Podstawowe zasady bezpieczeństwa w trakcie korzystania z bankowości elektronicznej i mobilnej

Wyjaśniamy

W Polsce według danych Głównego Urzędu Statystycznego ponad 90% gospodarstw domowych w 2020 r. miało dostęp do internetu[1]. W ostatnim roku przybyło ponad pół miliona użytkowników bankowości internetowej, dzięki której klient może samodzielnie, bez wychodzenia z domu dokonać przelewu, założyć lokatę czy na bieżąco kontrolować poziom swoich wydatków. Jednak nieznajomość lub nieprzestrzeganie zasad bezpiecznego korzystania z bankowości elektronicznej to prosta droga do strat finansowych. Zgodnie z badaniami Urzędu Ochrony Danych Osobowych niemal 22% badanych nigdy nie zmieniało haseł dostępu do swojego rachunku bankowego. Co więcej, tylko co czwarty Polak ma jakiekolwiek obawy o to, że jego dane zostaną przejęte przez cyberprzestępców.

Czy wiesz, że…

Zgodnie z danymi Związku Banków Polskich oraz Centrum Prawa Bankowego i Informacji na koniec 2019 r. w Polsce:

- od 17% badanych w ciągu ostatnich 12 miesięcy próbowano uzyskać prywatne dane za pośrednictwem e-mail lub telefonu,
- jedynie 49% badanych zmieniło hasło do bankowości internetowej w ciągu ostatnich 12 miesięcy,
- 65% Polaków słabo ocenia swoją wiedzę o cyberbezpieczeństwie.

Źródło: badanie ZBP i CPBil, grudzień 2019 r., https://www.zbp.pl

Podstawowe zasady bezpieczeństwa

Bezpieczeństwo w sieci zależy głównie od użytkownika i wymaga znajomości podstawowych zasad chroniących dane i zasoby, ale także żelaznej konsekwencji w ich przestrzeganiu.

Bezpieczne logowanie się i hasło

Podstawowe zasady bezpieczeństwa dotyczą loginu i hasła używanego do logowania się do bankowości elektronicznej. Hasło to podstawowe zabezpieczenie dostępu do konta. Aby spełniało swoją funkcję, musi być odpowiednio silne i nie może być łatwe do odgadnięcia.

Takie zasady dotyczą nie tylko bankowości internetowej; powinny być stosowane przy okazji korzystania ze wszelkich usług oferowanych w sieci. Należy przy tym pamiętać, aby używać odrębnych haseł do różnych kont (nie tylko bankowych). Przed jakąkolwiek operacją związaną z bankowością elektroniczną trzeba sprawdzić, czy na pasku adresowym widzimy dwa podstawowe elementy – znak kłódki oraz skrót „https://". Po naciśnięciu na znak kłódki sprawdźmy, czy certyfikat witryny jest aktualny i wystawiony przez uprawnionego wystawcę. Nasze wątpliwości powinny ponadto wzbudzić: długi czas logowania, nietypowe komunikaty (np. „nastąpiły

1 https://stat.gov.pl

zmiany w regulaminie banku, podaj swoje login i hasło ponownie"), pojawienie się niestandardowego pola z prośbą o powtórzenie hasła lub nieuzasadniony komunikat o błędzie przy wpisywaniu hasła.

Zasady tworzenia silnego hasła

1. Odpowiednia długość – hasło powinno się składać z co najmniej 8 znaków. Bezpieczna długość to około 14 znaków.
2. Różne znaki i symbole – powinny to być duże i małe litery, cyfry, znaki specjalne. Warto, aby na klawiaturze te znaki i symbole były umieszczone na jak najszerszym obszarze.
3. Oryginalność i kreatywność – nie używaj haseł oczywistych, powszechnie znanych (np. „12345") lub znaczących, np. dat, imion, adresów, numerów lub nazw (np. „Monika55").
4. Nie korzystaj z opcji zapamiętywania haseł.
5. Każde konto internetowe powinno mieć inne hasło.

Sprawdź się!

Które z wymienionych niżej haseł uznałbyś za bezpieczne?

a) zaq12wsx b) Wrocław789456 c) KYe%Wn.hND d) qw78as45zx12

Zgodnie z obowiązującą od 14 września 2019 r. dyrektywą unijną dotyczącą usług płatniczych (PSD2) tożsamość konsumenta, który korzysta z elektronicznych usług płatniczych, musi być podwójnie zweryfikowana. Podwójna weryfikacja powinna zostać przeprowadzona w momencie logowania się na konto bankowe lub dokonywania jakiejkolwiek czynności narażającej konsumenta na ataki cybernetyczne. Podwójna weryfikacja, jak sama nazwa wskazuje, przebiega w dwóch etapach. Pierwszy to wprowadzenie informacji, którą zna tylko użytkownik, np. hasła. Drugi etap to użycie czegoś, co znajduje się tylko w posiadaniu klienta banku. Przykładem może być konieczność podania dodatkowego hasła przesłanego w wiadomości SMS lub zatwierdzenie logowania przy użyciu aplikacji mobilnej. Zmiany wynikające z dyrektywy PSD2 dotyczą nie tylko sposobu logowania się, ale też innych czynności wykonywanych podczas korzystania z bankowości elektronicznej. Gdy będziemy wykonywali przelew, bank dodatkowo poprosi nasnp. o podanie kodu przesłanego w wiadomości SMS. Również dostęp do części danych będzie wymagał od użytkownika dodatkowej weryfikacji. Niektóre banki wprowadziły na przykład konieczność dodatkowej autoryzacji podczas sprawdzania historii operacji starszych niż 90 dni.

Nie udostępniaj nikomu loginu i hasła. Nie zapisuj w widocznym miejscu, np. na karcie. Zmieniaj hasło cyklicznie.

Dyrektywa PSD2 zmieniła również zakres odpowiedzialności banku za nieautoryzowane płatności. Przed 14 września 2019 r. odpowiedzialność banku za nieautoryzowane płatności – to znaczy takie, które nie wymagały np. użycia PIN-u – zaczynała się od kwoty 150 euro. Obecnie limit, od którego zaczyna się odpowiedzialność banku, został obniżony do 50 euro. Oznacza to, że jeśli przestępca ukradnie nam telefon lub kartę bankową i dokona przy ich użyciu płatności, nasza odpowiedzialność będzie ograniczona do 50 euro. Powyżej tej kwoty ryzyko ponosi bank.

W ramach wdrażania dyrektywy banki znacznie skróciły czas sesji w swoich serwisach internetowych lub mobilnych, czyli czas, po którym klient zostanie automatycznie wylogowany, jeśli nie będzie wykonywał żadnych czynności. Obecnie w każdym banku sesje bez aktywności klienta nie mogą być dłuższe niż 5 minut (wcześniej było to 10 minut).

Unikanie otwierania załączników i podejrzanych linków

Korzystając z bankowości elektronicznej, trzeba pamiętać, aby nigdy nie otwierać podejrzanych linków i załączników w otrzymanych wiadomościach e-mail lub SMS. Czujność powinien wzbudzić link, który zaczyna się protokołem http (zamiast https) i zawiera podejrzaną, nieznaną nam nazwę strony internetowej. Banki nigdy nie przesyłają klientom linków do logowania i próśb o przesłanie danych osobowych. Dotyczy to również linków do logowania otrzymanych za pośrednictwem mediów społecznościowych. Zawsze bardzo uważnie czytajmy informacje przesłane drogą mailową lub w wiadomościach SMS dotyczące żądań zapłaty, różnego rodzaju ostrzeżeń (np. przed blokadą dostępu do usług banku) czy korespondencji z załączonymi fakturami. Kliknięcie w fałszywy link czy odnośnik może przekierować użytkownika na stronę internetową, z której pobierane jest złośliwe oprogramowanie przejmujące kontrolę nad jego urządzeniami. W ten sposób może nastąpić zdobycie danych, które posłużą do logowania się na konto bankowe, i jednocześnie przejęcie kontroli nad wiadomościami autoryzacyjnymi wysyłanymi przez bank.

Nie otwieraj linków i załączników z podejrzanych wiadomości e-mail i SMS.

Korzystaj z aktualnego i legalnego oprogramowania antywirusowego.

Właściwe zabezpieczenie sprzętu

Na urządzeniu, z którego logujemy się do bankowości elektronicznej, trzeba zainstalować aktualne, pochodzące z legalnego źródła oprogramowanie antywirusowe i pamiętać o jego regularnym aktualizowaniu. Bardzo istotne jest też aktualizowanie systemów operacyjnych, aplikacji czy oprogramowania do wysyłania poczty elektronicznej. Brak aktualizacji otwiera cyberprzestępcom dostęp do naszego sprzętu. Może również dojść do sytuacji, w której złośliwe oprogramowanie zmienia parametry operacji bankowej, np. podczas wykonywania przelewu podmienia numer rachunku bankowego, jeśli stosujemy opcję „kopiuj–wklej". Korzystanie z tej wygodnej opcji może się stać przyczyną przelania środków do niewłaściwego adresata. Dlatego zaleca się, aby zawsze samodzielnie wpisywać numer rachunku bankowego, a następnie sprawdzać jego poprawność. Korzystanie z bankowości elektronicznej wymaga zachowania szczególnej ostrożności również, jeśli chodzi o używanie sprzętu komputerowego. Ściąganie jakichkolwiek programów z niepewnych źródeł może być niebezpieczne. Nawet jeśli mamy zaufanie do własnych urządzeń, to nie możemy mieć pewności, czy inne komputery (szczególnie publicznie dostępne) pozwalają na bezpieczne korzystanie z bankowości elektronicznej. Oddając sprzęt do naprawy, należy pamiętać o wylogowaniu się z aplikacji bankowych oraz o usunięciu wszystkich poufnych informacji.

Nigdy nie pobieraj programów z niezaufanych źródeł.

Unikaj używania opcji „kopiuj-wklej" przy wpisywaniu numeru rachunku bankowego.

Używaj zaufanego komputera oraz telefonu do logowania się na swoje konto w banku.

Ochrona i weryfikacja danych

Złośliwe oprogramowanie, jeśli zainfekowało komputer lub telefon, z którego korzystamy, może „podmienić" numer rachunku bankowego odbiorcy na fałszywy, np. w trakcie dokonywania przelewu. Dlatego konieczne jest cykliczne sprawdzanie poprawności numeru rachunku w przelewach wcześniej zdefiniowanych, dla których za każdym razem uzupełniamy zmienną część danych (np. kwotę). Warto często przeglądać historię rachunku bankowego pod kątem podejrzanych transakcji. Jeśli to możliwe, należy włączyć opcję powiadomienia SMS z informacją o każdej transakcji rejestrowanej na rachunku bankowym. Dobrą praktyką jest ustalenie odpowiednich limitów płatności przelewem i kartą płatniczą. Im niższy limit, tym mniejsze ryzyko utraty dużej kwoty z konta bankowego. Korzystając z bankowości mobilnej, trzeba koniecznie zabezpieczać swój telefon kodem PIN lub biometrycznie (np. odciskiem palca).

Cyklicznie przeglądaj historię rachunku bankowego pod kątem podejrzanych transakcji.

Unikaj wysokich limitów operacji dla przelewów i kart płatniczych.

Nie podawaj nikomu numeru karty, daty jej ważności oraz kodu CVC lub CVV.

Coraz bardziej popularnym działaniem przestępców jest kopiowanie kart płatniczych. Przestępcy mogą zamontować w bankomatach specjalną nakładkę, która skopiuje zawartość paska magnetycznego karty oraz odczyta numer PIN dzięki dodatkowej nakładce na klawiaturze bankomatu. Tak skopiowana zawartość paska jest następnie umieszczana na innej karcie, którą posługują się przestępcy.

Płacąc kartą płatniczą za zakupy lub usługi w sieci, podajemy numer karty, datę jej ważności oraz trzycyfrowy kod weryfikujący transakcję (CVC lub CVV). Wszystkie dane znajdują się na karcie, dlatego jej utrata możne narazić nas na straty. Tych danych nie należy nikomu podawać z wyjątkiem autoryzowanych transakcji zabezpieczonych zgodnie z powyższym opisem. Również pracownik banku telefonicznie czy mailowo nie poprosi nas o tego typu dane. Jeśli więc ktoś będzie chciał pozyskać od nas numer karty, datę jej ważności oraz kod CVC lub CVV, to prawdopodobnie będzie to przestępca. Zagrożenie w przypadku nieuprawnionego użycia naszych danych dotyczy nie tylko informacji na karcie płatniczej, ale również innych danych osobowych, zamieszczonych np. w dowodzie osobistym, legitymacji lub prawie jazdy. Ich utrata może spowodować, że przestępca posłuży się naszymi danymi, by zaciągnąć zobowiązanie bez naszej wiedzy. Dlatego w przypadku zgubienia karty pamiętajmy o jak najszybszym jej zastrzeżeniu, np. za pośrednictwem banku, na stronie www.zastrzegam.pl lub telefonicznie pod numerem 828 828 828.

Coraz częstszym działaniem przestępców jest oszustwo „na BLIK-a". Polega ono na tym, że przestępcy przejmują konto użytkownika w mediach społecznościowych, a następnie wysyłają do znajomych prośby o przesłanie kodu BLIK. Gdy oszuści otrzymają kod, okradają konto bankowe oszukanej osoby. Oszustwo „na BLIK-a" jest dobrym przykładem powiązania bankowości elektronicznej z innymi rodzajami aktywności w sieci. Jeśli chcemy chronić nasze środki w banku, musimy pamiętać również o zabezpieczaniu swoich kont w mediach społecznościowych.

Otwarte sieci jako potencjalne zagrożenie

Dla zachowania bezpieczeństwa ma znaczenie, gdzie i w jaki sposób łączymy się z internetem. Jedną z kluczowych zasad jest rezygnacja z korzystania z otwartych sieci WiFi, np. na lotnisku czy w kawiarni. Niezabezpieczona sieć WiFi może stanowić pułapkę zastawioną przez przestępców, którzy mają możliwość przechwycenia danych wrażliwych. Przykładem może być modyfikowanie przez przestępców adresu strony internetowej banku. W tej sytuacji nieświadomy użytkownik jest przekierowywany na stronę internetową do złudzenia przypominającą stronę banku. Adres internetowy strony, na którą nas przekierowano, może się różnić nieznacznie, np. jedną literką, od adresu strony służącej do logowania się do bankowości elektronicznej.

> Logując się do bankowości elektronicznej, zrezygnuj z korzystania z otwartych sieci WiFi.

Komunikaty bankowe cennym źródłem informacji

Dobrym źródłem ostrzeżeń o niebezpieczeństwach podczas korzystania z bankowości elektronicznej są komunikaty banku. Niestety wiele osób takie komunikaty pomija, a mogą one zwrócić uwagę na pułapki stosowane przez przestępców chcących wyłudzić nasze dane lub pieniądze. Jeśli już zaobserwujemy jakiekolwiek podejrzane lub nietypowe działania, powinniśmy niezwłocznie poinformować o tym nasz bank, by sprawdził i zabezpieczył nasze konto. Zawsze możemy skorzystać z infolinii swojego banku oraz pozyskać informacje na temat bezpieczeństwa wykonywanych transakcji za pośrednictwem internetu. Szybki kontakt z bankiem może ochronić nasze środki na rachunku przed cyberprzestępstwem, jeśli np. w historii rachunku zauważymy podejrzane transakcje lub otrzymamy komunikat o próbie logowania na nasze konto.

> Podejrzane lub nietypowe działania niezwłocznie zgłoś do banku.

Bezpieczeństwo aplikacji mobilnych

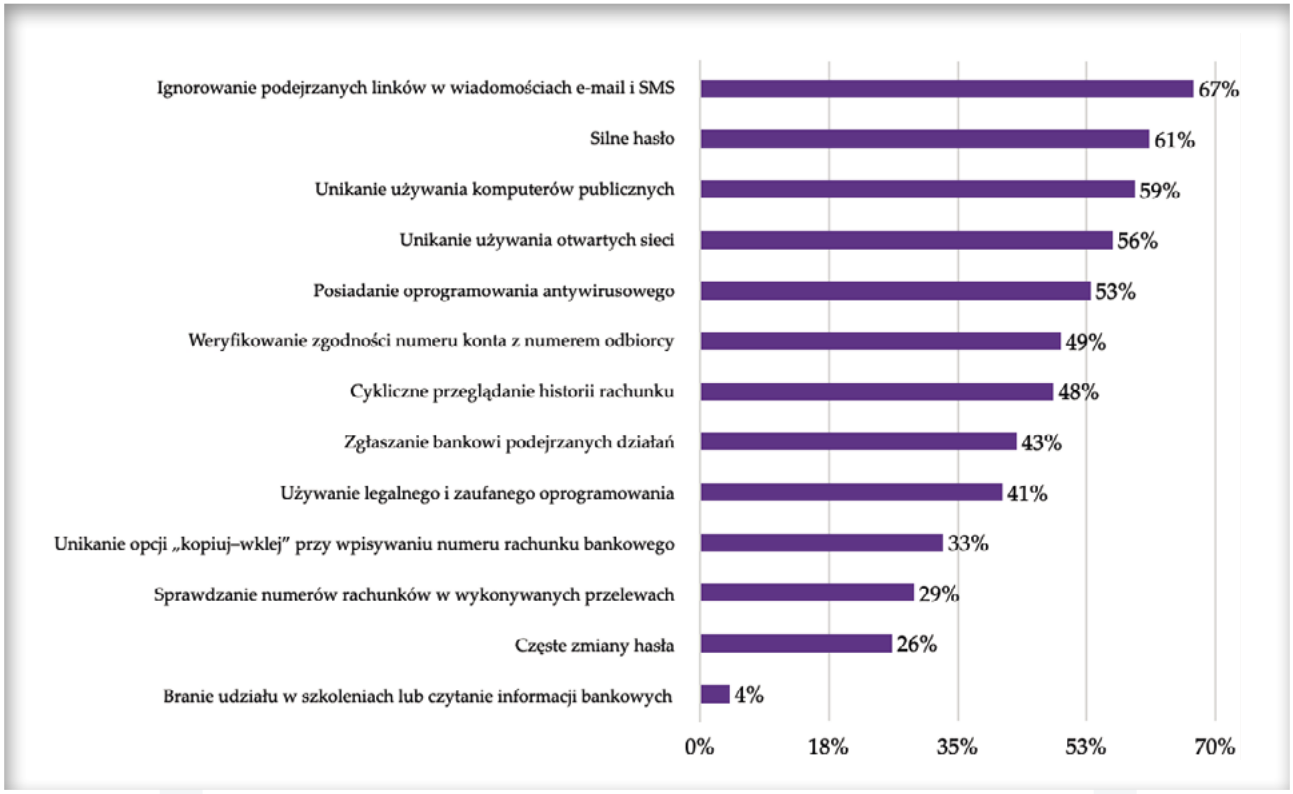
Wszystkie opisane wcześniej zasady dotyczą również bezpiecznego korzystania z aplikacji mobilnych. W przypadku posługiwania się tego typu narzędziami należy szczególnie zwrócić uwagę, by aplikacja bankowa była pobierana z wiarygodnego źródła. Należy korzystać tylko z oficjalnego sklepu z aplikacjami, a w razie wątpliwości skontaktować się z bankiem. Sklepy przeznaczone dla najpopularniejszych systemów operacyjnych to Google Play dla Android oraz App Store dla iOS. Niebezpieczeństwo może się wiązać z instalowaniem w telefonie nieznanych aplikacji (również tych niezwiązanych z bankowością mobilną). Oficjalne sklepy stosują wiele zabezpieczeń i korzystanie z umieszczonych tam aplikacji jest znacznie bezpieczniejsze niż w przypadku zasobów spoza tego typu sklepów. Pamiętajmy, że zabezpieczenie telefonu kodem PIN lub biometrycznie oraz ustalenie niskich limitów transakcji mobilnych znacznie ograniczy ryzyko utraty środków. Banki na bieżąco weryfikują bezpieczeństwo mobilnych kanałów dostępu, dlatego przygotowywane są aktualizacje, które pomagają coraz lepiej zabezpieczać aplikację. Nie należy więc odkładać aktualizacji oprogramowania całego systemu operacyjnego, programów antywirusowych czy – w szczególności – aplikacji bankowej. Uważajmy też przy korzystaniu z kodów QR. Kody tego typu, jeśli pochodzą z nieznanego źródła, mogą zawierać niebezpieczne oprogramowanie.

> Zwróć uwagę, by źródło pochodzenia kodu QR było wiarygodne.

Jak w rzeczywistości wyglądają nasze zachowania w bankowości internetowej

Badanie z 2020 r., przeprowadzone przez SGH w Warszawie w Katedrze Systemu Finansowego na próbie 1804 osób, pokazało, że Polacy, korzystając z sieci, nie zachowują się bezpiecznie. Jedynie co czwarty z badanych często zmienia hasło, a tylko 4% czyta przekazywane przez banki informacje o zagrożeniu w sieci.

Wykres. Jakie typy zachowań charakteryzują Polaków korzystających z internetu



Źródło: badanie przeprowadzone w Katedrze Systemu Finansowego SGH: Cichowicz E., Iwanicz-Drozdowska M., Kurowski Ł. (2021). „Cyber (nie)bezpieczeństwo społeczeństwa polskiego". Gazeta SGH. https://gazeta.sgh.waw.pl/meritum/cyber-niebezpieczenstwo-spoleczenstwa-polskiego.

Zadania dla uczniów

1. Dyskusja w rodzinie

Porozmawiajcie z rodzicami, czy i które z wymienionych powyżej zasad stosują podczas korzystania z bankowości elektronicznej.

2. Dyskusja w klasie

Czy warto mieć internetowe konto bankowe lub usługę bankowości mobilnej? A może wobec istniejących zagrożeń należy zrezygnować z bankowości elektronicznej?

3. Dyskusja w grupie

Wyobraźcie sobie, że jesteście członkami zespołu ds. bezpieczeństwa sieci w banku. Jakie działania byście podjęli, aby ograniczyć ryzyko związane z korzystaniem przez waszych klientów z bankowości internetowej? Zaprojektujcie kampanię edukacyjną, która byłaby najbardziej przekonująca dla Waszej grupy wiekowej.