Warsztaty uczniowskie „BEZPIECZNI W FINANSACH OSOBISTYCH”

Temat**: Ochrona danych i pieniędzy przed cyberzagrożeniami. Jakie konsekwencje finansowe niesie kradzież tożsamości?**

Czas zajęć: 45 minut

Efekty zajęć: Poznanie cyberzagrożeń. Konsekwencje finansowe kradzieży tożsamości. Jak zapobiegać kradzieży tożsamości.

Cel ogólny: Ochrona danych i pieniędzy przed cyberzagrożeniami.

Cele szczegółowe: Poznanie cyberzagrożeń. Konsekwencje finansowe kradzieży tożsamości. Jak zapobiegać kradzieży tożsamości.

Materiały pomocnicze: Prezentacja, studium przypadku, KODEKS CYBERBEZPIECZEŃSTWA

Metody nauczania: Studium przypadku „Kradzież tożsamości” , analiza przypadku i poznanie sposobów na odzyskanie tożsamości.

Formy realizacji: Studium przypadku, wykład w formie prezentacji.

Część organizacyjna: Sprawdzenie obecności

Część wprowadzająca: Zapoznanie uczestników z celem zajęć. Krótka prezentacja o cyberzagrożeniach, w tym o kradzieży tożsamości. Jolanta Nakonieczna przedstawia prezentację.

Paulina Cybul odczytuje przypadek w którym dochodzi do kradzieży tożsamości. Prezentowany jest przypadek z życia wzięty o Kradzieży tożsamości.

Paulina,

Siedziałam w długach, które zaczęły się od karty kredytowej. O ile karta kredytowa jest OK, kiedy ma się pieniądze, to przestaje być OK, kiedy traci się pracę a karta kredytowa zostaje. Pracę znalazłam, ale rosnący w błyskawicznym tempie (mimo spłacania) dług został. Postanowiłam coś z tym zrobić i tak trafiłam na kurs Pokonaj swoje długi Michała z jakoszczędzaćpieniądze.pl. Jednym z pomysłów na dodatkowe pieniądze było znalezienie dodatkowej pracy.
Pomyślałam o czymś najłatwiejszym przy pracy na cały etat, czyli pracy przez internet. Zaczęłam przeglądać portale z ofertami pracy, znalazłam kilka ogłoszeń, wysłałam CV. Dostałam odpowiedź z jednego miejsca, że super, że przesyłają kwestionariusz do umowy, że niedługo będzie szkolenie i mogę zacząć pracę. Aha, muszę jeszcze tylko zrobić przelew na kwotę 1 zł, żeby mieli pewność, że podałam właściwy rachunek do wysyłania wynagrodzenia.
Teraz wiem, że to była najgłupsza rzecz, jaką mogłam zrobić. Ten przelew. Ale wtedy tak bardzo się cieszyłam, że znalazłam pracę i wreszcie skończą się moje problemy finansowe, że całkowicie odłączyła mi się zdolność logicznego myślenia i… Zrobiłam ten przelew. Tego samego dnia przyszła umowa (podpisana i zeskanowana), którą powinnam podpisać i im odesłać.
Jakiś czas zajmowałam się w pracy HR i administracją, więc dokładnie wczytałam się w umowę (całe 2/3 strony A4) i znalazłam tyle nieścisłości, błędów i powtórzeń, że napisałam maila z pytaniami o kilka punktów. Gdyby oszust – nie bójmy się nazywać rzeczy po imieniu – postarał się bardziej i zadbał o profesjonalny wygląd umowy, wiem, że podpisałabym ten papier i tym samym udostępniłabym mój podpis. Ale tego nie zrobiłam.
Kiedy po dwóch dniach i kilku wysłanych mailach nie dostałam żadnej odpowiedzi, zorientowałam się, że coś jest nie tak. Zaczęłam szukać informacji na ten temat w internecie i znalazłam kilka wywiadów z osobami, których dane zostały wykradzione dokładnie w ten sam sposób. Jedyne o czym pomyślałam, to zgłoszenie sprawy na policji. Jeszcze tego samego dnia poszłam na najbliższy posterunek i usłyszałam, że… Dopóki moje dane nie zostaną użyte, oni nawet nie przyjmą moich zeznań.
W tym całym stresie, że ledwo udało mi się spłacić całość długu z karty kredytowej, to zaraz obudzę się z kilkumilionowym kredytem zaciągniętym przez kogoś na moje dane, zupełnie zapomniałam, czytamy o pewnej rzeczy (żeby zastrzec numer dowodu osobistego). Co lepsze, nie przeszło to przez myśl nawet funkcjonariuszce,

która odmówiła przyjęcia moich zeznań i odesłała mnie do domu z kwitkiem, bo jeszcze nikt moimi danymi się nie posłużył. Posłużył się nimi miesiąc później.

Odebrałam wiadomość na Facebooku oskarżającą mnie o oszustwo. Na początku pomyślałam, że ktoś robi sobie głupie żarty, ale im dłużej rozmawiałam z tą osobą, tym bardziej wyraźnie docierało do mnie, że kradzież mojej tożsamości stała się faktem i dopiero teraz moje zeznania będą przyjęte. Zebrałam wszystkie informacje o moich działaniach, począwszy od wysłania CV oraz informacje, które mogą pomóc w namierzeniu oszusta.

Dopiero podczas tych zeznań funkcjonariusz zadał mi pytanie, czy zablokowałam dowód osobisty. Zablokowałam go zaraz po zakończeniu zeznań. Wcześniej prześledziłam historię przelewów na konta założone na moje dane, począwszy od tego konta, którego założenie nieświadomie potwierdziłam przelewem 1 zł. Udało mi się dotrzeć do 4 banków. Zamknęłam w nich konta przedstawiając zaświadczenie z policji. W jednym uzyskałam również historię rachunku, która pokazywała kolejne ruchy oszusta, czym uzupełniłam moje zeznania. Wysłałam też informacje do kilkudziesięciu firm udzielających chwilówek, że ktoś może chcieć wziąć kredyt posługując się moimi danymi.

Kilka miesięcy później dostałam wezwanie na przesłuchanie w sprawie kolejnego oszustwa, w którym pojawiły się moje dane osobowe (a dokładnie tylko imię i nazwisko). W trakcie tego przesłuchania zobaczyłam potwierdzenie wykonania przelewu – oczywiście podrobione – na którym rzeczywiście było moje imię i nazwisko. Ale nie zgadzał się ani adres, ani PESEL, ani tym bardziej numer konta. Identycznie przebiegały kolejne dwa przesłuchania (oddalone od siebie w czasie o kilka miesięcy), powodem których były dokładnie takie same oszustwa ludzi z całej Polski.

OSZUST DZIAŁA NA ALLEGRO

Dlatego jeśli macie zamiar kupić drogą rzecz (thermomix był wymieniany najczęściej) lub cokolwiek, co przekracza kwotę, którą moglibyście wyrzucić do kosza, to dokonujcie płatności przez wewnętrzny system Allegro, nigdy bezpośrednio na rachunek podany w treści oferty – nie dajcie się oszukać. I koniecznie zgłoście takiego sprzedającego.

Nie wiem, co policja robi z moimi zeznaniami. Ktoś kiedyś musiał wypłacić te pieniądze a najłatwiej do tego dojść śledząc całą historię rachunków, które były widoczne na dostarczonym przeze mnie wyciągu z zamkniętego konta, które ktoś otworzył posługując się moimi danymi osobowymi. Kilka przelewów szło za pośrednictwem firmy Blue Media i jeden na konto (założone – a jakże – na moje dane) w kantorze internetowym Cinkciarz.

Wczoraj dostałam kolejne wezwanie. Ty razem robi się poważniej, bo muszę jechać na koniec Polski na wezwanie wydane przez prokuratora. Tradycyjnie – oszustwa przez Allegro potwierdzone podrabianymi potwierdzeniami przelewu, na których widnieje moje imię i nazwisko. Zaczynam się bać o swoją przyszłość i przy okazji coraz bardziej wątpić w skuteczność pracy policji. Poza mówieniem prawdy, nie mogę zrobić nic innego.

Uczcie się na moich błędach i bądźcie mega ostrożni, bo od wczoraj stres zdominował moje życie.

Paula

Część właściwa: Analiza przypadku. Uczniom zadawane są pytania analizujące dany przypadek, uczestnicy warsztatów starają się dokonać odpowiedzi na zadawane pytania (poprzez wybieranie odpowiedzi – karty odpowiedzi przygotowane na stoliku):

1. Co to jest cyberatak i jaki wystąpił w tym przykładzie?
2. Jaki pierwszy błąd popełniła Paulina?
3. Jaki kolejny błąd popełniła?
4. Czego nie zrobiła Paulina, aby uniknąć tego błędu?
5. Co należy zrobić, aby uniknąć kradzieży tożsamości?
6. Co należy zrobić aby odzyskać tożsamość?

Część podsumowująca: Uczestnicy warsztatu tworzą „Kodeks cyberbezpieczeństwa”

Załącznik 1

Zasady do utworzenia „Kodeksu cyberezpieczeństwa”

Załącznik 1

Zabezpiecz telefon i komputer oprogramowaniem antywirusowym. Aktualizuj oprogramowanie tak często, jak jest to wymagane.
Ustawiaj silne hasła – im dłuższe tym lepsze. Zmieniaj hasła co jakiś czas. Pamiętaj, aby hasło zawierało kombinację małych i wielkich liter, cyfr i znaków specjalnych.
Nigdy nie używaj tego samego hasła do logowania w dwóch różnych miejscach, szczególnie jeśli dane hasło zabezpiecza konto lub aplikację bankową.
Przed rozpoczęciem logowania sprawdź połączenie z bankiem: czy adres strony rozpoczyna się od protokołu „https:// („*s*" na końcu od ang. *secure* oznacza bezpieczne połączenie) i czy jest widoczna ikonka kłódki – to oznacza, że dane są zaszyfrowane. Kliknij w kłódkę i zweryfikuj datę ważności certyfikatu i do kogo należy.
Nie loguj się do bankowości elektronicznej, korzystając z ogólnodostępnej sieci Wi-Fi, np. udostępnionych w restauracjach, hotelach, etc.
Nigdy nie loguj się do bankowości z cudzych urządzeń.
Zawsze wpisuj adres strony banku bezpośrednio w przeglądarce internetowej.
Nigdy nie wchodź na stronę banku z użyciem linków otrzymanych mailem. Uważaj na linki w wiadomościach e-mail i SMS. Banki nigdy nie wysyłają próśb o login czy hasło.
Zawsze sprawdzaj podsumowanie transakcji przed jej zatwierdzeniem w aplikacji bankowej. Pamiętaj o weryfikacji numeru konta i kwoty do przelewu.
Czytaj komunikaty wysyłane przez bank w bankowości elektronicznej lub na stronie internetowej banku. Staraj się być na bieżąco z informacjami o nowych zagrożeniach.
Nie udostępniaj nikomu karty płatniczej oraz numeru PIN do niej. Nie umieszczaj numeru PIN w łatwo dostępnych miejscach.
Obejrzyj bankomat przed włożeniem do niego karty – jeśli coś zaniepokoi cię w jego wyglądzie, zrezygnuj z zaplanowanej czynności i skontaktuj się z operatorem bankomatu lub swoim bankiem.
Zasłaniaj kod PIN przy jego wpisywaniu podczas korzystania z bankomatu, w aplikacji bankowej oraz podczas dokonywania transakcji w sklepach.
Zawsze pamiętaj o wylogowaniu się z bankowości elektronicznej.
Nie zabezpieczaj telefonu i komputera oprogramowaniem antywirusowym. Aktualizuj oprogramowanie kiedy masz czas.
Ustawiaj proste hasła – im krótsze tym lepsze. Nie zmieniaj hasła zbyt często. Pamiętaj, aby hasło nie było zbyt kombinowane.
Używaj tego samego hasła do logowania w różnych miejscach, szczególnie jeśli dane hasło zabezpiecza konto lub aplikację bankową.
Przed rozpoczęciem logowania nie sprawdzaj połączenie z bankiem: czy adres strony rozpoczyna się od protokołu „https:// („*s*" na końcu od ang. *secure* oznacza bezpieczne połączenie) i czy jest widoczna ikonka kłódki.
Loguj się do bankowości elektronicznej, korzystając z ogólnodostępnej sieci Wi-Fi, np. udostępnionych w restauracjach, hotelach, etc.

Loguj się do bankowości z cudzych urządzeń – masz przecież swój login i hasło.
Wchodź na stronę banku z użyciem linków otrzymanych mailem. Używaj linków w wiadomościach e-mail i SMS.
Nie sprawdzaj podsumowanie transakcji przed jej zatwierdzeniem w aplikacji bankowej. Nie weryfikuj numeru konta i kwoty do przelewu.
Usuwaj komunikaty wysyłane przez bank w bankowości elektronicznej lub na stronie internetowej banku.
Udostępniaj kartę płatniczą oraz numeru PIN do niej jeżeli masz taką potrzebę. Umieszczaj numer PIN w łatwo dostępnych miejscach.
Bankomat jest zawsze bezpieczny do wypłaty gotówki, więc nie należy oglądać bankomatu przed włożeniem do niego karty.
Nie zasłaniaj kodu PIN przy jego wpisywaniu podczas korzystania z bankomatu, w aplikacji bankowej oraz podczas dokonywania transakcji w sklepach.
Nie ma konieczności wylogowywania się z bankowości elektronicznej.