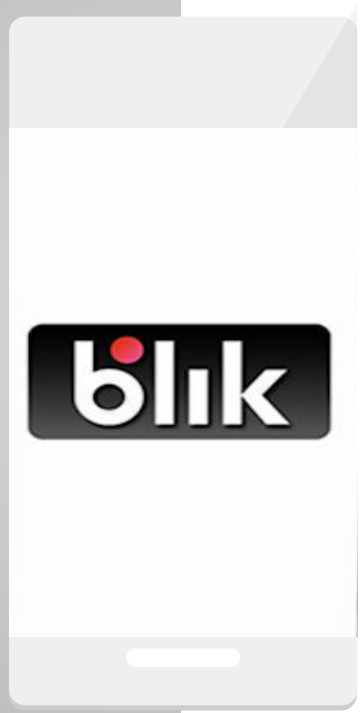
828 828 828

lub pod adresem: **zastrzegam.pl**

Jak korzystać z aplikacji mobilnych, płacić bezpiecznie telefonem oraz używać kodu BLIK?

Z pomocą aplikacji mobilnej można obecnie wykonać niemal wszystkie operacje bankowe – dokonywać przelewów, otworzyć lokatę lub konto oszczędnościowe, złożyć wniosek o pożyczkę czy zastrzec kartę. Aplikacje bankowe są tworzone przez specjalistów, którzy dużą wagę przykładają do bezpieczeństwa.

Za pomocą kodu BLIK można płacić za zakupy w sklepach stacjonarnych i internetowych, wypłacać gotówkę z bankomatu oraz przesyłać pieniądze na telefon innej osoby, nawet jeżeli nie pamięta ona swojego numeru konta (wystarczy do tego jego numer telefonu). Kod BLIK pozwala uniknąć logowania się do konta podczas płatności w internecie. W zamian generujemy w swojej aplikacji bankowej 6-cyfrowy kod BLIK ważny przez 2 minuty, który trzeba wpisać podczas dokonywania transakcji, a następnie potwierdza się ją w aplikacji.



Pierwszą zasadą jest instalowanie aplikacji z pewnego źródła.

Zapewnijmy, by telefon, na którym korzystamy z aplikacji bankowej był zabezpieczony oprogramowaniem antywirusowym.

Nie pożyczaj telefonu innym i nie pozostawiaj go bez kontroli. Nigdy nie loguj się do aplikacji z obcego smartfona. Dostęp do telefonu zawsze zabezpieczaj kodem PIN lub biometrycznie (np. odciskiem palca); zrezygnuj z odblokowywania telefonu za pomocą gestu lub rysowanego symbolu – te łatwo podejrzeć i skopiować.

Kodeks cyberbezpieczeństwa na podsumowanie

1. Zabezpiecz telefon i komputer oprogramowaniem antywirusowym. Aktualizuj oprogramowanie tak często, jak jest to wymagane.

2. Ustawiaj silne hasła – im dłuższe tym lepsze. Zmieniaj hasła co jakiś czas. Pamiętaj, aby hasło zawierało kombinację małych i wielkich liter, cyfr i znaków specjalnych.

3. Nigdy nie używaj tego samego hasła do logowania w dwóch różnych miejscach, szczególnie jeśli dane hasło zabezpiecza konto lub aplikację bankową.

4. Przed rozpoczęciem logowania sprawdź połączenie z bankiem: czy adres strony rozpoczyna się od protokołu „https:// („s” na końcu od ang. secure oznacza bezpieczne połączenie) i czy jest widoczna ikonka kłódki – to oznacza, że dane są zaszyfrowane. Kliknij w kłódkę i zweryfikuj datę ważności certyfikatu i do kogo należy.

5. Nie loguj się do bankowości elektronicznej, korzystając z ogólnodostępnej sieci Wi-Fi, np. udostępnionych w restauracjach, hotelach, etc.

6. Nigdy nie loguj się do bankowości z cudzych urządzeń.

7. Zawsze wpisuj adres strony banku bezpośrednio w przeglądarce internetowej.

8. Nigdy nie wchodź na stronę banku z użyciem linków otrzymanych mailem. Uważaj na linki w wiadomościach e-mail i SMS. Banki nigdy nie wysyłają próśb o login czy hasło.

9. Zawsze sprawdzaj podsumowanie transakcji przed jej zatwierdzeniem w aplikacji bankowej. Pamiętaj o weryfikacji numeru konta i kwoty do przelewu.

10. Czytaj komunikaty wysyłane przez bank w bankowości elektronicznej lub na stronie internetowej banku. Staraj się być na bieżąco z informacjami o nowych zagrożeniach.

11. Nie udostępniaj nikomu karty płatniczej oraz numeru PIN do niej. Nie umieszczaj numeru PIN w łatwo dostępnych miejscach.

12. Obejrzyj bankomat przed włożeniem do niego karty – jeśli coś zaniepokoi cię w jego wyglądzie, zrezygnuj z zaplanowanej czynności i skontaktuj się z operatorem bankomatu lub swoim bankiem.

13. Zasłaniaj kod PIN przy jego wpisywaniu podczas korzystania z bankomatu, w aplikacji bankowej oraz podczas dokonywania transakcji w sklepach.

Dziękuję za uwagę!