Co-funded by the
Erasmus+ Programme
of the European Union

INNOWACYJNE NARZĘDZIA EDUKACYJNE

VIRIBUS UNITIS
FUNDACJA ROZWOJU REGIONALNEGO

Temat: „KARTA PŁATNICZA”

Tomasz Zacłona

Monika Makowiecka

I. Uzasadnienie wyboru tematu

Co raz więcej i częściej płatności dokonujemy z użyciem karty płatniczej. Plastikowy pieniądz nie jest już dla nikogo atrakcją, spowszechniał, a co za tym idzie nie mamy poczucia, że możemy stracić pieniądze zgromadzone na rachunku bankowym.

Warto poznać zagrożenia, na które można zostać narażonym, a także sposoby jak ustrzec się przed utratą środków finansowych na koncie.

II. Ogólne cele kształcenia

- Stworzenie uczniom szansy na zaznajomienie się z szansami zagrożeniami związanymi z użytkowaniem kart płatniczych.
- Istotnym elementem realizacji tematu jest także poznanie sposobów przeciwdziałania występującym zagrożeniom.

III. Zakres tematyczny zajęć

1. Karta płatnicza – do czego służy i czy warto ją posiadać
2. Podstawowe informacje o kartach
3. Oszustwa bankowe
4. Niepewne bankomaty i terminale
5. Proste sposoby zabezpieczenia kart płatniczych
6. Ćwiczenia

IV.Metody prowadzenia zajęć

1) Mini wykład (w oparciu o prezentację)
2) Materiały poglądowe – interaktywny film
3) Praca pod kierunkiem
4) Praca w grupie

1. Karta płatnicza – do czego służy i czy warto ją posiadać?

Jaka jest definicja karty płatniczej?

Karta płatnicza to karta powiązana z naszym kontem w banku.

Karta pozwala nam korzystać ze swoich funduszy, które są na tym koncie zebrane.

1. Karta płatnicza – do czego służy i czy warto ją posiadać?

Co to oznacza?

Przy jej pomocy możliwa jest płatność na przykład w sklepie, kawiarni, restauracji itp.

Poza tym, karta służy nam również do podjęcia pieniędzy w bankomacie.

2. Podstawowe informacje o kartach

Każda karta płatnicza:

- ma wymiary 54 milimetry na 86 milimetrów,
- posiada pasek magnetyczny lub chip (gdzie znajdują się dane właściciela karty – konkretnie jego imię i nazwisko),
- nazwę banku, który ją wydał,
- jej identyfikator,
- datę ważności
- kod CVV/CVV2 lub CVC/CVC2.

Tak naprawdę najważniejsze są te ostatnie zabezpieczenia.

2. Podstawowe informacje o kartach

Kody stanowią źródło wrażliwych danych posiadacza plastikowego pieniądza.

- Pierwszy kod jest niezbędny do dokonywania transakcji np. w sklepie, jest on weryfikowany przy skanowaniu paska magnetycznego za pomocą terminalu,
- Drugi kod służy nam do płatności internetowych. Nieraz zdarza się, że wykonując transakcję przez internet, jesteśmy proszeni o numer karty, datę jej ważności, a także kod znajdujący się na odwrocie. Wówczas wpisujemy właśnie CVC/CVC2.
- Trzecim z najważniejszych kodów jest PIN.

2. Podstawowe informacje o kartach

Transakcje bezgotówkowe stały się częścią naszego życia. Dziś niemal każdy z nas ma w portfelu kartę płatniczą, za pomocą której może uregulować rachunek w restauracji, na stacji benzynowej, zrobić zakupy w supermarkecie czy też uiścić opłaty za mieszkanie.

2. Podstawowe informacje o kartach

Ciekawostka ☺

Obecnie tego typu elektroniczne narzędzia płatnicze wydają już nie tylko banki, ale również inne instytucje finansowe lub nawet sieci handlowe, stacje benzynowe oraz przedsiębiorstwa telekomunikacyjne.

2. Podstawowe informacje o kartach

Uwaga!

Plastikowy pieniądz nie jest już dla nikogo atrakcją, spowszechniał, a co za tym idzie nie mamy poczucia, że możemy stracić pieniądze zgromadzone na rachunku bankowym.

3. Oszustwa bankowe

Wynalazki współczesności bardzo często odwracająsię przeciwko nam samym.

Dawniej najczęstszym rodzajem kradzieży związanych z kartami płatniczymi, było wykradzenie samej karty i zdobycie PIN-u do niej. Ponieważ wzrosła świadomość społeczna dotycząca tego typu incydentów, sposób ten powoli odchodzi do lamusa.

3. Oszustwa bankowe

Zagrożenia:

W skali makro organizacje takie jak MasterCard dzielą fraudy – czyli nadużycia dotyczące kart – na dwie grupy:

- groźne
- niegroźne

3. Oszustwa bankowe

Zagrożenia groźne:

To takie, w których organizacja obsługująca płatności ma styczność z masowym zagrożeniem, np. dla milionów kart.

Przykład: włamanie hackerów do firmy Sony, gdzie weszli oni w posiadanie danych klientów korzystających z PlayStation Network.

Za takie zdarzenie można byłoby uznać także złamanie zabezpieczeń Amazona lub systemów płatności takich jak Apple Pay. Serwisy te przechowują informacje o milionach ich klientów oraz posiadają wszystkie informacje o ich kartach niezbędne do realizacji transakcji.

3. Oszustwa bankowe

Zagrożenia niegroźne:

Te o których najczęściej przeczytacie w mediach ☺

Przykład: kradzież pieniędzy z konta po zeskanowaniu karty oraz podejrzeniu PIN-u, nieautoryzowane transakcje dokonywane przez Internet, np. po powrocie z zagranicznych wakacji. Krótko mówiąc wszystkie te zdarzenia, które mają charakter zdarzeń jednostkowych i cechują się małą skalą.

4. Niepewne bankomaty i terinale

Karty zbliżeniowe..

To właśnie "zbliżeniówki" wywołują obecnie największe emocje.

Z kilku powodów:

- Banki wydają karty zbliżeniowe bez względu na to czy chcemy korzystać z tej funkcjonalności czy nie.
- Wyobrażamy sobie, że każdy może podejść do nas z tyłu z czytnikiem, np. w komunikacji miejskiej i obciążyć naszą kartę na maksymalną kwotę.
- Obawiamy się, że po ewentualnej kradzieży takiej karty, złodziej będzie mógł jej wielokrotnie używać bez podawania PIN-u – i chociaż może to być prawda, to nie oznacza to wcale, że będziemy musieli ponieść koszty takich operacji.

4. Niepewne bankomaty i terminale

Typowe zagrożenia:

Bankomat:

- Zeskanowanie karty
- Podejrzenie PIN-u
- Fizyczna kradzież karty przy bankomacie
- Fizyczna kradzież gotówki po jej wyjęciu

4. Niepewne bankomaty i terminale

Typowe zagrożenia:

Transakcja w sklepie:

- Zeskanowanie karty przez obsługę sklepu lub restauracji.
- Podejrzenie PIN-u.
- Fizyczna kradzież karty.

4. Niepewne bankomaty i terminale

Typowe zagrożenia:

Używanie karty zbliżeniowej:

- Szansa przypadkowej zapłaty bez naszej świadomości – w praktyce mit.
- Możliwość wykonania transakcji zbliżeniowych offline i bez PIN-u – np. po kradzieży karty.
- Możliwość zbliżeniowego odczytania z chipa karty danych karty (ale bez kodu CVC) oraz historii ostatnio wykonanych transakcji offline.

4. Niepewne bankomaty i terminale

Typowe zagrożenia:

Płatność w internecie:

- Dane karty zostaną "podsłuchane" przez Internet – pomiędzy stroną sklepu a nami.
- Dane karty zostaną wykorzystane przez sklep internetowy w innym celu niż obsługa transakcji.
- Dane karty zostaną wykradzione ze sklepu.
- Zapłacimy, a towar do nas nie dotrze

5. Proste sposoby zabezpieczenia kart płatniczych

Dobrym rozwiązaniem może okazać się ustawienie na karcie płatniczej niskich limitów, a także włączenie powiadomień o wszelkich operacjach na rachunku bankowym.

Jeśli od razu zgłosimy kradzież bankowi, a także pójdziemy ze sprawą na policję, możliwe jest odzyskanie pieniędzy.

Instytucje finansowe za oszustwa przeprowadzane w ten sposób biorą bowiem odpowiedzialność na siebie i w wielu przypadkach oddają utracone środki.

5. Proste sposoby zabezpieczenia kart płatniczych

Co robić w trudnych sytuacjach?

Bankomat:

- Sprawdzić, czy na bankomacie nie ma żadnych nakładek – złodzieje potrafią zamontować dodatkową mikrokamerę nad bankomatem, dodatkowy skaner do paska i nakładkę na klawiaturę.
- Wybierać bankomaty w miejscach wyposażonych w monitoring, np. kamery bankowe.
- Wybierać bankomaty w miejscach zamkniętych – np. przedsionki placówek bankowych.
- Zasłaniać dłoń przy wpisywaniu PIN-u.
- Korzystać z bankomatu w czyimś towarzystwie – jeśli jest z nami ktoś znajomy, to taka "grupa" jest mniej narażona na atak niż pojedyncza osoba.
- Przerywać transakcję, jeśli w trakcie niej poczujemy się zagrożeni.

5. Proste sposoby zabezpieczenia kart płatniczych

Co robić w trudnych sytuacjach?

Transakcja PIN-em w sklepie:

- Nie spuszczać karty z oka – nigdy!
- Jeśli jest to terminal czytujący dane z mikrochipa na karcie – to sami wkładajmy i wyciągajmy z niego kartę.
- Zwracać uwagę, czy sprzedawca przeciąga kartę jednokrotnie i czy na pewno przez terminal.
- Zasłaniać dłoń przy wpisywaniu PIN-u.
- Ostrożność wskazana przede wszystkim za granicą.

5. Proste sposoby zabezpieczenia kart płatniczych

Co robić w trudnych sytuacjach?

Używanie karty zbliżeniowej:

- Nosić w portfelu dwie karty zbliżeniowe zetknięte ze sobą – to stanowi stuprocentowe zabezpieczenie przed ewentualnym obciążeniem karty. Takie karty skutecznie zakłócają swoje radio.
- Zbliżać kartę do terminala płatniczego wyłącznie po zobaczeniu ile mamy zapłacić.

5. Proste sposoby zabezpieczenia kart płatniczych

Co robić w trudnych sytuacjach?

Płatność w internecie:

- Strona sklepu powinna obsługiwać szyfrowanie SSL.
- Warto sprawdzać poprawność certyfikatu SSL sklepu internetowego.
- Sprawdzać czy podajemy dane karty sklepowi, czy firmie pośredniczącej w obsłudze płatności (acquirer).
- Nie zapisywać danych karty kredytowej w sklepie internetowym.
- Korzystać z tzw. eWalletów, czyli elektronicznych portfeli – takim portfelem jest np. MasterPass.

5. Proste sposoby zabezpieczenia kart płatniczych

Dobre praktyki:

- PIN do karty i kod CVC/CVV musimy chronić jak oka w głowie – to one właśnie służą do potwierdzania, że to my wykonaliśmy transakcję.
- Pod żadnym pozorem PINu nie wolno przechowywać razem z kartą, np. zapisanego na karcie albo w portfelu.
- Wszystkie karty powinniśmy trzymać przy sobie, niezależnie gdzie będziemy.
- Warto systematycznie sprawdzać wyciągi z kont bankowych i kart – jeśli spisujemy wydatki, to szybko wyłowimy te transakcje, których sami nie dokonywaliśmy.
- Zastąp jak największej ilości transakcji autoryzowanych PIN-em – transakcjami zbliżeniowymi.

5. Proste sposoby zabezpieczenia kart płatniczych

Inne sposoby zwiększania bezpieczeństwa:

Banki oraz organizacje płatnicze wprowadzają także dodatkowe zabezpieczenia transakcji dokonywanych w Internecie, np. 3D Secure (oznaczany także nazwami "MasterCard SecureCode" oraz "Verified by Visa").

3D Secure to rozwiązanie, w którym – po wprowadzeniu danych karty bankowej – przekierowywani jesteśmy na stronę banku w celu podania dodatkowego kodu zabezpieczającego. Zazwyczaj jest on przesyłany na nasz telefon komórkowy jako SMS.

6. Ćwiczenia praktyczne

Dziękuję za uwagę