PODSTAWOWE ZASADY BEZPIECZEŃSTWA W TRAKCIE KORZYSTANIA Z BANKOWOŚCI ELEKTRONICZNEJ I MOBILNEJ.

Złote szkoły NBP

II edycja programu 2021/2022

Bezpieczni w finansach osobistych

wykonała: Julia Pieńkus

PODSTAWOWE ZASADY BEZPIECZEŃSTWA

Pamiętaj!!!

Bezpieczeństwo w sieci zależy przede wszystkim 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.
- Należy 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.

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.

3. Oryginalność i kreatywność – nie używaj haseł oczywistych, powszechnie znanych (np. „12345”) lub znaczących, np. dat, imion, adresów, numerów lub nazw.

4. Nie korzystaj z opcji zapamiętywania haseł.

5. Każde konto internetowe powinno mieć inne hasło.

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.
- 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.

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.

OCHRONA I WERYFIKACJA DANYCH

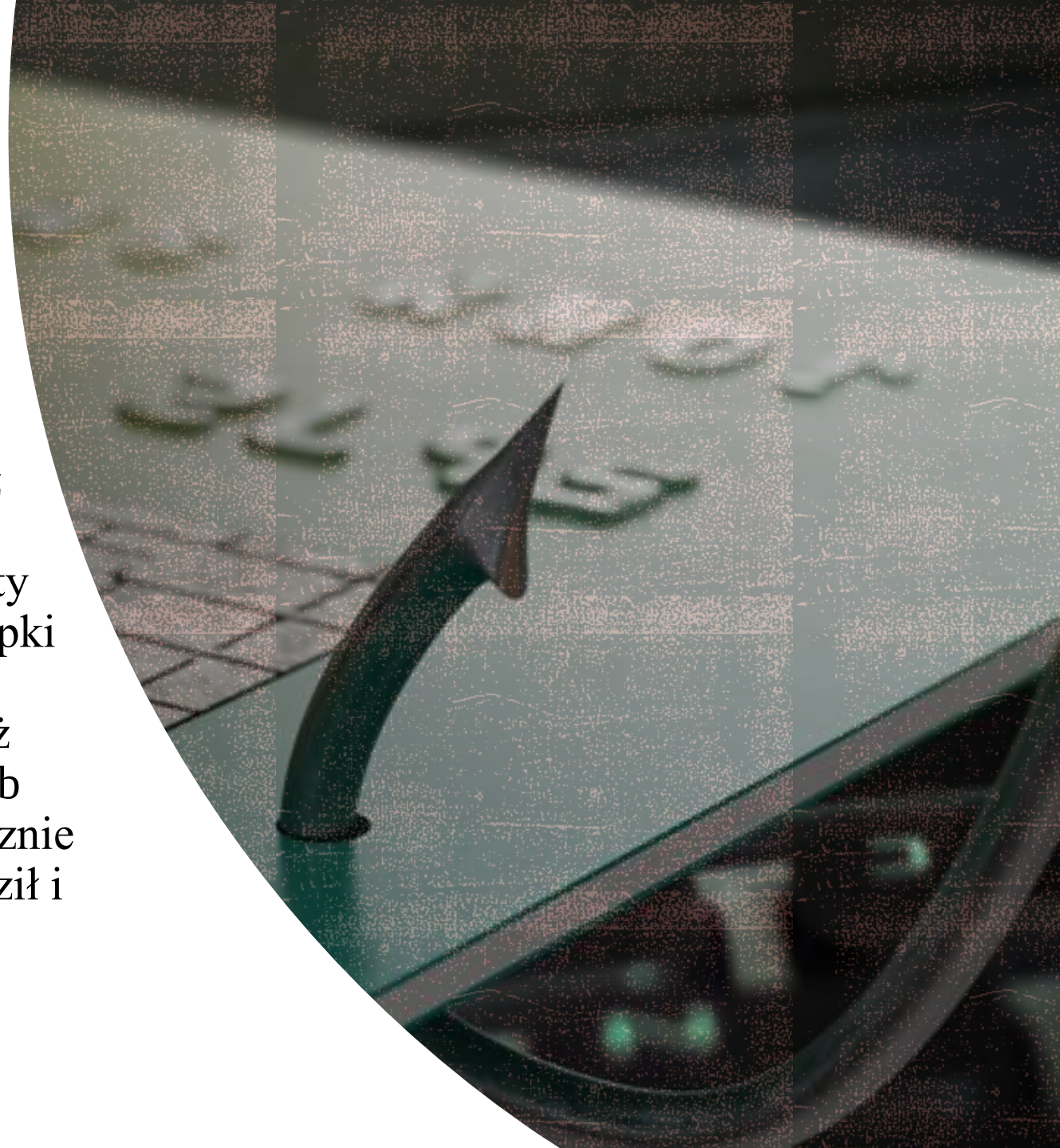
- Złośliwe oprogramowanie, jeśli zainfekowało komputer lub telefon, z którego korzystamy, może „podmienić” numer rachunku bankowego odbiorcy na fałszywy, np. w trakcie dokonywania przelewu. Dlatego konieczne jest cykliczne sprawdzanie poprawności numeru rachunku w przelewach wcześniej zdefiniowanych, dla których za każdym razem uzupełniamy zmienną część danych (np. kwotę). Warto często przeglądać historię rachunku bankowego pod kątem podejrzanych transakcji.
- 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.

OTWARTE SIECI JAKO POTENCJALNE ZAGROŻENIE

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.

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.



BEZPIECZEŃSTWO 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. Sklepy przeznaczone dla najpopularniejszych systemów operacyjnych to Google Play oraz App Store. Oficjalne sklepy stosują wiele zabezpieczeń i korzystanie z umieszczonych tam aplikacji jest znacznie bezpieczniejsze. Pamiętajmy, że zabezpieczenie telefonu kodem PIN oraz ustalenie niskich limitów transakcji mobilnych znacznie ograniczy ryzyko utraty środków.

DZIĘKUJE ZA UWAGĘ