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

Wyjaśniamy

Rozwój technologii powoduje, że systemy zabezpieczające są coraz bardziej zaawansowane, jednak oszuści nieustannie szukają sposobów na przejęcie naszych danych i pieniędzy przy użyciu komputera, telefonu czy bankomatu. Musimy być świadomi, że w każdej chwili możemy stać się ofiarą cyberataku. Z danych pochodzących od agentów rozliczeniowych i banków wynika, że w I kwartale 2021 r. odnotowano ok. 61,2 tys. operacji oszukańczych na kwotę 19,2 mln zł (źródło: raport NBP: „Informacja o transakcjach oszukańczych dokonywanych przy użyciu bezgotówkowych instrumentów płatniczych w I kwartale 2021 r.").

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:

Na dyskusję o bezpieczeństwie w sieci można przeznaczyć lekcję informatyki.

- utrata środków na koncie osoby lub instytucji, której dane zostały wykradzione, a w konsekwencji nawet bankructwo osoby lub przedsiębiorstwa dotkniętego cyberatakiem,
- utrata reputacji osoby, wiarygodności marki w przypadku firmy,
- utrata własności intelektualnej.

Najpopularniejsze rodzaje cyberataków

Do najpopularniejszych cyberprzestępstw zaliczamy kradzież tożsamości. Jest to bezprawne wejście w posiadanie danych osoby lub instytucji i wykorzystanie ich bez wiedzy i woli właściciela. Najczęściej przestępca podszywa się pod inną osobę, używając wykradzionych danych lub wizerunku ofiary, zazwyczaj w celu osiągnięcia korzyści majątkowej. Przykładem tego przestępstwa jest np. przejęcie dostępu do konta społecznościowego czy skrzynki e-mail. Przy użyciu skradzionych danych przestępca może zaciągnąć kredyt czy założyć konto bankowe. Przestępca może również na nasz koszt zrobić zakupy w sklepie internetowym.

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* – przestępca podszywa się np. pod bank i kradnie dane dające mu dostęp do zasobów pieniężnych ofiary;
- nieświadomie użyjemy złośliwego oprogramowania (*malware*) na komputerach lub telefoniach zainfekowanych np. wiadomością e-mail z linkiem, którego kliknięcie umożliwia przejęcie kontroli nad urządzeniem;
- 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).

Ochrona danych poprzez bezpieczne logowanie się do konta

Najpopularniejszymi okolicznościami „hakowania" kont w internecie są:

1. dostęp do konta po odgadnięciu prostych haseł bądź związanych z danymi osoby, do której konto należy;
2. po złamaniu hasła używanego w serwisach, do których już wcześniej udało się włamać;
3. po przejęciu lub wyłudzeniu hasła.

Do cyberataku i kradzieży danych może dojść wtedy, gdy nie potrafimy lub nie przykładamy dużej wagi do ochrony informacji o nas, co jest szczególnie ważne przy korzystaniu z bankowości elektronicznej. Banki są zobowiązane do dbania o bezpieczeństwo swoich klientów i dokładają starań, by logowanie do bankowości elektronicznej było bezpieczne. Oferują różne metody logowania: z użyciem aplikacji za pomocą loginu i kodu PIN oraz poprzez stronę internetową banku również z użyciem loginu i hasła czy weryfikację kodem SMS. Banki publikują na swoich stronach komunikaty bezpieczeństwa z ostrzeżeniami przed najnowszymi zagrożeniami, opisując oszustwa, na które możemy być narażeni.

Stosowane przez banki zabezpieczenia nie zwalniają nas z troski o ochronę naszego konta. To my jesteśmy odpowiedzialni za wymyślenie odpowiednio skomplikowanego hasła zabezpieczającego dostęp np. do konta bankowego.

Silne hasło powinno zawierać kombinację dużych i małych liter, cyfr oraz znaków specjalnych. Serwis internetowy banku nie zaakceptuje hasła niespełniającego wszystkich wymaganych zabezpieczeń. Nie wolno używać w hasłach oczywistych sformułowań (np. „hasło", „qwerty" lub „123456"), słów mających silne powiązania z nami (np. imię i nazwisko, data urodzenia). Stanowczo nie powinniśmy używać tych samych haseł w różnych miejscach. Warto przyswoić zasadę – im dłuższe hasło, tym trudniej je złamać. Długie hasła mogą być trudne do zapamiętania, dlatego warto rozważyć korzystanie z managera haseł. Manager haseł jest aplikacją, która generuje za nas unikalne hasła i przechowuje je w stworzonej do tego celu bazie danych (elektronicznym sejfie). Korzystając z takiego managera, pozostają nam do zapamiętania dwa hasła: do komputera i właśnie do managera haseł.

Oprócz hasła dodatkowym zabezpieczeniem jest uwierzytelnianie wieloskładnikowe (najczęściej dwuskładnikowe). Wymóg takiego uwierzytelniania przy logowaniu do bankowości elektronicznej wprowadziła dyrektywa PSD2 (dyrektywa Parlamentu Europejskiego i Rady UE dotycząca usług płatniczych). Co oznacza uwierzytelnienie wieloskładnikowe? Do zalogowania na konto potrzebna jest znajomość hasła oraz potwierdzenie tożsamości np. poprzez wpisanie kodu weryfikacyjnego wysłanego SMS-em. Nawet jeśli przestępca przechwyci hasło do logowania, może nie będzie w stanie potwierdzić tożsamości w drugim etapie logowania.

Czym jest *phishing* i jak się przed nim bronić?

Phishing to metoda kradzieży przy użyciu internetu. Oszuści podszywają się pod instytucje lub osoby w celu wyłudzenia danych umożliwiających im dokonanie kradzieży. 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. Oszust może wykorzystać logo banku, a link do strony może łudząco przypominać adres instytucji, pod którą podszywa się przestępca. Sama wiadomość też może wyglądać bardzo podobnie jak znana nam strona banku – ta sama czcionka, motywy graficzne, kolory. Każde z tych działań ma osłabić naszą czujność i przekonać, że chodzi o rutynowe przekazanie danych np. takich, jakie podajemy zawsze przy logowaniu. Te działania prowadzą do zainstalowania wirusa na komputerze lub telefonie, na którym kliknęliśmy w zainfekowany link i w efekcie do kradzieży danych dających przestępcy dostęp do konta bankowego.

Jak bronić się przed *phishingiem*? Jeżeli otrzymamy wiadomość przypominającą informację wysłaną przez instytucję finansową, w pierwszej kolejności sprawdźmy, z jakiego adresu e-mail został wysłany. Jeżeli adres e-mail założono w ogólnodostępnej domenie, w której każdy z nas może mieć skrzynkę pocztową, to sygnał, że nie jest to wiadomość z banku. 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. Banki nigdy nie wysyłają wiadomości e-mail ani SMS oraz nie dzwonią do nas z prośbą o podanie haseł czy danych poufnych tj. numeru karty czy numeru CVV/CVC (trzycyfrowy numer na odwrocie karty służy do potwierdzania płatności online, gdy podajemy numer karty). Nie wysyłają też próśb o kliknięcie w podany link w celu natychmiastowego zalogowania się do konta. Banki nie zmieniają sposobu logowania do konta bez wcześniejszego uprzedzenia o tym klientów.

Słowo *phishing* to skrót od: *password harvesting fishing*, czyli łowienie haseł. Słowo ma kojarzyć się z angielskim słowem *fishing*. Przestępcy stosujący metodę *phishingu* zachowują się podobnie jak wędkarze – rzucają przynętę, na którą mamy się złapać.

Rodzajem phishingu z użyciem wiadomości SMS jest smishing. W tym przypadku dostajemy SMS-a rzekomo np. z banku, wiadomość zachęca nas do czynności, która później umożliwi przestępcy dostęp do naszego konta lub karty. Inną metodą jest wyłudzanie danych podczas rozmowy telefonicznej (tzw. vishing). Oszust, udając pracownika banku, próbuje namówić nas na podanie np. loginu i hasła do bankowości internetowej lub oferuje telefonicznie lokatę lub pożyczkę i przy tej okazji zdobywa poufne dane umożliwiające dokonanie kradzieży.

To, co koniecznie powinniśmy zrobić w przypadku otrzymania podejrzanej wiadomości lub telefonu, to sprawdzenie na stronie internetowej

banku, czy nie opublikowano tam ostrzeżeń dotyczących podobnych ataków. Jeżeli ostrzeżenia nie ma, powinniśmy zadzwonić na infolinię banku. Pracownik banku może potwierdzić, czy wiadomość pochodzi z ich domeny, a zgłoszone zdarzenie przeanalizują eksperci. Jeśli był to atak i mógł dotyczyć większej liczby klientów, wtedy bank podejmie dodatkowe działania chroniące klientów.

Jeżeli natomiast nie zauważyliśmy niczego podejrzanego w wiadomości, która była fałszywa, i zorientowaliśmy się, że oszust wyłudził od nas dane w pierwszej kolejności powinniśmy natychmiast zmienić hasła dostępu. Jeżeli podobnych haseł używaliśmy w innych miejscach, należy je zmienić na nowe, bezpieczne. Jeżeli natomiast podaliśmy dane do logowania do bankowości elektronicznej lub klikając w podsunięty link, wykonaliśmy przelew, musimy niezwłocznie skontaktować się z bankiem. Bank może zablokować np. wychodzący przelew, zmienić dane logowania czy powiadomić policję.

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. Podczas korzystania z sieci publicznej nie wiemy, w jaki sposób jest ona chroniona oraz kto z niej korzysta równocześnie z nami.

Zapamiętaj! 11 zasad bezpiecznego korzystania z internetu

1. Zabezpiecz hasłem dostęp do domowego internetu.
2. Stosuj uwierzytelnienie dwuetapowe wszędzie, gdzie to możliwe.
3. Miej zawsze włączoną funkcję szyfrowania danych.
4. Utwórz kopię bezpieczeństwa danych, których nie chcesz utracić bezpowrotnie.
5. Używaj tylko najnowszych wersji aplikacji bankowych i instaluj je ze sprawdzonych źródeł.
6. Przy instalowaniu aplikacji za pośrednictwem sklepu, zawsze sprawdź, czy to Twój bank jest jej producentem.
7. W komputerze czy telefonie włącz funkcję, która uniemożliwia instalowanie oprogramowania z nieznanych źródeł.
8. Nigdy nie loguj się do konta bankowego, korzystając z cudzego urządzenia.
9. Zawsze wyloguj się z konta bankowego po zakończeniu wykonywanych operacji.
10. Bądź wyczulony na wiadomości z propozycją aktualizacji systemu operacyjnego, upewnij się, że informacja pochodzi od Twojego operatora. Jeśli masz wątpliwości, skontaktuj się ze sprzedawcą oprogramowania i sprawdź, czy nie jest to próba wyłudzenia danych.
11. W przypadku utraty urządzenia jak najszybciej zastrzeż numer telefonu w bankowości elektronicznej lub zgłoś np. skradziony telefon do operatora, podając numer IMEI i SIM.

Bądźmy wyczuleni na wiadomości z propozycją aktualizacji systemu operacyjnego. Z czujnością sprawdzajmy, czy pochodzą od naszego operatora. W razie jakichkolwiek wątpliwości, skontaktujmy się ze sprzedawcą oprogramowania i zweryfikujmy, czy otrzymana wiadomość nie jest próbą wyłudzenia naszych danych. Pamiętaj, jeśli został Ci skradziony komputer lub smartphone, który nie posiadał hasła logowania a hasła dostępowe do konta zostały zapisane w przeglądarce internetowej, wówczas nie nastąpi weryfikacja dwuetapowa. A to może ułatwić niepowołany dostęp do twojej bankowości elektronicznej.

Złamanie ochrony naszego urządzenia, przejęcie nad nim kontroli oraz uzyskanie dostępu do naszych danych przez nieuprawnione osoby jest najgroźniejszą sytuacją. Kiedy przestępca włamie się do naszego urządzenia, pozostałe zabezpieczenia np. silne hasła nie są już dla niego zaporą – przestępca może bowiem śledzić każde nasze działanie poprzez nagrywanie, podsłuchiwanie czy oglądanie wykonywanych czynności.

Bezpieczne używanie karty płatniczej

Użytkownicy kart płatniczych są narażeni na przestępstwo zwane skimmingiem, które polega na kopiowaniu danych z paska magnetycznego karty płatniczej. Dane – takie jak numer karty czy data ważności – służą przestępcy do wykonania kopii karty płatniczej, a następnie umożliwiają mu zrealizowanie płatności internetowej lub wypłaty z bankomatów środków z konta ofiary. 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. Dodatkowo przestępcy montują małe kamery, które rejestrują wpisywany przez właściciela karty kod PIN. Ochroną przed tego typu atakiem jest chip wbudowany w karty płatnicze (kiedyś standardem były karty wyłącznie z paskiem magnetycznym). Jednak przestępcy coraz częściej próbują złamać i to zabezpieczenie przy użyciu urządzenia pod nazwą shimmer, które potrafi kopiować dane z kart z mikroprocesorem. 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. Złodzieje mogą również montować w miejscu wydawania pieniędzy nakładkę, do której przyklejają się banknoty. Osoba widzi komunikat o wydaniu banknotów, które nie zostały wydane przez bankomat. Po oddaleniu użytkownika od bankomatu przestępca może ukraść pozostawione pieniądze. Jeżeli bankomat nie budzi naszych zastrzeżeń, pamiętajmy, by zasłonić wpisywany kod PIN ręką – tak by nie zarejestrowała go żadna kamera i nie zobaczyła osoba stojąca za nami.

> Podrabianie karty płatniczej jest przez Kodeks karny traktowane jako podrabianie „innego środka płatniczego". Grozi za to odpowiedzialność karna – od 5 do 25 lat pozbawienia wolności.

Pamiętajmy, by płacąc kartą, nigdy nie tracić jej z pola widzenia. Ograniczamy w ten sposób możliwość skopiowania karty np. przez nieuczciwego sprzedawcę lub usługodawcę. Płatność zbliżeniowa niweluje ten typ zagrożenia. Dodatkowo w przypadku transakcji do kwoty 100 zł nie musimy podawać kodu PIN.

Ważnym zabezpieczeniem (szczególnie gdy przestępcy udało się zrobić duplikat naszej karty) jest posiadanie dziennego limitu transakcji bezgotówkowych – w ten sposób przestępca nie będzie mógł zrealizować transakcji powyżej ustalonej kwoty.

Jeżeli podejrzewamy, że mogliśmy paść ofiarą skimmingu (lub odkryjemy na naszym koncie transakcje, których nie robiliśmy), musimy jak najszybciej zastrzec kartę, powiadomić bank oraz zgłosić zdarzenie na policję, ponieważ skimming jest przestępstwem. Kartę możemy zastrzec w każdym banku lub w Zintegrowanym Systemie Zastrzegania Kart (który jednak nie obejmuje wszystkich instytucji, które wydają karty płatnicze).

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?

Dzięki korzystaniu z bankowości mobilnej zyskujemy łatwy dostęp do konta bankowego, który nie wymaga logowania się przez stronę internetową banku. 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. Jednak również w tym przypadku bezpieczne logowanie zależy przede wszystkim od nas. Pierwszą zasadą jest instalowanie aplikacji z pewnego źródła. Również aplikacje, które nie są powiązane z obsługą konta bankowego (np. komunikator), nie mogą być aplikacjami niewiadomego pochodzenia. Zapewnijmy, by telefon, na którym korzystamy z aplikacji bankowej był zabezpieczony oprogramowaniem antywirusowym. Podstawowym zabezpieczeniem jest zapora sieciowa, która radzi sobie z atakami hakerskimi. Dopytajmy, czy instalowany przez nas program antywirusowy jest wyposażony w mechanizmy skanujące aplikacje, które pobieramy na telefon, pobierane pliki oraz odwiedzane strony. W przypadku zidentyfikowanego zagrożenia, oprogramowanie powiadomi nas o tym, podejmując działanie blokowania złośliwego oprogramowania bądź dostępu do strony rozpoznanej jako złośliwa. Aktualizujmy system operacyjny zgodnie z komunikatami w telefonie – każda aktualizacja lepiej zabezpiecza aplikację.

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.

W 2020 r. odsetek osób, które najczęściej dokonywały płatności przy pomocy telefonu wynosił 9%, w 2019 r. było to 5% badanych (źródło: raport NBP: „Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2020 r."). Płatności telefonem można realizować, korzystając ze specjalnej aplikacji – naszą karta płatnicza jest „dodawana" do wirtualnego portfela. Dane karty, którą dodamy do aplikacji, są szyfrowane, a każda skonfigurowana karta otrzymuje własny numer VAN, który jest przechowywany w urządzeniu. Jest to metoda równie bezpieczna jak płatności kartą, pod warunkiem zapewnienia odpowiedniej ochrony smartfonowi. Zasady bezpieczeństwa są identyczne, jak w przypadku aplikacji mobilnej. Pamiętajmy, aby logować się do smartphone za pomocą mocnego hasła, numeru PIN do odblokowania telefonu, który składa się z min. 6 cyfr, alternatywnie przy użyciu odcisku palca. Wyposażmy telefon w oprogramowanie antywirusowe. Warto pamiętać, że w razie zgubienia telefonu możemy wyłączyć kartę w telefonie za pomocą systemu bankowości elektronicznej lub przez infolinię. Wyłączenie karty w telefonie nie jest tożsame z zablokowaniem karty płatniczej – możemy jej wciąż używać do wykonywania transakcji. Możemy również czasowo zablokować kartę w przypadku, gdy np. wyjeżdżamy za granicę i wiemy, że przez dłuższy czas nie będziemy z niej korzystać. W analogiczny sposób działają płatności smartwatchem.

Według prawa zlecenie płatnicze uznaje się za wykonane na rzecz właściwego odbiorcy, jeśli zostanie przeprowadzone zgodnie z podanym identyfikatorem (np. numerem rachunku), niezależnie od tego, jakie dane osobowe zostały podane jako dodatkowe.

W II półroczu 2020 r. wartość transakcji zrealizowanych za pomocą kodu BLIK wynosiła 33,4 mld zł, a średnia dzienna liczba zleceń transakcji wynosiła 1,36 mln. Na koniec 2020 r. system BLIK obejmował 14 banków i 16,9 mln użytkowników w Polsce (źródło: raport NBP: „Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2020 r."). 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. Jak łatwo się domyślić również ten sposób płatności jest na celowniku oszustów. Najczęściej do oszustwa dochodzi po przejęciu przez hakerów konta w mediach społecznościowych – oszust, w imieniu właściciela konta, wysyła do jego znajomych prośbę o wykonanie przelewu BLIK. Dobrowolne podanie kodu BLIK pozbawia nas praw do odzyskania pieniędzy, które oszust ukradnie w ten sposób. Podczas płatności internetowych zawsze sprawdzaj poprawność wpisywanych danych – przede wszystkim numer konta.

Bank nie ponosi odpowiedzialności za przelew, którego odbiorca (identyfikowany na podstawie numeru rachunku) był niewłaściwy. W przypadku kiedy wykonamy transakcje z użyciem błędnie podanego numeru rachunku, musimy zgłosić to bankowi, który w ciągu trzech dni musi albo bezpośrednio, pisemnie, skontaktować się z odbiorcą przelewu (jeśli jest on również klientem tego samego banku), albo zwrócić się do banku odbiorcy. W obu przypadkach odbiorca otrzymuje informacje o możliwościach zwrotu przelewu, który otrzymał. Płatnik, który wykonywał transakcję może otrzymać zwrot na wskazany przez siebie rachunek lub poprzez wypłatę środków w formie gotówki.

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.
14. Zawsze pamiętaj o wylogowaniu się z bankowości elektronicznej.

Zadania dla uczniów

1. Zadanie indywidualne

W jaki sposób najczęściej korzystasz z bankowości elektronicznej i dokonujesz transakcji? Sprawdź, czy stosujesz wszystkie zasady z Kodeksu cyberbezpieczeństwa?

2. Dyskusja w klasie

Przeczytajcie raz jeszcze Kodeks cyberbezpieczeństwa. Przyporządkujcie zasady do różnych form bankowości elektronicznej.