Case study do ćwiczenia „Internet jako ułatwiacz codzienności

Sytuacja 1.
Instrukcja: Zapoznajcie się z poniższą historią. Zastanówcie się:
• Jakie mogą być negatywne konsekwencje tego zachowania dla użytkownika?
• Jak w opisanej sytuacji można się zachować, by nie narazić się na niebezpieczeństwo w sieci?

Hania jest pełnoletnia. Chętnie robi zakupy przez internet. Znalazła wymarzoną sukienkę w promocji, więc jak najszybciej chciała ją kupić. Postanowiła zrobić zakupy łącząc się z siecią wifi na smartfonie siedząc w kawiarni. Weszła na stronę sklepu, po czym złożyła zamówienie i przeszła do płatności: w pasku przeglądarki pojawił się adres banku: http://..... I czerwona kłódka.

Odpowiedzi:
• Jakie mogą być negatywne konsekwencje tego zachowania dla użytkownika?
- korzystając z sieci wifi (bez klucza) z urządzeń mobilnych może narazić się na to, że jej dane będą przechwycone
Gdy użytkownik próbuje łączyć się z innymi użytkownikami sieci bezprzewodowych z urządzeń mobilnych, wskazane jest, aby uzyskiwać połączenie tylko z sieciami bezprzewodowymi wymagającymi klucza zabezpieczeń sieciowych lub mającymi inne formy zabezpieczeń, takie jak certyfikat. Przed podłączeniem do sieci Wi-Fi takiej jak sieć publiczna w kawiarence czy na lotnisku, należy dokładnie zapoznać się z oświadczeniem o zasadach zachowania poufności i dowiedzieć się, które pliki, o ile w ogóle jakieś, są zachowywane na komputerze oraz jakie informacje usługodawca pobiera z komputera. Należy pamiętać również, aby przy logowaniu się do poczty, banku lub innego serwisu używać połączenia szyfrowanego

- niezabezpieczony adres banku (brak zielone kłódki, błędny adres: http, zamiast htpps – jej dane logowania mogą zostać przechwycone
- ryzyko straty pieniędzy
- sklep – czy znała regulamin, czy sprawdziła dane i wiarygodność właściciela – czy zgodziła się na wykorzystywanie danych osobowych i czy wie, w jakim celu?
- smartfon – czy jest chroniony programem antywirusowym, Należy również pamiętać o instalacji programów antywirusowych na wszystkich urządzeniach, na których można je stosować (PC, laptop, tablet, smartfone).

• Jak w opisanej sytuacji można się zachować, by nie narazić się na niebezpieczeństwo w sieci?
• używać własnego komputera podczas korzystania z usług bankowości elektronicznej (np. nie korzystać z komputerów w kafejkach internetowych do tego celu);
• dbać o bezpieczeństwo własnego komputera, korzystając z legalnego oprogramowania oraz stosując konieczne aktualizacje, w tym aktualizowany na bieżąco program antywirusowy;
• nie udostępniać osobom trzecim numeru klienta, haseł, karty kodów jednorazowych itp. (także nie przesyłać takich danych e-mailem), nie podawać tego typu danych na stronach internetowych, które nie stosują szyfrowania i certyfikatu cyfrowego;
• nie odpowiadać na e-maile z prośbą o ujawnienie czy zweryfikowanie danych osobowych, informacji dotyczących numeru konta czy karty kredytowej. Bank nigdy nie wysyła e-maili z prośbą o podanie takich danych. W wypadku otrzymania takiego e-maila należy od razu skontaktować się z bankiem; • nie zapisywać haseł ani numerów PIN, tylko je zapamiętać;
• regularnie monitorować rachunek bankowy, wyciągi bankowe;
• upewnić się, czy połączenie jest szyfrowane (czy adres strony w oknie przeglądarki rozpoczyna się

od https://, bo zwykłej zaczyna się od http://) oraz czy na pasku u dołu lub u góry ekranu pojawia się ikona z zamkniętą kłódką;
• wylogowywać się po zakończeniu działań na rachunku;
• ręcznie wpisywać adres strony banku i/lub stworzyć do niego zakładkę w przeglądarce, nie korzystać z „podpowiadaczy" i linków.
- Ostrzegamy przed złośliwym oprogramowaniem dla urządzeń mobilnych (tablety, telefony komórkowe) podszywającym się pod aplikacje Banków oraz innych instytucji.
(Phishing – metoda podstępnego uzyskiwania haseł dostępu do internetowych kont bankowych użytkownika za pośrednictwem np. e-maili, w tym wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów dot. karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję.
Pharming – bardziej niebezpieczna dla użytkownika oraz trudniejsza do wykrycia forma phishingu. Charakterystyczne dla pharmingu jest to, że nawet po wpisaniu prawidłowego adresu strony www, ofiara zostanie przekierowana na fałszywą (choć mogącą wyglądać tak samo) stronę www. Ma to na celu przejęcie wpisywanych przez użytkownika do zaufanych witryn haseł, numerów kart kredytowych i innych poufnych danych.
Skimming – nielegalne kopiowanie zawartości paska magnetycznego karty bankowej bez wiedzy jej posiadacza, w celu wykonywania nieuprawnionych transakcji.
Vishing – metoda oszustwa, mająca swoje podstawy w phisingu i metodach socjotechnicznych, polegająca na tym, że oszuści wykorzystując telefonię internetową podszywają się pod instytucje finansowe.
szyfrowana transmisja danych – realizowana za pośrednictwem protokołu SSL,
proste uwierzytelnianie – (identyfikator, hasło, PIN),
silne uwierzytelnianie – (np. token, certyfikat użytkownika, klucz prywatny),
podpis elektroniczny.

Inne zagrożenia: zakupy online:
- spreparowane sklepy internetowe np. z elektroniką, czy markową odzieżą, które wyglądają zupełnie legalnie lub wykorzystują do tego aukcje internetowe, np. na Allegro, kusząc klientów okazjonalną ofertą cenową. W rzeczywistości sprzedawane są na nich towary podrobione, niezgodne z rzeczywistością lub co gorsza po zapłacie nie są wcale dostarczane do kupującego. Oszuści kuszą łatwymi pieniędzmi, które rzekomo dana osoba wygrała w loterii a „jedynym" warunkiem odebrania pieniędzy jest wypełnienie wniosku i wniesienie opłaty.
- Zawsze należy zapoznać się z regulaminem zamieszczanym przez sprzedającego oraz uważnie sprawdzać wszelkiego rodzaju ukryte koszty
- Starać się zawsze sprawdzić wiarygodność Sprzedającego lub np. Pracodawcy. W Internecie często można znaleźć informacje od innych użytkowników np. na forach internetowych.
- Jeśli cena wydaje się zbyt atrakcyjna, należy podchodzić do transakcji bardziej podejrzliwie.
- Warto zadzwonić na numer obsługi Klienta, jeśli nie ma żadnego numeru kontaktowego, to powinno wzbudzić podejrzliwość uytkownika.
- W przypadku usług „krypto płatnych" np.: SMS Premium lub infolinii premium, należy sprawdzić czy podawany koszt jest rzeczywisty. Informacji o kosztach można szukać na stronach UOKIK, KRRiT, oraz UKE.
- Należy sprawdzić, czy sklep internetowy posiada szyfrowanie treści w procesie zakupu
- W przypadku płatności kartą kredytową, pierwszym warunkiem koniecznym jest szyfrowana transakcja w sklepie
- Należy zwracać uwagę na poprawność gramatyczną treści korespondencji od sprzedającego. Często przestępcy instalując fałszywe strony czy aukcje nie mówią w języku polskim, a wszelkiego

rodzaju korespondencja e-mail jest tłumaczona za pośrednictwem słowników internetowych.
- Istotne, by zwrócić uwagę z jakiej domeny przychodzi korespondencja od sprzedającego. Czy jest taka sama jak strony internetowej (np. strona: www.twojsklep.pl i e-mail: biuro@twojsklep.pl).
- Jeśli pojawiają się wątpliwości przy stwierdzeniu, czy dana oferta jest wiarygodna czy nie, lepiej z niej nie korzystać.
- Jeśli padnie się ofiarą oszustwa internetowego, należy zgłosić sprawę na policję. Ponadto, jeżeli ofiara korzystała z karty kredytowej, bezzwłocznie powinna ją zablokować w banku.

Sytuacja 2.
Instrukcja: Zapoznajcie się z poniższą historią. Zastanówcie się:
• Jakie mogą być negatywne konsekwencje tego zachowania dla użytkownika?
• Jak w opisanej sytuacji można się zachować, by nie narazić się na niebezpieczeństwo w sieci?

Justyna już od kilku lat z zamiłowaniem biega. Na urodziny dostała w prezencie smartfona. Zainstalowała aplikację do śledzenia postępów w bieganiu. Podczas instalacji wyraziła zgodę na to, by aplikacja miała dostęp do informacji w jej telefonie. Chodziło między innymi o dane na temat zużycia baterii i aktualnego użycia karty pamięci telefonu, książkę telefoniczną, informację o lokalizacji. Teraz za każdym razem, kiedy idzie biegać, bierze ze sobą telefon. Aplikacja rejestruje trasę jej biegu, zlicza przebiegnięte kilometry i spalone kalorie. Te informacje automatycznie zamieszczane są na portalu społecznościowym, na którym Justyna ma konto. Dzięki temu wszyscy jej znajomi wiedzą, kiedy Justyna biega, i mogą ją dopingować.

- Potencjalny złodziej może się dowiedzieć, w jakich godzinach Justyny nie ma w domu.
- Na podstawie wyników sportowych Justyny firma ubezpieczeniowa może ocenić jej stan zdrowia i wykorzystać tę informację do ustalenia wysokości stawki ubezpieczeniowej.
- Nieprzychylna Justynie osoba, wiedząc, w jakich miejscach można ją spotkać biegającą, może tę informację wykorzystać na niekorzyść dziewczyny.
• Ktoś może oceniać, na ile Justyna w danym momencie jest w formie.
• Liczba kalorii spalanych przez Justynę w trakcie biegu może być źródłem złośliwych komentarzy.

Sytuacja 3.
Instrukcja: Zapoznajcie się z poniższą historią. Zastanówcie się:
• Jakie mogą być negatywne konsekwencje tego zachowania dla użytkownika?
• Jak w opisanej sytuacji można się zachować, by nie narazić się na niebezpieczeństwo w sieci?

Po przeprowadzce i rozpoczęciu nauki w nowej szkole masz gorszy nastrój. Nie chcesz wychodzić z domu i spotykać się z kolegami i koleżankami z klasy. Tęsknisz za poprzednią szkołą. Postanawiasz poszukać pomocy w sieci. Korzystasz z forum na portalu oferującym pomoc psychologiczną. Zakładasz konto, podajesz swoje imię i nazwisko, opisujesz sytuację.

• brak gwarancji anonimowości: Podając swoje prawdziwe imię i nazwisko na portalu internetowym, umożliwiasz swoją identyfikację osobom prowadzącym serwis, a także innym osobom, które mają dostęp do danych zamieszczonych w serwisie.
• Różne osoby mogą się dowiedzieć o Twoich intymnych sprawach. Masz ograniczony wpływ na to, jak prywatne informacje będę wykorzystywane przez właścicieli portalu.
• starać się nie ujawniać tylu intymnych informacji o sobie: Najlepiej skorzystać z pomocy psychologicznej poza siecią. Ewentualnie możesz zalogować się na portalu z użyciem fikcyjnego imienia i nazwiska. Zawsze przed skorzystaniem z takich usług zapoznaj się z regulaminem.

Sytuacja 4.
Instrukcja: Zapoznajcie się z poniższą historią. Zastanówcie się:
• Jakie mogą być negatywne konsekwencje tego zachowania dla użytkownika?
• Jak w opisanej sytuacji można się zachować, by nie narazić się na niebezpieczeństwo w sieci?

Chcesz podzielić się z innymi zdjęciami z imprezy. Ty i Twoi znajomi jesteście widoczni na zdjęciach. Wrzucasz fotografie na portal społecznościowy. Oznaczasz znajomych. Teraz wszyscy mogą je oglądać.

- *Publikując zdjęcia ze swoim wizerunkiem na portalu społecznościowym, umożliwiasz identyfikację swojej osoby wszystkim, którzy mają do nich dostęp (w przypadku niektórych ustawień prywatności może to być każdy człowiek korzystający z Internetu). Oznaczenie osób ułatwia identyfikację.*
- *Inne osoby mogą się dowiedzieć, z kim, gdzie i w jaki sposób spędzasz czas. W ten sposób informacje o Twoich zwyczajach mogą trafić na przykład do potencjalnych pracodawców.*
- *Przed udostępnianiem zdjęć lub informacji warto zastanowić się, czy rzeczywiście chcesz dzielić się nimi ze wszystkimi (weź pod uwagę nie tylko swoje preferencje, ale również prywatność innych osób). Zdjęcia można przekazać bezpośrednio za pomocą przenośnej pamięci, ewentualnie przesłać e-mailem albo udostępnić w sieci w taki sposób, by miały do nich dostęp tylko wybrane osoby.*