edukacja medialna

Bankowość elektroniczna

WIEDZA W PIGUŁCE

Współczesna bankowość różni się bardzo od tego, co jeszcze kilkanaście lat temu było standardem. Czasy, gdy szło się do oddziału banku, aby dokonać przelewu lub wypłacić gotówkę, odchodzą w niepamięć. Dziś serwisy on-line, dostępne na naszych komputerach i smartfonach, ułatwiają nam korzystanie z usług banków, a jednocześnie czynią je tańszymi. Wkraczając w dorosłość, warto dowiedzieć się, co zapewni bezpieczeństwo twoim pierwszym zarobionym pieniądzom.

Korzystanie z bankowości elektronicznej jest wygodne, ale też wiąże się z wieloma zagrożeniami, dlatego zawsze zwracaj uwagę na to, gdzie i w jaki sposób łączysz się ze swoim bankiem. Serwisy bankowe muszą być udostępniane za pomocą bezpiecznego protokołu HTTPS. Jeśli komputer wykrył jakiś problem z nim związany, nie podawaj żadnych swoich danych ani haseł. Niepokojące informacje o certyfikacie klucza HTTPS zwykle są wyświetlane automatycznie, jednak dla pewności sprawdzaj kolor ikonki kłódki przy pasku adresowym — jeśli jest zielony, śmiało loguj się na swoje konto internetowe.

Dobrym nawykiem jest również niekorzystanie z linków i wyników wyszukiwania przy wchodzeniu na stronę bankowości internetowej. Oszuści często podszywają się pod banki, tworząc fałszywe strony o adresach łudząco podobnych do tych prawdziwych. Wpisuj raczej ręcznie adres banku albo korzystaj z własnych zakładek.

Każdy, komu zależy na bezpieczeństwie swojego sprzętu i danych, pamięta o posiadaniu programu antywirusowego. Nie każdy jednak zwraca uwagę, za pośrednictwem jakiej sieci łączy się z bankowością internetową. Nie ufaj publicznym, niezabezpieczonym sieciom, do których dostęp mają przypadkowe osoby. Hakerzy są w stanie za pomocą takiego połączenia dostać się do danych w twoim komputerze. Lepiej dokonuj przelewów w domu.

Nikomu nie podawaj swoich danych autoryzacyjnych: pinów, kodów jednorazowych czy innych danych. Żaden bank nigdy nie prosi o podawanie takich informacji. Jeśli spotkasz się z podobnym żądaniem (np. w mailu), wiedz, że z pewnością nie było ono sformułowane w dobrej wierze.

Przed oddawaniem telefonu czy komputera do serwisu odinstaluj wszystkie kluczowe aplikacje, zwłaszcza bankowe. Upewnij się też, że nie masz w pamięci swoich urządzeń zapisanych danych do logowania.

Złote zasady korzystania z bankowości mobilnej

- Zwracaj uwagę, kto ma dostęp do twojego smartfona i zawsze dbaj o to, aby był on zabezpieczony odpowiednim hasłem lub symbolem.
- Nie noś ze sobą zapisanych haseł i pinów. Niektórzy trzymają je nawet w etui swoich telefonów! W przypadku kradzieży telefonu złodziej ma wówczas wszelkie informacje, aby przelać sobie wszystkie twoje oszczędności.
- Zadbaj o dobry, zaktualizowany program antywirusowy na swoim smartfonie. Jest on narażony na ataki w równym stopniu, co każdy komputer.
- Zwracaj uwagę, czy przypadkiem twój telefon nie połączył się z niezabezpieczoną, publiczną siecią WIFI.

Bankowość elektroniczna to także transakcje za pomocą kart płatniczych. Przy pomocy kodu CVC oraz numeru karty można dokonywać transakcji kartą również on-line. Dlatego

tak ważne jest, aby nikomu nie udostępniać tych informacji. Zdarza się, że młodzi ludzie po otrzymaniu swojej pierwszej karty czy dowodu osobistego robią im zdjęcia, które następnie wrzucają na portale społecznościowe. To bardzo niebezpieczne! Znając informacje podawane na karcie, ktoś może jej użyć do dokonania własnej płatności, a dane z twojego dowodu mogą posłużyć do obciążenia cię kredytem!

Jeśli będziesz stosować się do podstawowych zasad bezpieczeństwa, na pewno nic nie grozi twoim pieniądzom, a ty możesz wygodnie z nich korzystać.

POMYSŁ NA LEKCJĘ

Coraz więcej osób, posiadając konto w banku, nie wyobraża sobie braku dostępu do niego przez internet. Codziennością jest dla nas korzystanie z bankomatów czy płatności kartą. Podczas lekcji uczestnicy i uczestniczki poznają wady i zalety korzystania z bankowości elektronicznej, dowiedzą się, jak bezpiecznie z niej korzystać i jak uchronić się przed próbami wyłudzania danych.

Cele operacyjne

Uczestniczki i uczestnicy:

- wiedzą, czym jest bankowość elektroniczna;
- znają wady i zalety korzystania z bankowości elektronicznej;
- znają zasady bezpieczeństwa podczas korzystania z bankowości elektronicznej;
- potrafią rozpoznać typowe próby phishingu.

Przebieg zajęć

1.

Czas: 2 min
Forma: rozmowa
Pomoce: brak

Powiedz, że tematem dzisiejszej lekcji będzie bankowość elektroniczna, która umożliwia dostęp do rachunku bankowego za pomocą urządzeń elektronicznych. Może to być dostęp do konta bankowego przez internet, przez aplikację komórkową, a także płatności kartą i płatności zbliżeniowe. Zapytaj, czy osoby obecne na lekcji znają kogoś, kto korzysta z wymienionych form bankowości, lub same z nich korzystają.

2.

Czas: 15 min
Forma: praca indywidualna
Pomoce: długopisy, **karta pracy "Porównanie bankowości"**

Zapowiedz, że teraz przyjrzymy się różnicom pomiędzy bankowością tradycyjną a bankowością elektroniczną. Porównamy dwa rodzaje kont bankowych: obsługiwanego w placówkach banku oraz z dostępem do serwisu transakcyjnego on-line. Rozdaj uczestnikom i uczestniczkom **kartę pracy „Porównanie bankowości"** i poproś, aby wypełnili (każdy indywidualnie) tabelę, biorąc pod uwagę różne obszary dotyczące np. dostępności usług czy bezpieczeństwa. Odczytaj wspólnie z grupą wnioski i podsumuj, wskazując, że zarówno bankowość elektroniczna, jak i tradycyjna mają swoje wady i zalety.

3.

Czas: 10 min
Forma: burza mózgów
Pomoce: tablica, kreda lub marker, postity w dwóch kolorach

Następnie poproś uczestniczki i uczestników, by dobrali się w pary i spisali na zielonych karteczkach, jakie są plusy, a na żółtych karteczkach, jakie są minusy bankowości elektronicznej. Zwróć uwagę, że należy uwzględnić także płatności kartą zbliżeniową i korzystanie z aplikacji bankowych. Następnie przyklej odpowiedzi na tablicy. Odczytując wnioski, podkreśl, że do plusów należy przede wszystkim szybki i bezpośredni dostęp do konta, łatwe zarządzanie, prosta obsługa, mniejsze opłaty. Natomiast do minusów można zaliczyć: brak dostępu, gdy nie ma sieci, mniejsze bezpieczeństwo spowodowane już samym faktem, że logując się do systemu, pozostawiamy po sobie ślad, zagrożenie „wirusami", kradzieżą haseł lub karty, hakowaniem systemu, próbami wyłudzenia danych logowania.

4.

Czas: 10 min
Forma: praca wgrupach
Pomoce: tablica, kreda lub marker, **instrukcja dla grup „Pytania"**

Poproś, aby uczestniczki i uczestnicy wyobrazili sobie, że mają doradzić starszej osobie, jak powinna korzystać z bankowości elektronicznej, o czym powinna pamiętać i na co uważać. Poproś, aby aktywność została wykonana w trzech grupach: konto bankowe on-line, karta płatnicza, aplikacja. Każdej z grup daj materiał z pytaniami pomocniczymi **(instrukcja dla grup „Pytania")**, które mają ułatwić spisanie rad. Zadaniem grup jest sformułowanie rad w formie notatki i przedstawienie pozostałym grupom. Na podstawie wniosków zebranych z pracy w grupach utwórz ABC bezpieczeństwa korzystania z bankowości elektronicznej. Spisz je na tablicy.

5.

Czas: 8 min
Forma: praca indywidualna
Pomoce: długopisy, **karta pracy „Przykład maila - phishing"**

Powiedz, że ważnym aspektem korzystania z bankowości elektronicznej jest ochrona swoich danych do logowania. Wyjaśnij, że próbę wyłudzenia takich danych nazywamy phishingiem. Zazwyczaj otrzymujemy wtedy fałszywą wiadomość na skrzynkę mailową lub SMS z prośbą o logowanie i podanie swoich danych. Rozdaj karty pracy zawierające przykład maila **(karta pracy „Przykład maila - phishing")** stanowiącego próbę phishingu; poproś o pokazanie elementów, które wskazują na wyłudzenie. Zwróć uwagę, że żaden bank nie prosi poza serwisem transakcyjnym o podanie danych do logowania i często same banki ostrzegają przed phishingiem. Wiadomości phishingowe są bardzo podobne do maili od banków (logo, podpisy, użyte zwroty). Jeśli klikniemy w podany link, zostaniemy przekierowani na inną stronę niż naszego banku, lecz łudząco do niej podobną. Często adres tej strony różni się tylko jedną literą, więc trudno nam wyłapać tę nieścisłość. Jeśli mamy wątpliwości, czy mail autentycznie pochodzi z banku, możemy się upewnić, dzwoniąc na infolinię.

W podsumowaniu przypomnij, że bankowość elektroniczna coraz częściej zastępuje tę tradycyjną, dlatego ważna jest świadomość, jak bezpiecznie z niej korzystać i zapewnić bezpieczeństwo naszym pieniądzom. Warto wiedzieć, jak ustrzec się przed próbami kradzieży

pieniędzy, jakie narzędzia i wyrobienie jakich codziennych nawyków może nam w tym pomóc. Do tych ostatnich zaliczyć można: korzystanie z zaufanej sieci internetowej, posiadanie dobrego programu antywirusowego, częste i regularne robienie aktualizacji systemu, sprawdzanie certyfikatów zabezpieczeń stron banków, nieudostępnianie swoich numerów PIN, haseł, danych logowania, numeru karty.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- wiedzą, czym jest bankowość elektroniczna;
- znają wady i zalety korzystania z bankowości elektronicznej;
- znają zasady bezpieczeństwa korzystania z bankowości elektronicznej;
- potrafią rozpoznać typowe próby phishingu?

Opcje dodatkowe

Jeśli masz więcej czasu, możesz poprosić uczestników i uczestniczki o narysowanie mapy myśli zawierającej wszystkie zasady bezpiecznego korzystania z bankowości elektronicznej, w tym korzystania z konta, aplikacji oraz płatności zbliżeniowych. Zachęć, aby mapa była opatrzona grafiką, była atrakcyjna wizualnie i miała prosty przekaz.

MATERIAŁY

- **karta pracy "Porównanie bankowości"**
- **instrukcja dla grup "Pytania"**
- **karta pracy "Przykład maila - phishing"**

ZADANIE DLA UCZNIA

Zadanie 1.

Wstaw brakujące słowa:

- publiczną
- zielonego
- phishingiem
- konto internetowe, aplikacje mobilne

1. Bankowość elektroniczna daje nam dostęp do konta bankowego poprzez _____ [rozwiązanie: konto internetowe, aplikacje mobilne]
2. Wchodząc na stronę internetową banku, sprawdzamy kłódkę przy adresie strony: jeśli jest koloru _____ [rozwiązanie: zielonego], certyfikat strony jest aktualny.
3. Korzystając z mobilnej aplikacji bankowej w telefonie, nie łączymy się z _____ [rozwiązanie: publiczną] siecią internetową.
4. Wyłudzenie danych poprzez fałszywe maile czy SMS-y nakłaniające do podania haseł i loginów dostępu do konta nazywamy _____ [rozwiązanie: phishingiem].

SŁOWNICZEK

- **protokół HTTPS**: (ang. Hypertext Transfer Protocol Secure), rozszerzenie protokołu HTTP. Umożliwia przesyłanie w sieci zaszyfrowanych informacji, dzięki czemu dostęp do treści mają jedynie nadawca oraz odbiorca komunikatu.
- **certyfikat strony**: elektroniczny podpis strony internetowej, niezbędny do nawiązania połączenia https://.
- **kod CVC**: kod weryfikacyjny karty, który jest wydrukowany na odwrocie karty debetowej lub kredytowej. W przypadku większości kart (np. Visa, MasterCard czy kart bankowych) są to trzy ostatnie cyfry wydrukowane na pasku podpisu na odwrocie karty.

CZYTELNIA

- BEZPIECZNA BANKOWOŚĆ ONLINE - 3 PRAKTYCZNE WSKAZÓWKI DLA KAŻDEGO, Rightclick.pl, [dostęp: 02.11.2016], Dostępny w Internecie: rightclick.pl

Tekst: Urszula Dobrowolska, scenariusz: Monika Prus-Głaszczka, konsultacja merytoryczna: Marcin Grudzień. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/bankowosc-elektroniczna/.

Publikacja zrealizowana w ramach projektu "Cybernauci - kompleksowy projekt kształtowania bezpiecznych zachowań w sieci", finansowanego ze środków Ministra Edukacji Narodowej.

Podstawa programowa:

Informatyka, IV poziom edukacyjny
Cele kształcenia
I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.
V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Podstawy przedsiębiorczości, IV poziom edukacyjny
Treści nauczania
Instytucje rynkowe

Nowa podstawa programowa:

2018/LO/podstawy przedsiębiorczości/t2.8

2018/LO/informatyka/t3.1

2018/LO/informatyka/t3.2

2018/LO/informatyka/t5.3