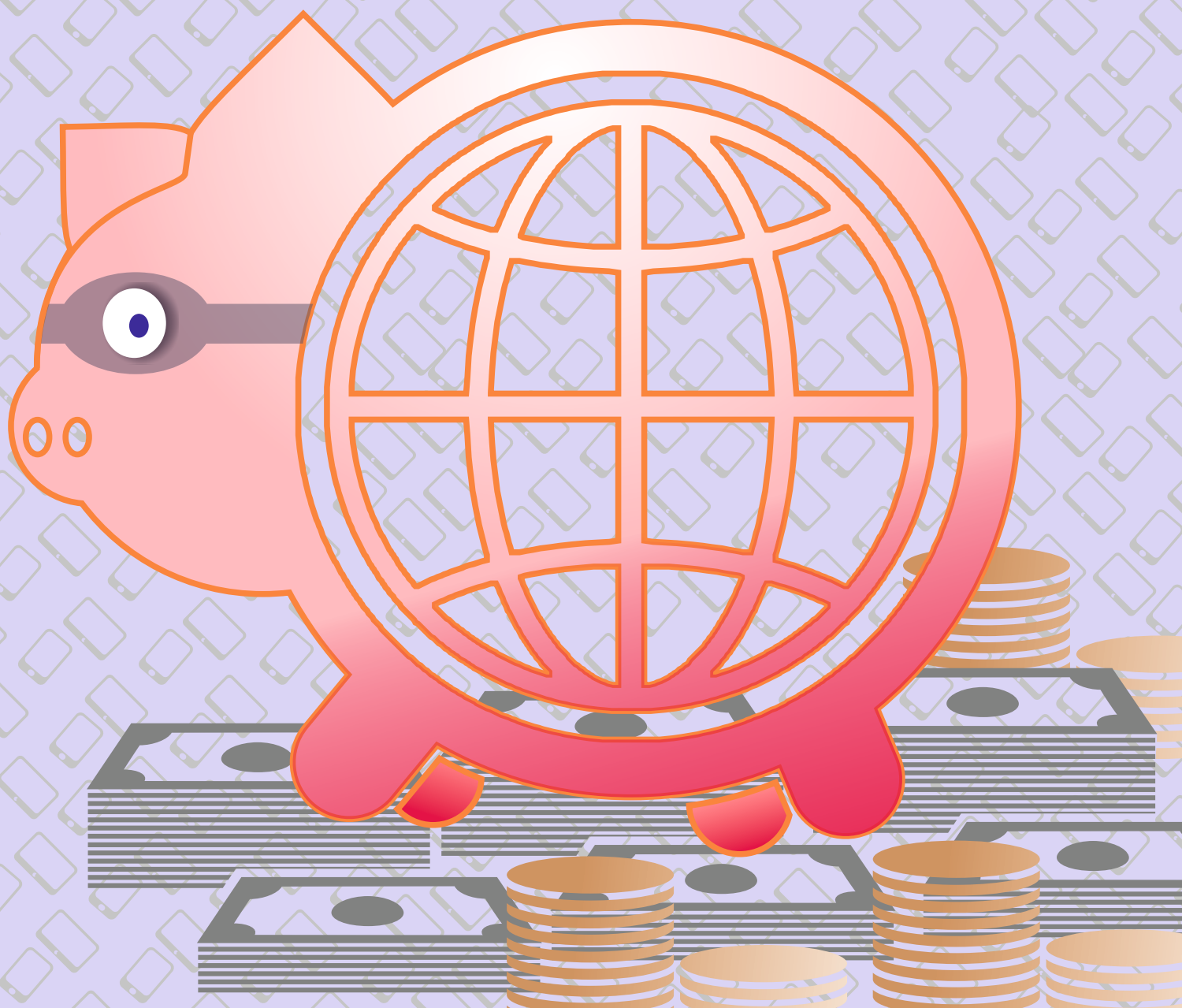


Bezpieczeństwo finansów w Internecie

scenariusz lekcji dla uczniów szkół ponadgimnazjalnych



Autorzy: dr Łukasz Srokowski

Kontakt:

Stowarzyszenie "Miasta w Internecie"

ul. Krakowska 11a

33-100 Tarnów

tel.: +48 14 628 42 10, 688 80 12

fax: +48 14 628 43 11

Artur Krawczyk

tel. +48 502 357 587



Więcej informacji na temat projektu:
CYFROWOBEZPIECZNI.pl - Bezpieczna Szkoła Cyfrowa,
na stronie www.cyfrowobezpieczni.pl



Więcej informacji na temat Stowarzyszenia "Miasta w Internecie"
na stronie www.fabrykaprzyszlosci.pl

Projekt jest współfinansowany przez Ministerstwo Edukacji Narodowej w ramach zadania publicznego "Poprawa kompetencji pracowników szkoły, uczniów i ich rodziców w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz reagowania na zagrożenia"



Uznanie autorstwa-Użycie niekomercyjne-Na tych samych warunkach 3.0 Polska
– Licencja ta pozwala na rozpowszechnianie, przedstawianie i wykonywanie utworu jedynie w celach niekomercyjnych oraz tak długo jak utwory zależne będą również obejmowane tą samą licencją. <http://creativecommons.org/licenses/by-nc-sa/3.0/pl/>

O projekcie Cyfrowobezpieczni.pl

Projekt „Cyfrowobezpieczni.pl – Bezpieczna Szkoła Cyfrowa”, nazywany dalej Cyfrowobezpieczni.pl jest współfinansowany ze środków budżetu państwa otrzymanych od Ministra Edukacji Narodowej w ramach rządowego programu „Bezpieczna +” mającego na celu wspomaganie organów prowadzących szkoły w zapewnianiu bezpiecznych warunków nauki, wychowania i opieki w szkołach w latach 2015-2018.

Projekt ten ma stanowić odpowiedź na problemy związane z coraz silniejszą obecnością technologii cyfrowych w życiu uczniów. Ze względu na bardzo dużą złożoność tego tematu, konieczne było zaplanowanie działań, które będą w systemowy sposób dotykały wszystkich aspektów zetknięcia się świata cyfrowego i polskiej szkoły.

Temat ten ma bowiem co najmniej dwa oblicza. Z jednej strony komputery, smartfony i ciągły dostęp do Internetu prowadzą do pojawiania się wielu zupełnie nowych zagrożeń, na które nie są przygotowane ani dzieci, ani rodzice ani system oświatowy. Z drugiej strony mądre wykorzystywane narzędzi cyfrowych w edukacji może prowadzić do bardzo dobrych efektów: większego zaangażowania uczniów, lepszych wyników edukacyjnych, rozwoju ciekawszego i bardziej aktywizującego środowiska nauki. Obie strony problemu są więc istotne dla szkoły i konieczne jest dobre wyważenie działań, tak aby zabezpieczyć dzieci przed zagrożeniami, a jednocześnie nie zniechęcić ich do korzystania z narzędzi cyfrowych.

Jak wynika z badań socjologów, obecność świata cyfrowego działa jako swoisty „wzmocniacz” dla tego, co dzieje się w szkole. Jeżeli szkoła pracuje dobrze, nauczyciele odpowiednio dobierają metody pracy do potrzeb uczniów i umieją wesprzeć ich w rozwoju, wykorzystywanie narzędzi cyfrowych może wzmocnić efekty pracy szkoły. Jednak, jeżeli między uczniami relacje są złe, oparte na braku empatii i życzliwości, narzędzia cyfrowe mogą być katalizatorem wielu negatywnych zjawisk, takich jak nękanie, izolowanie i agresja rówieśnicza. Tak więc, gdy myślimy o zagrożeniach bezpieczeństwa uczniów, nie same narzędzia cyfrowe są kluczowym problemem, ale zjawiska, które eskalują.

Projekt Cyfrowobezpieczni.pl ma na celu zaproponować szkołom systemowe rozwiązania, które pozwolą lepiej wykorzystywać narzędzia cyfrowe dla wspierania rozwoju uczniów, przy jednoczesnym zapewnieniu dzieciom bezpieczeństwa i nauczaniu ich zasad mądrego korzystania z Internetu i urządzeń cyfrowych.

W ramach projektu:

- *Odbędzie się blisko 2500 spotkań w szkołach, w ramach Szkolnych Dni Bezpieczeństwa Cyfrowego. W trakcie każdego takich Dni będą miały miejsce spotkania z dyrekcją, nauczycielami oraz uczniami, przeprowadzone przez edukatorów projektu.*
- *Zrealizowane zostaną 3 edycje konkursu „Jesteśmy Cyfrowobezpieczni!”, w ramach których szkoły będą mogły wygrać cenne nagrody, w tym pełne wyposażenie nowoczesnej pracowni informatycznej.*
- *Powstaną specjalne punkty konsultacyjne dla dyrektorów szkół, nauczycieli i rodziców.*
- *Odbędą się 3 Ogólnopolskie Konwenty Bezpiecznej Szkoły, na które zaproszeni będą nauczyciele z całej Polski.*
- *Przeprowadzone zostaną szkolenia dla blisko 2500 szkolnych liderów bezpieczeństwa cyfrowego.*
- *Powstanie portal Cyfrowobezpieczni.pl, na którym dostępne będą wszelkie materiały projektowe, w tym 24 scenariusze lekcji dla 4 etapów edukacyjnych, materiały multimedialne i kursy e-learningowe dla nauczycieli.*

Niniejszy scenariusz stanowi więc tylko część szerszego projektu – dlatego też zachęcamy Cię do zapoznania się z pozostałymi materiałami projektowymi, dostępnymi również na portalu **Cyfrowobezpieczni.pl**



Spis treści

Wprowadzenie 2



Scenariusz lekcji

Metody pracy 3

Cel lekcji 3

Efekty kształcenia 4

Do przygotowania przed lekcją 4

Przebieg lekcji 5

Załącznik 1: aplikacje do robienia testów 7



Materiały dodatkowe

Mikropłatności 9

Phishing 10

Dane karty kredytowej i dane logowania do bankowości elektronicznej. 10

Nigeryjski szwindel i inne próby wyłudzeń 12

Korzystanie z internetu w miejscach publicznych 13

Szyfrowanie połączeń – czyli czym różni się http od https 14

Relacje między dziećmi a rodzicami jako najważniejszy bezpiecznik 15

Informacje metodyczne 15

Współpraca z rodzicami 16

Zadania rozwojowe dla nauczyciela 17



Wprowadzenie

Uczniowie na poziomie ponadgimnazjalnym korzystają z Internetu pod bardzo wieloma względami tak samo jak dorośli. Wielu z nich ma już swoje karty kredytowe lub korzysta sprawnie z kart kredytowych rodziców – robią zakupy, płacą przelewami... krótko mówiąc, zarządzają swoimi finansami w Internecie. I w przeciwieństwie do starszych pokoleń najczęściej nie widzą żadnej potrzeby, aby kiedykolwiek wybrać się do placówki banku, skoro wszystkie swoje sprawy mogą załatwić w sieci.



Ta wiara w totalną użyteczność Internetu niestety rzadko idzie w parze z refleksją na temat zagrożeń, związanych z bezpieczeństwem transakcji finansowych robionych online. Tymczasem młodzi użytkownicy bankowości internetowej wcale nie są bardziej bezpieczni niż ich rodzice. Wprawdzie znacznie sprawniej poruszają się w świecie cyfrowym, ale jednocześnie brak im doświadczenia życiowego i świadomości tego, jakie zagrożenia mogą czyhać na nich przy robieniu zakupów przed ekranem komputera.



Temat ten jest dość skomplikowany od strony techniczno-informatycznej – jednak wiedza techniczna nie jest niezbędna do przeprowadzenia tego scenariusza. Do ochrony przed większością zagrożeń, związanych z ryzykiem dla finansów, wystarczy minimalna świadomość tego jak działa przesyłanie informacji przez Internet i zdrowy rozsądek.



Ze względu na fakt, że uczniowie na poziomie ponadgimnazjalnym są bardzo sprawni w korzystaniu z technologii cyfrowych, lekcja ta oparta jest na założeniu, że najwięcej się nauczą na temat bezpieczeństwa swoich finansów, jeżeli dostaną wskazówkę, czego mają się uczyć i narzędzia do tego, by nauka ta była atrakcyjna. W porównaniu do pozostałych lekcji, przedstawionych w tym cyklu scenariuszy, plan zajęć na temat bezpieczeństwa finansowego w sieci daje bardzo dużą dozę wolności uczniom. Rolę nauczyciela kierunkuje zaś na tworzenie ram do pracy i pomoc uczniom w formułowaniu wniosków. Dlatego też warto, aby była to ostatnia lekcja z cyklu wszystkich zajęć prowadzonych na temat cyberbezpieczeństwa, dzięki czemu uczniowie będą już przyzwyczajeni i do tego tematu i do sposobu pracy, bazującego na pracy z technologiami cyfrowymi.

Intencją lekcji, opisanej w tym scenariuszu jest dostarczenie uczniom podstawowej wiedzy na temat zawarty w tytule i zabezpieczenie ich przynajmniej przed najczęściej występującymi zagrożeniami, mogącymi prowadzić do strat finansowych.





Scenariusz lekcji

Lekcja ta została zaprojektowana z myślą o uczniach ostatniej klasy szkół ponadgimnazjalnych, jest jednak także możliwa do zrealizowania w klasach młodszych. W większości wypadków im starsi uczniowie, tym więcej będą mieli własnych doświadczeń, związanych z płatnościami w Internecie. Niektóre wykonywane przez nich operacje i transakcje mogą mieć charakter bardzo podstawowy, ale nie da się wykluczyć, że część uczniów zaczęła korzystać już z zaawansowanych metod płatniczych. Dlatego rekomendujemy przeprowadzanie jej przede wszystkim w starszych klasach.

Lekcja ta zaczyna się od analizy przez uczniów filmu, dostarczonego wraz ze scenariuszem, a następnie opracowaniu w grupach, na jego podstawie, testów, za pomocą których uczniowie będą sprawdzać nawzajem swoją wiedzę.



Metody pracy

Lekcja ma mieć charakter mocno aktywny i bazować na samodzielnej pracy warsztatowej uczniów przygotowujących swoje zadanie w grupach. Podstawową metodą jest metoda projektu edukacyjnego, realizowanego w trakcie lekcji.

Metoda ta jest szczegółowo opisana w dalszej części scenariusza, w sekcji informacje metodyczne.



Cel lekcji



Poznanie przez uczniów najważniejszych zasad korzystania z Internetu w sposób bezpieczny dla ich finansów.



Efekty kształcenia

W zakresie wiedzy:

uczniowie znają najpopularniejsze zagrożenia dla ich pieniędzy w Internecie

uczniowie wiedzą, w jaki sposób bezpiecznie dokonywać transakcji finansowych w Internecie

uczniowie rozumieją mechanizm funkcjonowania mikropłatności

W zakresie umiejętności:

uczniowie umieją rozpoznać próby wyłudzenia od nich danych i pieniędzy

uczniowie potrafią odpowiednio zareagować w przypadku próby wyłudzenia

W zakresie postaw:

uczniowie traktują Internet jako przestrzeń, w której można bezpiecznie dokonywać transakcji finansowych pod warunkiem zachowania odpowiednich środków ostrożności



Do przygotowania przed lekcją

Na lekcji wcześniejszej zapowiedz uczniom, że na następnej godzinie wychowawczej będą przygotowywać testy w Internecie. Poproś ich, aby każdy z nich znalazł w sieci jakieś narzędzie, umożliwiające przygotowanie i przeprowadzenie prostego testu. Możesz im podpowiedzieć narzędzia takie jak: formularze Google, Nearpod, czy Kahoot, możesz także zostawić im dowolność – w zależności od preferowanego przez Ciebie stylu pracy. Bardziej szczegółowy opis przykładowy narzędzi znajduje się w dalszej części dokumentu, w załączniku 1.

Ze względu na to, że lekcja będzie wymagała od uczniów dostępu do Internetu, powinna odbywać się w sali informatycznej – lub też uczniowie muszą mieć w inny sposób zapewnioną możliwość łączenia się z siecią. Mogą także przynieść własny sprzęt, jeżeli szkoła wyraża na to zgodę. Urządzenia, które będą wykorzystywane, powinny mieć możliwość odtwarzania dźwięku – w przypadku komputerów szkolnych może to oznaczać konieczność podłączenia głośników lub słuchawek.

Do niektórych aplikacji, służących do prowadzenia testów, będzie niezbędny rzutnik multimedialny - przygotuj go, jeżeli więc chcesz uczniom umożliwić korzystanie z narzędzi takich jak Plickers czy Kahoot.



Przebieg lekcji

Ze względu na występujące w szkołach różnice w dostępie do sprzętu, proponowany poniżej scenariusz opiera się na założeniu o posiadaniu przez szkołę ilości komputerów równą jednej czwartej liczby uczniów w klasie. Jeżeli Wasza szkoła dysponuje większą ilością sprzętu, możecie odpowiednio modyfikować konspekt, zmniejszając na przykład liczebność grup i zwiększając ich liczbę. Dodatkowo, jeżeli w szkole korzystacie z narzędzia takiego, jak Google Drive lub innego rozwiązania chmurowego, warto zmodyfikować scenariusz tak, by w pełni wykorzystywał te możliwości.



5 min.

Sprawy organizacyjne

- 1 Sprawdzenie obecności.
- 2 Inne sprawy organizacyjne.



2 min.

- 3 Zapytaj uczniów, czy któryś z nich płacił kiedykolwiek za coś w Internecie. Spytaj tych, którzy się zgłoszą, za co płacili (bez podawania kwot).
- 4 Powiedz, że dzisiaj zajęcia poświęcone będą bezpieczeństwu finansów w Internecie.



20 min.

- 5 Połącz uczniów w grupy, liczące sobie po 4 osoby.
- 6 Wyświetl na rzutniku adres, pod którym dostępny jest film, dołączony do tego scenariusza.
- 7 Powiedz uczniom, że ich zadaniem będzie obejrzeć film w całości i przygotować test, za pomocą którego sprawdzą wiedzę swoich kolegów na temat tego, co było przedstawione w filmie.
- 8 Każda grupa ma przygotować jeden test, który będzie dostępny przez Internet dla innych uczniów. Każda grupa może korzystać z innego narzędzia do robienia testów, mogą też wszyscy zastosować to samo narzędzie.
- 9 Powiedz też, że na koniec lekcji będą oceniali testy opracowane przez inne grupy.
- 10 Daj grupom 20 minut na to, aby obejrzeli film i przygotowali w wybranym przez siebie narzędziu test.



15
min.

11

Gdy skończą, powiedz, aby każda grupa wysłała link do swojego testu co najmniej dwóm innym grupom (w mniej licznych klasach mogą wysłać do wszystkich kolegów).

12

Daj uczniom dziesięć minut na testowanie się nawzajem.

13

Zapytaj o wrażenia z testów. Możesz poprosić teraz o to, by każda grupa podeszła do grup, których testy wypełniała i dała im informację zwrotną na temat tego, jak im się podobał test, czy był trudny i czy sobie poradzili z jego rozwiązaniem. W klasie zapewne zapanuje spory harmider, ale w tym wypadku jest to akceptowalne.



3
min.

Podsumowanie

14

Podsumuj lekcję, zwracając im uwagę na jeden podstawowy wniosek:

Przez Internet można robić różne transakcje finansowe, trzeba jednak zachować przy tym odpowiednią ostrożność.



Załącznik 1: Aplikacje do robienia testów

W Internecie dostępnych jest bardzo wiele narzędzi, mogących służyć do tworzenia i przeprowadzania testów. Większość z nich jest bardzo prosta w obsłudze. Poniżej wymieniamy trzy, jednak wystarczy Ci chwila spędzona z wyszukiwarką, by znaleźć ich znacznie więcej.

Formularze Google

W ramach dysku Google, możliwe jest tworzenie formularzy, mających charakter ankiet lub testów. Aby z nich skorzystać, niezbędne jest posiadanie bezpłatnego konta Google.

Formularz bez nazwy

Opis formularza

Tytuł pytania:

Tekst pomocy:

Typ pytania: Wybierz z listy Przejdź do strony w oparciu o odpowiedź

1.

2.

Wymagane

Kahoot

Prosta aplikacja sieciowa, pozwalająca na przygotowywanie testów z pytaniami, na które uczestnicy mogą łatwo odpowiadać na telefonach komórkowych. Aby stworzyć test, należy wejść na stronę www.getkahoot.com, a by wypełnić test, stworzony przez kogoś, na adres www.kahoot.it. W serwisie Youtube po wpisaniu hasła Kahoot możesz znaleźć szereg filmów instruktażowych, pokazujących krok po kroku, jak przygotować test.

Q1 What does the digestive system do?

6

Next

0 Answers

Breaks down and handles food

Pumps blood throughout the body

Helps you breathe

Helps your arms and legs move

Plickers

Bardzo oryginalne narzędzie testowe, pozwalające na przeprowadzenie sprawdzianu za pomocą telefonu komórkowego i wydrukowanych, na podstawie wzoru ze strony, kartek z kodami podobnymi do kreskowych. Prowadzący test wyświetla pytanie na rzutniku, a uczniowie podnoszą w odpowiedzi kartki. W zależności od tego, w którą stronę obróć kartkę, oznaczać to będzie wybór odpowiedzi A, B, C lub D. Prowadzący test kieruje następnie w stronę klasy obiektyw aparatu w telefonie komórkowym, a tam specjalna aplikacja odczytuje odpowiedzi i wyświetla na rzutniku informacje, którzy uczniowie odpowiedzieli na pytania poprawnie, a którzy nie.



Getting Started:

www.plickers.com



Sign Up for an Account

Download the App



Oprócz tych trzech, zupełnie różnych narzędzi, dostępnych w Internecie aplikacji do testowania jest znacznie więcej. Ważne jest, abyś przed przeprowadzeniem tej lekcji poinformował uczniów, że będą mieli za zadanie opracować test i że powinni przygotować się do tego, ucząc się obsługi wybranej aplikacji lub narzędzia. Uprzedź, że w przypadku wyboru aplikacji Plickers powinni wydrukować przed lekcją karty z kodami, a w przypadku Kahoota muszą upewnić się, czy wszyscy ich koledzy będą mieli do dyspozycji urządzenie z dostępem do Internetu, by odpowiedzieć. Jeżeli zaś wybiorą jakąś inną aplikację lub narzędzie, powinni upewnić się, że umieją je obsługiwać i że zadziała bez problemu w trakcie lekcji.



Mikropłatności

Producenci gier na komputery, tablety i inne urządzenia cyfrowe wymyślili w ostatnich latach nowy sposób na zarabianie. Większość gier dostępnych na przykład na telefony komórkowe jest możliwa do ściągnięcia bezpłatnie. Gracz może zacząć grać i do pewnego poziomu bawić się, nie wydając ani grosza. W pewnym momencie gra robi się jednak dość skomplikowana i, by przejść dalej albo pokonać przeciwnika, trzeba uruchomić jakieś ulepszenie. A to jest już płatne. Niewiele, zwykle kilkadziesiąt groszy, rzadko kilka złotych. Mikropłatności są dostępne za pomocą jednego przycisku i po kliknięciu „kup” można kontynuować grę z silniejszym bohaterem, mającym większe szanse na wygraną.

Od strony psychologicznej, producenci gier wykorzystują tutaj wszystkie możliwe mechanizmy, aby rozmyć świadomość użytkownika, że w ogóle wydaje jakieś pieniądze. Najczęściej dokonując zakupu nie kupujemy bezpośrednio ulepszenia (np. pozwalającego naszemu bohaterowi poruszać się szybciej), ale jakąś formę wewnętrznej waluty gry – na przykład kilka złotych monet. A dopiero te złote monety wymieniamy na ulepszenia. W efekcie korzyść z wydanych pieniędzy jest rozłożona na dłuższy czas i przypomina bardziej obrót walutą niż zakupy. Rzecz jasna, waluty wewnętrznej w grze nie możemy już wymienić z powrotem na prawdziwe pieniądze – transakcja jest jednostronna.

Drugi wykorzystywany mechanizm to owo miękkie wymuszanie. Zakup nie jest niezbędny. Nie ma jakiegoś konkretnego momentu, w którym gracz musi podjąć decyzję: dalej nie gram, bo musiałbym zapłacić. Jest to świadoma strategia producentów gier, którzy wiedzą, że wielu graczy w takiej sytuacji po prostu zrezygnowałoby z gry. Nie chcą więc wymuszać na nich decyzji typu płacę albo nie gram – pozwalają grać bardzo długo bez mikropłatności, przy czym gracz chcący radzić sobie bezpłatnie, coraz rzadziej osiąga sukces w grze. Zainwestowanie nawet złotówki pozwala natychmiast przejść kolejny poziom, dostarczając odpowiedniej korzyści psychologicznej i zachęcając gracza do dokonania kolejnych zakupów.

Mikropłatności najbardziej popularne są w grach na urządzenia przenośne – smartfony i tablety. Tradycyjne gry komputerowe, czy konsolowe nadal w zdecydowanej większości działają na zasadzie jednego zakupu, robionego na początku. Jednak i do nich powoli zaczynają wkradać się mikropłatności i niewykluczone, że wkrótce opanują wszystkie obszary rozrywki cyfrowej.



Phishing

Jednym ze sposobów w jaki złodzieje mogą wykraść dane logowania jest tzw. phishing. Oznacza to wyłudzenie danych logowania poprzez podszywanie się pod jakąś oficjalną instytucję, np. bank. Zwykle ofiara manipulacji otrzymuje wiadomość wyglądającą jak wysłana z jej banku. W wiadomości pojawia się na przykład informacja o konieczności zresetowania hasła ze względów bezpieczeństwa i link do strony. Gdy odbiorca takiego maila kliknie link, wejdzie na stronę łudząco podobną do strony jego banku, na której będzie mógł podać swoje dane.

Istotą phishingu jest fakt, że strona jest jednak fałszywa i nie należy do banku. Adres www może być bardzo podobny – np. ze zmienioną jedną literą, sama strona również zostaje wystylizowana tak, by wyglądać dokładnie tak samo, jak strona prawdziwej instytucji. Gdy jednak ofiara wpisze swoje dane logowania, są one natychmiast przekazywane złodziejom, którzy za ich pomocą mogą zalogować się już do prawdziwego banku.

Aby obronić się przed phishingiem:

- ▶ Należy pamiętać, że niemal żadna instytucja nie wysyła maili, w których żąda podania na nowo swojego hasła.
- ▶ Patrzeć uważnie na adresy banków i innych instytucji, jeżeli wchodzimy na ich stronę z linków przysłanych pocztą lub np.. komunikatorem.
- ▶ Jeżeli już wejdziemy na fałszywy adres i nie zorientujemy się na czas, należy natychmiast skontaktować się z instytucją, pod którą podszywają się złodzieje i zgłosić sytuację – dostaniemy wówczas instrukcje, co zrobić i jak zabezpieczyć się przed utratą pieniędzy.



Dane karty kredytowej i dane logowania do bankowości elektronicznej

Karty kredytowe kiedyś były symbolem luksusu, dostępnego tylko najbogatszym. Dzisiaj, ze względu na politykę banków, ma je coraz więcej Polaków. A już zdecydowana większość rodzin posiada przynajmniej jedną kartę debetową, pozwalającą płacić w sklepach za zakupy czy wypłacać pieniądze z bankomatu.

Kartą wydaną przez bank można płacić także za zakupy robione przez Internet. Niektóre sklepy akceptują wyłącznie karty kredytowe, ale w coraz większej ilości miejsc można zapłacić także innymi rodzajami karty (np. debetową lub przedpłaconą). Coraz częściej można także robić zakupy po prostu za pomocą

przelewu internetowego. Wymaga to od nas jedynie kliknięcia odpowiedniej opcji podczas robienia zakupów, postępowanie zgodnie ze wskazówkami na ekranie i z reguły podania kodu, który przyjdzie smsem z banku, albo który mamy na jednorazowej karcie kodów.

W zdecydowanej większości transakcje takie są bezpieczne i nie grożą nam żadnymi negatywnymi konsekwencjami. Musimy mieć jednak świadomość występowania także kilku różnych rodzajów zagrożeń, związanych ze zdobyciem przez złodziei naszych danych.

Podanie naszych danych karty kredytowej osobom nieuprawnionym

Należy uważać na jakiegokolwiek próby wyłudzenia danych naszej karty, na przykład za pomocą maila, takiego jak we wcześniejszych przykładach, lub wpisania jej na niezabezpieczonych stronach. W przeciwieństwie do rachunku bankowego, który do zrobienia przelewu wymaga jeszcze potwierdzenia hasłem sms, dane karty kredytowej samodzielnie wystarczą do dokonania płatności. Tak więc, jeżeli ktoś zrobiłby zdjęcie obydwu stron naszej karty kredytowej, jest w stanie za pomocą tych danych płacić w naszym imieniu.

Wirusy zmieniające numer konta

Obecnie istnieje kilka wirusów, które mogą podmienić numer konta podczas robienia transakcji bankowej. Użytkownik może nie być nawet świadomy tego, że wpisuje numer konta osoby, której chce przelać pieniądze, a wirus w ostatniej chwili podmienia ten numer i środki trafiają na obce konto. Najsprytniejsze wersje tego oszustwa prezentują właściwy numer przez cały czas, a jedynym sposobem zorientowania się w sytuacji jest dokładne sprawdzenie numeru konta w potwierdzeniu, które bank przyśle nam smsem – lub też, które zostanie wyświetlone w podsumowaniu transakcji. No i oczywiście niezbędny jest dobry program antywirusowy.

Podanie komuś loginu i hasła do naszego profilu, na którym są dane karty

W wypadkach niektórych profili tworzonych w Internecie (np. przy rejestracji na urządzenia firmy Apple czy smartfony i tablety z Androidem) konieczne jest podanie danych swojej karty kredytowej, nawet jeżeli nie planujemy robić na nim żadnych zakupów. Jest to wymagane niejako „na zapas” – bez tego, nie da się korzystać z wielu funkcji urządzenia. Dane naszej karty są więc zapisane w urządzeniu na stałe. Jeżeli ktoś przejmie nasze hasło do logowania się na koncie Google (które jest tożsame z kontem na Androidzie) lub hasło do konta Apple (na wszystkie urządzenia takie jak iPhone, iPad i komputery tego producenta), będzie mógł z niego dokonywać różnych zakupów. Nie przejmie wprawdzie danych naszej karty, są one bowiem zabezpieczone, ale w naszym imieniu może wydać dużą ilość pieniędzy.



Nigeryjski szwindel i inne próby wyłudzeń

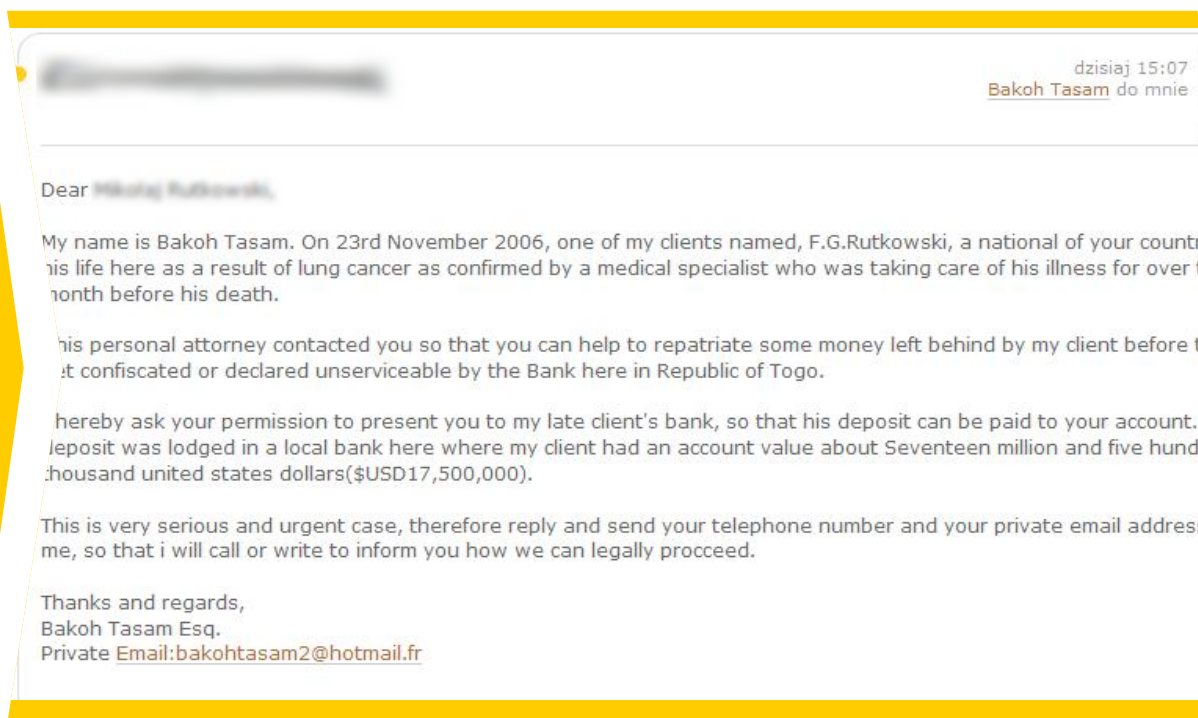
We wczesnych latach Internetu bardzo popularne były tzw. nigeryjskie przekręty. Był to mało wyrafinowany model oszustwa, na który jednak nabierała się część odbiorców. Proceder ten polegał na wysłaniu masowo maili z prośbą o pomoc w trudnej sytuacji. Przekręt robił na większości użytkowników dość komiczne wyrażenie, ponieważ mail napisany był z licznymi błędami językowymi i ortograficznymi i na pierwszy rzut oka budził mógł podejrzenia. Nadawcą maila miał być nigeryjski książę, pozbawiony przez zamach stanu możliwości wybrania z banku posiadanych tam pieniędzy w wysokości kilku milionów dolarów. Zwracał się on do odbiorcy maila z prośbą o pomoc w przetransferowaniu tych pieniędzy do bezpiecznego kraju i obiecywał odwdziżyć się okazałą częścią majątku.

Jeżeli odbiorca odpisał, rozpoczynała się korespondencja, w ramach której odbiorca poznawał kolejne szczegóły sytuacji „księcia”, pozyskującego stopniowo zaufanie swojej ofiary. W końcu złodziej prosił o pomoc i przelewanie niewielkiej kwoty (np. kilku dolarów) na przelew bankowy, za pomocą którego przesłane miały być te miliony. Potem okazywała się konieczna kolejna płatność, tym razem na potrzeby organizacji wyjazdu księcia, lub na łapówki strażników w obozie, w którym osadzony jest „książę”. Przekręt trwał tak długo, jak długo naiwna ofiara gotowa była płacić coraz to większe kwoty. Jeżeli natomiast odbiorca w którymś momencie zbuntował się i postanowił przerwać płacenie, „książę” zniknął, razem ze wszystkimi wpłaconymi dotąd pieniędzmi.

Przekręt ten ma wiele różnych wersji. W niektórych odzywa się nie nigeryjski książę, a księżniczka, albo też uchodźca polityczny z innego kraju. Łączy te wszystkie próby wyłudzeń ten sam mechanizm, a także sposób napisania pierwszej wiadomości – z reguły bardzo słabym angielskim (czasami, rzadziej wiadomości są tłumaczone na polski). Co ciekawe, niektórzy eksperci twierdzą, że pierwsza wiadomość ma celowo tak bardzo naiwny charakter. Jej założeniem jest bowiem odsiać na samym początku zbyt domyślnych odbiorców, którzy i tak by zrezygnowali na dalszym etapie kontaktu. Ci, którzy uwierzą w bardzo naciąganą historię będą prawdopodobnie bardziej skłonni do zrobienia przelewu złodziejom.

Bardziej wyrafinowane wersje nigeryjskiego szwindlu opierają się na wysłaniu wiadomości o spadku od krewnego, o takim samym nazwisku jak potencjalna ofiara przekrętu. Potem mechanizm jest taki sam: potrzebne są pieniądze na koszty organizacyjne, związane ze zrobieniem przelewu, które trzeba wpłacić na podane konto. Rzecz jasna, żaden spadek nigdy nie dociera na konto osoby, która uwierzy w taką wiadomość, a złodziei próżno szukać, ponieważ zarówno rachunki bankowe jak i konta mailowe zarejestrowane są zwykle w krajach, w których będzie trudno złapać oszustów.

Mimo więc, że sam mechanizm jest dość banalny, warto ostrzec przed nim uczniów, nie jest bowiem wykluczone, że niektórzy z nich mogą się dać na to nabrać – teraz lub w przyszłości.



Rys. 1: przykładowa wiadomość, rozpoczynając nigeryjski szwindel, tym razem za pomocą portalu społecznościowego.

Źródło: <http://www.fraudiq.eu/2010/przekret-419-czyli-szwidnel-nigeryjski.html>



Korzystanie z Internetu w miejscach publicznych

W coraz większej ilości miejsc dostępne są dzisiaj sieci bezprzewodowe, z których możemy skorzystać, by połączyć się z Internetem za pomocą telefonu komórkowego czy komputera. W restauracji, urzędzie miejskim, galerii handlowej – wszędzie, na naszym komputerze, może pojawić się ikonka wi-fi, czyli sieci bezprzewodowej.

Musimy mieć jednak świadomość, że sieci publiczne, a zwłaszcza sieci publiczne nie wymagające hasła są znacznie mniej bezpieczne niż nasza sieć domowa, do której dostęp mają tylko członkowie rodziny. Warto więc powstrzymać się od wykorzystywania takich sieci do robienia przelewów bankowych czy jakichkolwiek innych operacji finansowych.

Co więcej, zdarzają się oszuści, którzy tworzą ogólnodostępne sieci wi-fi właśnie po to, by wyciągnąć dane od osób, które zwabione bezpłatnym dostępem do Internetu zalogują się do nich.

Warto więc powiedzieć uczniom, aby korzystając z publicznie dostępnych sieci, pamiętali o tym, że:

- ▶ Jeżeli sieć ta jest dostępna publicznie i każdy może się do niej zalogować, nie powinni wykonywać na niej żadnych operacji wymagającej danych wrażliwych, takich jak numer konta, login i hasło do banku czy numer karty kredytowej.
- ▶ Jeżeli nie znają sieci i nie wiedzą, kto jest jej administratorem, lepiej się z nią nie łączyć. Nie oznacza to oczywiście, że administratora trzeba znać osobiście. Można założyć, że sieci w lokalizacjach takich jak kawiarnie, czy galerie handlowe są prowadzone przez instytucje bez złych intencji. Jeżeli jednak w miejscu publicznym zobaczymy sieć o nieznanym nazwie, której nie potrafimy powiązać z żadną lokalną restauracją czy inną instytucją, najbezpieczniej będzie się z nią nie łączyć.

Istnieją aplikacje i programy, które pozwalają zabezpieczyć się dodatkowo, właśnie na wypadek korzystania z sieci publicznych. Są to najczęściej dodatki do programów antywirusowych. Jeżeli więc ktoś często korzysta z niezabezpieczonego wi-fi, a jednocześnie wykonuje za jego pomocą różne transakcje płatnicze, zainwestowanie w taki program może być dobrym rozwiązaniem.



Szyfrowanie połączeń – czyli czym różni się http od https

Często, przy wchodzeniu na jakąś stronę możemy zobaczyć przed jej adresem literki http lub też https. Owo „s” na końcu ma duże znaczenie – pochodzi od słowa „secure”, czyli bezpieczny i oznacza, że połączenie z daną stroną jest szyfrowane. Oznaczenie takie mają banki i wiele sklepów internetowych, a także część portali społecznościowych, do których logujemy się za pomocą hasła (np. Facebook). Oczywiście zabezpieczenie takie nie gwarantuje, że nasze dane na pewno nie zostaną w żaden sposób wykradzione, ale znacząco zmniejsza prawdopodobieństwo takiego zdarzenia.

Warto więc pamiętać, by nie robić żadnych operacji związanych z płatnościami, jeżeli jesteśmy na stronie rozpoczynającej się od http, a nie od https.



Relacje między dziećmi a rodzicami jako najważniejszy bezpiecznik

W większości wypadków dzieci kupując różne rzeczy w Internecie korzystają z pieniędzy rodziców. Nawet w przypadku starszych nastolatków, często ich własne zarobki łączone są z jakąś formą kieszonkowego od rodziców. To powoduje, że w mniejszym stopniu niż dorośli doceniają wartość pieniędzy i nie przejmują się aż tak bardzo zabezpieczeniem ich przed utratą.

Tak, jak i w przypadku innych tematów, jednym z najważniejszych elementów, niezbędnych do zachowania bezpieczeństwa przy korzystaniu z narzędzi cyfrowych są dobre, autentyczne relacje pomiędzy rodzicami i dziećmi. Potrzebna jest zwłaszcza szczerza rozmowa na temat tego, na co rodzinę stać, a na co nie – dzieci bardziej świadome stanu domowych finansów będą rozsądniej rozporządzać pieniędzmi w sieci.

Pieniądze są z pewnością trudnym tematem do rozmowy. Każda rodzina rozstrzyga po swoim, jak chce o nich mówić swoim dzieciom. Niezależnie jednak od szczegółowych rozwiązań, ważnym elementem w budowaniu w dzieciach nawyków świadomego i bezpiecznego korzystania z internetowych transakcji jest rozmowa na ten temat z rodzicami.



Informacje metodyczne

Podstawową metodą, wykorzystywaną w trakcie lekcji będzie metoda projektu. W tym wypadku opiera się ona na opracowaniu przez grupę uczniów samodzielnie stworzonego testu, który następnie będzie wykorzystywany przez autorów do sprawdzania wiedzy kolegów i koleżanek z innych grup.

W ten sposób każda grupa uczniów będą jednocześnie testującymi i testowanymi – zdobywając wiedzę w obydwu rolach. Zgodnie ze starą zasadą edukacyjną, najwięcej uczymy się, nauczając innych – a można też dodać, że niewiele mniej, sprawdzając ich wiedzę. Dlatego grupy, opracowując testy będą musiały jednocześnie przygotować się do ich wypełniania i dzięki temu będą cały czas aktywizowały i wywoływały z pamięci informacje zawarte w filmie, dzięki temu bardzo mocno je zapamiętując.

Takie zastosowanie metody projektu opiera się na założeniu, że aby miał on charakter edukacyjny, w jego trakcie uczniowie muszą nauczyć się czegoś nowego, bez czego nie będą w stanie wykonać projektu. W ten sposób nauka dzieje się niejako przy okazji, pod pretekstem wykonywania zadania.



Współpraca z rodzicami

Tak, jak wspomniano we wcześniejszych elementach, rodzice i ich dobre relacje z dziećmi są najważniejsze dla zapewnienia bezpieczeństwa dzieci w kontakcie z technologią. Dlatego też warto zaangażować rodziców w ten temat i zapewnić współpracę na takim poziomie na jakim będzie ona możliwa.

Większość rodziców ma świadomość tego, że nie wszystkie transakcje, robione w Internecie są bezpieczne. Wielu z nich słyszało także o zagrożeniach, związanych z wyłudzeniami i próbami oszustwa. Dlatego też są w stanie przekazać dzieciom wiele wiedzy i doświadczeń. Rekomendujemy więc następujący sposób włączania rodziców w zapewnienia cyberbezpieczeństwa w tym obszarze:

1

Powiedz rodzicom o tym, że odbyła się lekcja opisana w niniejszym scenariuszu

Jeżeli jeszcze nie zdają sobie z tego sprawy, uświadomi im to, że problem ten może być już ważny dla ich dzieci. Możesz opowiedzieć o tym, co robiliście w ramach zajęć, a także podzielić się swoimi wnioskami i spostrzeżeniami, wyciągniętymi na podstawie wypowiedzi dzieci.

2

Zaangażuj rodziców

Jeżeli wśród rodziców znajdzie się ktoś, kto ma odpowiednie przygotowanie do pracy z uczniami na taki temat (np. informatyk, pracownik działu bezpieczeństwa w jakiejś instytucji finansowej) być może także mógłby przeprowadzić jakieś warsztaty na ten temat i porozmawiać z dziećmi. Rodzice często mogą wiele zaoferować szkole, jeżeli tylko da się im taką możliwość.

3

Jeżeli korzystacie z maila, możesz wysłać także rodzicom link do filmu, który obejrzeliby uczniowie

Jest on dostępny w ramach platformy projektu Cyfrowobezpieczni.pl. Możesz wysłać im także inne materiały, które uznasz za wartościowe.

4

Zadaj rodzicom zadanie domowe

Rozmowę ze swoimi dziećmi na temat tego, co działo się na lekcji, a także na temat tego, jakie transakcje robią w Internecie i czy umieją je przeprowadzić bezpiecznie.



Zadania rozwojowe dla nauczyciela i literatura dodatkowa

Dla lepszego zrozumienia omawianego tematu, możesz wykonać jedno lub więcej spośród następujących zadań:

- 1 Porozmawiaj ze swoimi dziećmi lub z uczniami na temat mikroplątności – poproś ich, aby pokazali Ci jakąś grę, w której pojawiają się mikroplątności i wyjaśnili, do czego są potrzebne.
- 2 Jeżeli w szkole macie założone wi-fi dostępne dla uczniów, porozmawiaj z osobą odpowiedzialną za dostęp do Internetu w szkole (np. nauczycielem informatyki lub szkolnym informatykiem) na temat jego zabezpieczeń przed ewentualnymi próbami włamania.
- 3 Wyszukaj w Internecie co najmniej dwa artykuły prasowe na temat serwisu Pobieraczek.pl – opowiedz historię serwisu uczniom podczas tej lub następnej godziny wychowawczej.
- 4 Załóż konto na wybranym narzędziu do prowadzenia testów i naucz się jego obsługi. Użyj go do przeprowadzenia testu na innej lekcji, np. w ramach swojego przedmiotu.



A series of horizontal lines for writing notes, consisting of 25 evenly spaced lines extending across the page.



cyfrowobezpieczni.pl

BEZPIECZNA SZKOŁA CYFROWA