

Zeszyt ćwiczeń

Jak nie dać się oszukać w internecie: hasła, telefon, konta i pieniądze

Kurs VITA: vita.edu.pl/courses/jak-nie-dac-sie-oszukac-w-internecie

27 ćwiczeń, po jednym do każdej lekcji. Na końcu znajdziesz przykładowe odpowiedzi. Najpierw spróbuj odpowiedzieć samodzielnie, dopiero potem zajrzyj do wzorów. Postacie i sytuacje w ćwiczeniach są przykładowe. Zeszyt jest materiałem edukacyjnym, nie poradą prawną, lekarską ani psychologiczną. Kurs nie obiecuje stuprocentowej ochrony ani zwrotu pieniędzy po oszustwie.

Ćwiczenia

Moduł 1. Jak działają oszuści

Lekcja 1.1. Jak działa socjotechnika: pośpiech, strach, autorytet i nagroda

Przykład fikcyjny. Pani Halina dostaje SMS: „Twoje konto zostanie zablokowane w ciągu 2 godzin z powodu nietypowej transakcji. Zaloguj się i potwierdź dane: [link]”. Zaznacz, które cztery naciski występują w tej wiadomości i zapisz jednym zdaniem, co robi pani Halina. Potem poszukaj w swojej skrzynce lub telefonie jednej podejrzanej wiadomości z ostatnich miesięcy i zrób z nią to samo.

Lekcja 1.2. Najczęstsze oszustwa w Polsce: osiem scenariuszy w jednym miejscu

Przykład fikcyjny. Pan Andrzej dostaje trzy wiadomości w jeden wieczór: a) SMS „Twoja paczka czeka, dopłać 2,10 zł: [link]”, b) telefon od osoby, która mówi „jestem z Twojego banku, ktoś próbuje wziąć kredyt, proszę zainstalować aplikację do weryfikacji”, c) reklamę w serwisie społecznościowym: „Zainwestuj 250 zł, zarób 5000 zł w miesiąc”. Dopasuj do każdej wiadomości scenariusz z tabeli i zapisz pierwszy krok.

Lekcja 1.3. Zanim klikniesz: sześć pytań i zasada „zatrzymaj się, sprawdź, oddzwon”

Przykład fikcyjny. Pani Ewa dostaje telefon: „Dzień dobry, dzwonię z działu bezpieczeństwa banku. Ktoś próbuje zalogować się na Pani konto. Proszę podać kod z SMS-a, który zaraz przyjdzie, i nikomu o tym nie mówić.” Zaznacz, na które z sześciu pytań odpowiedź brzmi „tak”, i napisz jedno zdanie, którym pani Ewa kończy rozmowę. Potem wydrukuj kartę i wpisz na niej numer swojego banku z tyłu karty.

Moduł 2. Hasła na popołudnie

Lekcja 2.1. Jedno hasło do wszystkiego i wycieki danych: dlaczego to ryzykowne

Przykład fikcyjny. Pan Tomasz ma jedno hasło „Kasia2019!” do poczty, do banku internetowego i do sklepu z elektroniką. Sklep ogłosił wyciek danych. Napisz, w jakiej kolejności pan Tomasz zmienia hasła i co robi jeszcze. Potem

zrób listę swoich pięciu najważniejszych kont w kolejności, w jakiej je zabezpieczysz.

Lekcja 2.2. Mocne hasło bez aplikacji: fraza hasłowa i długość zamiast wymyślnych znaków

Przykład fikcyjny. Pani Krystyna ma do banku hasło „Janek1985!”, bo Janek to wnuk. Zamień je na frazę hasłową. Zasada: cztery zwykłe słowa, które nie tworzą cytatu, plus jedno nieoczywiste, bez imion i dat. Zapisz propozycję, ale nie wysyłaj jej nikomu i nie używaj jej naprawdę. Potem ułóż własną frazę dla poczty i zapamiętaj ją, nie zapisując w telefonie.

Lekcja 2.3. Gdzie trzymać hasła: menedżer, zeszyt i co zrobić po wycieku

Przykład fikcyjny. Pani Grażyna z Lublina, 68 lat, ma smartfon, ale nie lubi aplikacji. Ma dwanaście kont: poczta, bank, dwa sklepy, serwis telewizyjny i kilka innych. Wybierz dla niej sposób przechowywania haseł i napisz, jak ułożyć notes. Potem zdecyduj, jak Ty przechowujesz hasła, i zapisz trzy kroki do zrobienia w tym tygodniu.

Moduł 3. Drugi składnik i konta kluczowe

Lekcja 3.1. Weryfikacja dwuetapowa: SMS, aplikacja, klucz dostępu i kody zapasowe

Przykład fikcyjny. Pan Henryk, 72 lata, ma smartfon z Androidem i konto Google. Nie ma głowy do instalowania aplikacji. Wybierz dla niego rodzaj drugiego etapu i wyjaśnij, co zrobi z kodami zapasowymi. Potem zrób to samo dla swojego konta: sprawdź, czy weryfikacja dwuetapowa jest włączona.

Lekcja 3.2. Poczta, od której zależą wszystkie konta: odzyskiwanie i numer telefonu

Przykład fikcyjny. Pani Danuta ma jeden adres e-mail, na który założyła konto w banku, na Allegro i na Facebooku. Numer telefonu w koncie pocztowym jest sprzed dziesięciu lat, jeszcze z poprzedniej umowy. Wypisz trzy zmiany, które pani Danuta powinna zrobić dziś. Potem sprawdź własne konto pocztowe i zapisz, które z danych do odzyskiwania są nieaktualne.

Lekcja 3.3. Plan na 30 minut: zabezpiecz pocztę, bank i Facebooka

Przykład fikcyjny. Pan Wojciech z Gdyni ma pocztę, bank i Facebook. Hasło do poczty i Facebooka jest to samo, drugiego etapu nie ma nigdzie, a powiadomień z banku nie czyta, bo wyłączył je kiedyś, „żeby nie dzwoniło”. Ułóż dla niego plan na 30 minut w kolejności i napisz, co zrobi w każdym kroku. Potem wykonaj własny plan na tych trzech kontach i zapisz datę.

Moduł 4. Telefon, Facebook i WhatsApp

Lekcja 4.1. Telefon pod kontrolą: blokada ekranu, aktualizacje, uprawnienia i aplikacje

Przykład fikcyjny. Pani Maria z Poznania ma telefon z Androidem. Ekran odblokowuje wzorem „L”, systemu nie aktualizowała od roku, a aplikacja z grą ma dostęp do jej kontaktów i mikrofonu. Wypisz cztery rzeczy, które zrobi w kwadrans. Potem sprawdź w swoim telefonie: rodzaj blokady, datę ostatniej aktualizacji i jedną aplikację, której cofniesz uprawnienie.

Lekcja 4.2. Facebook i Messenger: przejęte konto, fałszywy profil znajomego i prośba o BLIK

Przykład fikcyjny. Pani Aneta dostaje na Messengerze wiadomość od koleżanki Kasi: „Hej, jesteś? Kupuję coś w sieci i płatność idzie tylko kodem BLIK, a ja nie mam. Wygeneruj, oddam jutro, 800 zł”. Napisz, co robi pani Aneta, i ułóż trzy zdania, które przygotujesz dla swoich bliskich na podobne sytuacje. Sprawdź też, czy włączyłeś w swoim banku powiadomienia o transakcjach BLIK.

Lekcja 4.3. WhatsApp: kod weryfikacyjny, „wyślij mi kod przez pomyłkę” i linki od znajomych

Przykład fikcyjny. Pan Krzysztof dostaje na WhatsAppie wiadomość od kolegi Pawła: „Cześć, zagłosuj na moje zdjęcie w konkursie: [link]”. Na stronie pojawia się prośba o wpisanie kodu z SMS-a, który właśnie przyszedł. Napisz, co robi pan Krzysztof, i zapisz, jak włączysz weryfikację dwuetapową w swoim WhatsAppie.

Moduł 5. SMS, mail, linki i zakupy

Lekcja 5.1. SMS „dopłać do paczki”, fałszywe płatności i „banki”: jak zareagować w minutę

Przykład fikcyjny. Pan Andrzej z Łodzi dostaje SMS: „Paczka nie została dostarczona, dopłać 2,50 zł pod linkiem, inaczej wróci do nadawcy.” Nie pamięta, żeby cokolwiek zamawiał. Napisz, co robi krok po kroku. Potem sprawdź w swoim telefonie, czy umiesz przekazać wiadomość na 8080 (najlepiej na przykładzie starego SMS-a).

Lekcja 5.2. Phishing w mailu i na stronie logowania: jak sprawdzić link, zanim cokolwiek wpiszesz

Przykład fikcyjny. Pani Halina dostaje mail: „Twoje konto zostanie zablokowane w 24 godziny. Zaloguj się: <https://twojbank.pl.weryfikacja-konta.com/logowanie>”. Napisz trzy sygnały ostrzegawcze i to, co zrobi. Potem znajdź w swojej skrzynce jedną starą wiadomość z linkiem i sprawdź, do jakiej domeny prowadzi.

Lekcja 5.3. Zakupy i ogłoszenia: fałszywe sklepy, „kupujący” z linkiem i inwestycje z reklamy

Przykład fikcyjny. Pani Karolina sprzedaje rower w serwisie ogłoszeniowym. Kupujący pisze na WhatsAppie, że zapłacił, i przysyła link „do odbioru płatności”, który prosi o numer karty. Napisz, co robi pani Karolina, i ułóż dla siebie krótką regułę dotyczącą sprzedaży online. Potem sprawdź sklep internetowy, w którym ostatnio kupowałeś: czy ma regulamin

z danymi firmy.

Moduł 6. Telefon z banku, BLIK i bliscy

Lekcja 6.1. Telefon z „banku” lub od „policjanta”: dlaczego „bezpieczne konto” nie istnieje

Przykład fikcyjny. Pan Tadeusz z Lublina odbiera telefon: „Dzień dobry, mówi konsultant banku. Z Pana konta próbowano wykonać przelew na 4800 zł. Aby go zablokować, proszę podać dwa kody BLIK i nie rozłączać się.” Napisz, co robi pan Tadeusz, i zapisz, skąd weźmie numer do swojego banku.

Lekcja 6.2. Kod BLIK, „babciu, to ja” i „wnuczek”: jak sprawdzić, czy prosi bliska osoba

Przykład fikcyjny. Pani Wanda ze Szczecina odbiera telefon: „Babciu, to ja. Miałem wypadek, potrzebuję 8000 zł, ktoś przyjedzie po pieniądze.” Głos jest przytłumiony, bo „przeziębiony”. Napisz, co robi pani Wanda i jak brzmi hasło, które ustalisz w swojej rodzinie. Wypisz też trzy osoby, z którymi je omówisz.

Lekcja 6.3. Zdalny dostęp: AnyDesk i podobne programy, o których instalację prosi „pomocnik”

Przykład fikcyjny. Pan Ireneusz z Poznania dostaje telefon z „Biura Informacji Kredytowej”. Rozmówca mówi, że ktoś próbuje wziąć kredyt na jego dane, i prosi o zainstalowanie AnyDesk, żeby „zablokować wniosek”. Napisz, co robi pan Ireneusz, i znajdź w swoim telefonie lub komputerze, czy któryś z programów do zdalnego dostępu jest zainstalowany.

Moduł 7. Gdy coś się stało

Lekcja 7.1. Pierwsza godzina po oszustwie: bank, karta, hasła i zapis zdarzeń

Przykład fikcyjny. Pani Grażyna z Gdańska rozmawiała z „konsultantem banku”, podała dwa kody BLIK i zainstalowała AnyDesk. Po godzinie widzi, że z konta zniknęło 3500 zł. Ułóż dla niej kolejność działań i napisz, co zapisze na kartce. Potem znajdź w domu numer infolinii swojego banku z tyłu karty i wpisz go na kartę z lekcji 1.3.

Lekcja 7.2. Policja, reklamacja w banku i Rzecznik Finansowy: co wolno, co możesz i czego nie wiadomo

Przykład fikcyjny. Pan Leszek z Kielc podał „konsultantowi” kod BLIK i stracił 2600 zł. Zgłosił to w banku i na policji. Napisz trzy zdania reklamacji i wypisz, jakie dokumenty dołączy. Potem sprawdź na stronie swojego banku, jak można złożyć reklamację i na jaki adres.

Lekcja 7.3. Przejęte konto i kradzież tożsamości: zastrzeż PESEL, sprawdź BIK, odzyskaj pocztę i Facebooka

Przykład fikcyjny. Pani Dorota z Rzeszowa wysłała „pracownikowi inwestycyjnemu” zdjęcie dowodu osobistego. Po tygodniu dowiaduje się z poczty, że ktoś założył na jej dane rachunek w obcym banku. Napisz pięć kroków i zapisz, kiedy sama zastrzeżesz swój PESEL. Jeśli możesz, zrób to dziś.

Moduł 8. Rodzice i dziadkowie

Lekcja 8.1. Rozmowa z rodzicami i dziadkami o oszustwach: jak zacząć bez pouczania

Przykład fikcyjny. Pani Halina ma 74 lata i mówi: „Mnie nikt nie oszuka, ja nie jestem głupia.” Jej wnuk Piotr chce porozmawiać. Napisz trzy zdania, od których zacznie, i trzy rzeczy, które zaproponuje do ustalenia. Potem wybierz osobę ze swojej rodziny i zaplanuj termin rozmowy.

Lekcja 8.2. „Ustawiamy telefon razem”: godzina przy telefonie rodzica, krok po kroku

Przykład fikcyjny. Pan Zbigniew z Opola ma 71 lat i telefon z Androidem. Ma PIN „1234”, nie aktualizował systemu od dawna, a jedno hasło stosuje do poczty i do sklepu. Syn Michał jedzie do niego na godzinę. Napisz, w jakiej kolejności Michał z nim pracuje i co zostawia na kolejną wizytę. Potem zaplanuj godzinę dla własnego rodzica.

Lekcja 8.3. Karta na lodówkę „Zanim klikniesz” i zasada „dzwoń przed przelewem”

Przykład fikcyjny. Pani Krystyna ma 78 lat. Dzwoni „konsultant banku”, mówi, że z jej konta ktoś próbuje wypłacić pieniądze, i prosi, żeby przelała oszczędności na „bezpieczne konto”. Na lodówce wisi karta „Zanim klikniesz”. Napisz, co pani Krystyna robi krok po kroku, i przygotuj własną kartę: trzy zdania i dwa numery.

Moduł 9. Wdrożenie i egzamin końcowy

Lekcja 9.1. Plan na jedno popołudnie: co zrobić dziś, a co w tym miesiącu

Przykład fikcyjny. Pani Ewa z Torunia ma tylko jedno popołudnie w sobotę. Ma jedno hasło do poczty i Allegro, nie włączyła drugiego etapu logowania i ma w telefonie PIN „0000”. Powiedz, od czego zacznie i co zostawi na później. Potem wpisz w kalendarz własne popołudnie i zapisz trzy rzeczy, które zrobisz w pierwszej godzinie.

Lekcja 9.2. Po oszustwie: wstyd, złość i kiedy poprosić o wsparcie

Przykład fikcyjny. Pan Andrzej z Rzeszowa przekazał kod BLIK osobie, która podała się za konsultanta banku. Stracił 3000 zł. Pierwszego wieczoru nikomu nie powiedział, bo wstydzi się przed żoną, i nie śpi. Napisz, co może zrobić tego samego wieczoru, i ułóż zdanie, od którego zacznie rozmowę z żoną. Potem zapisz własne zdanie na wypadek

podobnej sytuacji.

Lekcja 9.3. Projekt końcowy: Twój plan ochrony i egzamin

Przykład fikcyjny. Pan Tomasz z Lublina ma żonę, dwoje dorosłych dzieci i starszą mamę. Zrobił już nowe hasło do poczty i drugi etap. Wypełnij za niego kartkę: co jest zrobione, trzy rzeczy na miesiąc, numery i data przeglądu. Potem przygotuj własną kartkę.

Przykładowe odpowiedzi

Moduł 1. Jak działają oszuści

Lekcja 1.1. Jak działa socjotechnika: pośpiech, strach, autorytet i nagroda

Przykładowa odpowiedź: pośpiech („w ciągu 2 godzin”), strach („nietypowa transakcja”), autorytet (podszyć się pod bank). Nagrody tu nie ma. Pani Halina nie klika linku, otwiera aplikację banku ręcznie, sprawdza, czy są tam jakieś komunikaty, a SMS przekazuje na numer 8080. Sprawdź swoją odpowiedź: czy wskazałeś naciski w konkretnych słowach wiadomości?

Lekcja 1.2. Najczęstsze oszustwa w Polsce: osiem scenariuszy w jednym miejscu

Przykładowa odpowiedź: a) scenariusz paczka, pan Andrzej nie klika i sprawdza w aplikacji kuriera, b) konsultant banku połączony ze zdalnym pulpitem, rozłącza się i dzwoni na numer z karty, nie instaluje niczego, c) fałszywa inwestycja, nie wpłaca, a firmę sprawdza w rejestrach KNF. Sprawdź swoją odpowiedź: czy przy każdym scenariuszu masz konkretny krok, na przykład „sprawdzam w aplikacji”, zamiast ogólnego „uważam”?

Lekcja 1.3. Zanim klikniesz: sześć pytań i zasada „zatrzymaj się, sprawdź, oddzwon”

Przykładowa odpowiedź: „tak” przy pytaniach 1 (pilność), 2 (kod z SMS-a), 3 (nieoczekiwany telefon) i 6 (można sprawdzić w aplikacji). Zdanie: „Dziękuję, tego kodu nikomu nie podaję, oddzwonię sam na numer z mojej karty.” Pani Ewa się rozłącza, dzwoni do banku na numer z karty i pyta, czy w jej sprawie jest cokolwiek. Sprawdź swoją odpowiedź: czy zdanie jest na tyle krótkie, że powiesz je w stresie?

Kartę „Zanim klikniesz” możesz pobrać tutaj: [karta „Zanim klikniesz” (PDF)](/downloads/karta-zanim-klikniesz.pdf). Wpisz na niej numer swojego banku z tyłu karty płatniczej.

Moduł 2. Hasła na popołudnie

Lekcja 2.1. Jedno hasło do wszystkiego i wycieki danych: dlaczego to ryzykowne

Przykładowa odpowiedź: najpierw pocztę (przez nią resetuje się resztę), potem bank, na końcu sklep. Każde hasło inne. Dodatkowo pan Tomasz włącza drugi składnik w poczcie i banku oraz sprawdza w poczcie, czy nie ma niezaplanowanych logowań. Moja lista wygląda tak: poczta, bank, Facebook, sklep z zapisaną kartą, chmura. Sprawdź swoją odpowiedź: czy poczta jest na liście jako pierwsza lub druga?

Lekcja 2.2. Mocne hasło bez aplikacji: fraza hasłowa i długość zamiast wymyślnych znaków

Przykładowa odpowiedź: „cegła smutna lampa maszeruje ananas” (pięć słów, 35 znaków). Nie ma w niej imion ani dat, a zestawienie jest nieoczywiste. Sprawdź swoją odpowiedź: czy w Twojej frazie nie ma imienia bliskiej osoby, daty ani znanego cytatu?

Lekcja 2.3. Gdzie trzymać hasła: menedżer, zeszyt i co zrobić po wycieku

Przykładowa odpowiedź: pani Grażyna wybiera papierowy notes trzymany w domu, z listą kont (nazwa serwisu, login, hasło), dwa najważniejsze hasła, do poczty i banku, pamięta jako frazy. Notes nie jest podpisany „Hasła”. Dla mnie: 1) wybieram menedżer haseł, 2) przenoszę pięć najważniejszych kont, 3) zmieniam hasła do poczty i banku. Sprawdź swoją odpowiedź: czy każdy krok masz zaplanowany na konkretny dzień tygodnia?

Moduł 3. Drugi składnik i konta kluczowe

Lekcja 3.1. Weryfikacja dwuetapowa: SMS, aplikacja, klucz dostępu i kody zapasowe

Przykładowa odpowiedź: pan Henryk wybiera potwierdzenie na telefonie albo kod w SMS-ie, bo nie wymaga to nowej aplikacji. Kody zapasowe drukuje i chowa z dokumentami. Na własnym koncie sprawdzam w sekcji „Zabezpieczenia i logowanie”, czy opcja jest włączona, i dodaję drugi sposób, jeśli mam tylko jeden. Sprawdź swoją odpowiedź: czy wiesz, gdzie leżą Twoje wydrukowane kody?

Lekcja 3.2. Poczta, od której zależą wszystkie konta: odzyskiwanie i numer telefonu

Przykładowa odpowiedź: 1) zmienić numer telefonu na aktualny, 2) włączyć drugi etap logowania i wydrukować kody zapasowe, 3) dodać drugi adres do odzyskiwania i sprawdzić listę zalogowanych urządzeń. Dodatkowo ustalić nowe,

unikalne hasło do poczty. Sprawdź swoją odpowiedź: czy zacząłeś lub zaczęłaś od poczty, zamiast zmieniać wszystkie konta naraz?

Lekcja 3.3. Plan na 30 minut: zabezpiecz pocztę, bank i Facebooka

Przykładowa odpowiedź: poczta (10 min): nowe hasło, drugi etap, kody zapasowe. Bank (10 min): włączyć powiadomienia o każdej operacji, sprawdzić sposób potwierdzania, zapisać numer z karty. Facebook (10 min): nowe, inne hasło, drugi etap, wylogowanie nieznanych urządzeń. Zapis w notesie z datą. Sprawdź swoją odpowiedź: czy pan Wojciech ma inne hasło do poczty i do Facebooka na końcu planu?

Moduł 4. Telefon, Facebook i WhatsApp

Lekcja 4.1. Telefon pod kontrolą: blokada ekranu, aktualizacje, uprawnienia i aplikacje

Przykładowa odpowiedź: 1) zmienia wzór na PIN i odcisk palca, 2) sprawdza dostępność aktualizacji i włącza automatyczne, 3) w uprawnieniach aplikacji z grą wyłącza kontakty i mikrofon, 4) sprawdza, czy Google Play Protect jest włączony. U mnie: PIN, włączone aktualizacje i odebrane uprawnienie do mikrofonu aplikacji, której używam rzadko. Sprawdź swoją odpowiedź: czy w telefonie zmieniło się coś realnie, zamiast zostać tylko przeczytanym?

Lekcja 4.2. Facebook i Messenger: przejęte konto, fałszywy profil znajomego i prośba o BLIK

Przykładowa odpowiedź: pani Aneta nie generuje kodu, dzwoni do Kasi na numer zapisany w telefonie i pyta, czy pisała. Jeśli Kasia nie pisała, pani Aneta ostrzega znajomych, że konto Kasi jest przejęte. Trzy zdania dla bliskich: „Zadzwoń i potwierdź”, „Nigdy nie podaję kodu BLIK przez Messengera” i „Ustalmy rodzinne hasło”. Sprawdź swoją odpowiedź: czy pierwszym krokiem pani Anety jest telefon, zamiast odpowiedzi w komunikatorze?

Lekcja 4.3. WhatsApp: kod weryfikacyjny, „wyslij mi kod przez pomyłkę” i linki od znajomych

Przykładowa odpowiedź: pan Krzysztof kodu nie wpisuje, zamyka stronę i dzwoni do Pawła, żeby zapytać, czy wysłał wiadomość. SMS z kodem to kod rejestracyjny jego konta, więc nikomu go nie podaje. U mnie: otwieram ustawienia WhatsAppa, wybieram weryfikację dwuetapową, ustawiam hasło i zapisuję je w notesie w domu. Sprawdź swoją odpowiedź: czy wpisałeś hasło do zapisania w bezpiecznym miejscu?

Moduł 5. SMS, mail, linki i zakupy

Lekcja 5.1. SMS „dopłać do paczki”, fałszywe płatności i „banki”: jak zareagować w minutę

Przykładowa odpowiedź: pan Andrzej nie klika linku, otwiera aplikację kuriera lub sklepu i sprawdza, czy na jego nazwisko jest przesyłka. Jeśli jej nie ma, przekazuje SMS na 8080 bez zmian i usuwa wiadomość. Jeżeli kliknął i wpisał dane karty, dzwoni do banku i zastrzega kartę. Sprawdź swoją odpowiedź: czy wiadomość przekazałeś w oryginalnej formie? Zrzut ekranu CERT odrzuca.

Lekcja 5.2. Phishing w mailu i na stronie logowania: jak sprawdzić link, zanim cokolwiek wpiszesz

Przykładowa odpowiedź: sygnały: 1) presja czasu, 2) adres należy do domeny „weryfikacja-konta.com”, więc bank nie jest jej właścicielem, 3) wiadomość każe zalogować się przez link, zamiast przez aplikację banku. Pani Halina nie klika, otwiera aplikację banku lub wpisuje adres ręcznie, a mail zgłasza na incydent.cert.pl i usuwa. Sprawdź swoją odpowiedź: czy ustaliłeś domenę, czytając adres od prawej?

Lekcja 5.3. Zakupy i ogłoszenia: fałszywe sklepy, „kupujący” z linkiem i inwestycje z reklamy

Przykładowa odpowiedź: pani Karolina nie klika linku i nie podaje danych karty. Odpisuje, że rozlicza się tylko przez serwis, sprawdza w banku, czy wpłata naprawdę wpłynęła, i zgłasza rozmowę administratorowi serwisu. Moja reguła: „Pieniądze odbieram bez karty i bez linków, wysyłam dopiero po wpłacie w banku.” Sprawdź swoją odpowiedź: czy w regule jest zdanie o wpłacie widocznej w banku?

Moduł 6. Telefon z banku, BLIK i bliscy

Lekcja 6.1. Telefon z „banku” lub od „policjanta”: dlaczego „bezpieczne konto” nie istnieje

Przykładowa odpowiedź: pan Tadeusz nie podaje kodów, mówi „Rozłączam się i dzwonię sam” i kończy rozmowę. Numer do banku znajduje z tyłu karty płatniczej, dzwoni i pyta, czy coś się dzieje na koncie. Jeśli nic się nie dzieje, rozmowę zgłasza policji. Sprawdź swoją odpowiedź: czy numer wzięłeś z karty lub ze strony banku? Wyświetlacz nie

jest dobrym źródłem.

Lekcja 6.2. Kod BLIK, „babciu, to ja” i „wnuczek”: jak sprawdzić, czy prosi bliska osoba

Przykładowa odpowiedź: pani Wanda odkłada słuchawkę, dzwoni do wnuka na numer zapisany w jej telefonie i pyta, czy dzwonił. Nikomu nie wydaje pieniędzy i nie mówi, ile ma w domu. Hasło u mnie: słowo, którego nikt poza rodziną nie zna, ustalone osobiście. Omówię je z mamą, bratem i dziećmi. Sprawdź swoją odpowiedź: czy hasło ustaliłeś na żywo lub telefonicznie? Komunikator nie jest do tego dobrym miejscem.

Lekcja 6.3. Zdalny dostęp: AnyDesk i podobne programy, o których instalację prosi „pomocnik”

Przykładowa odpowiedź: pan Ireneusz nie instaluje niczego, rozłącza się i sam dzwoni na numer ze strony BIK lub swojego banku. Jeśli rozmówca podał się za bank, wchodzi na stronę banku i dzwoni na numer z jej zakładki kontaktowej. Sprawdzam swoje urządzenia i usuwam programy, których nie pamiętam. Sprawdź swoją odpowiedź: czy pan Ireneusz sam wybrał numer, na który dzwoni?

Moduł 7. Gdy coś się stało

Lekcja 7.1. Pierwsza godzina po oszustwie: bank, karta, hasła i zapis zdarzeń

Przykładowa odpowiedź: 1) telefon do banku z numeru z karty: zablokowanie karty i dostępu, numer zgłoszenia, 2) zamknięcie AnyDesk, odinstalowanie, odłączenie od internetu, 3) zmiana haseł z telefonu córki, najpierw poczta i bank, 4) zapis godzin, kwot i numerów, rzuty ekranu, 5) policja i incydent.cert.pl, potem reklamacja. Sprawdź swoją odpowiedź: czy pierwszym krokiem jest bank? Szukanie winnego może poczekać.

Lekcja 7.2. Policja, reklamacja w banku i Rzecznik Finansowy: co wolno, co możesz i czego nie wiadomo

Przykładowa odpowiedź: „Zgłaszam reklamację operacji BLIK z dnia 12 października na kwotę 2600 zł. Zdarzenie opisuję poniżej zgodnie z prawdą. Wnoszę o rozpatrzenie i o pisemne uzasadnienie stanowiska.” Załączniki: potwierdzenie zawiadomienia z policji, rzuty ekranu, zapis zdarzeń. Sprawdź swoją odpowiedź: czy opisałeś także to, co sam zatwierdził pan Leszek?

Lekcja 7.3. Przejęte konto i kradzież tożsamości: zastrzeż PESEL, sprawdź BIK, odzyskaj pocztę i Facebooka

Przykładowa odpowiedź: 1) zastrzec PESEL w mObywatelu, 2) pobrać Raport BIK i sprawdzić zobowiązania, 3) zgłosić bankowi, że ktoś użył jej danych, 4) zmienić hasło do poczty i włączyć drugi etap, 5) zgłosić sprawę na policji i do CERT Polska. U mnie: zastrzeżenie PESEL w sobotę rano, ustawiam przypomnienie w telefonie. Sprawdź swoją odpowiedź: czy w planie jest konkretny dzień i godzina?

Moduł 8. Rodzice i dziadkowie

Lekcja 8.1. Rozmowa z rodzicami i dziadkami o oszustwach: jak zacząć bez pouczania

Przykładowa odpowiedź: „Babciu, wczoraj dzwonił do mnie ktoś udający bank, ledwo się zorientowałem.” „Ciekaw jestem, czy do ciebie też dzwonił.” „Możemy ustalić jedną zasadę na wszelki wypadek?” Trzy rzeczy: hasło rodzinne, zasada „dzwonię do ciebie przed przelewem”, numer Piotra zapisany dużymi cyframi przy telefonie. Sprawdź swoją odpowiedź: czy zdania zaczynają się od doświadczenia Piotra i nie oceniają babci?

Lekcja 8.2. „Ustawiamy telefon razem”: godzina przy telefonie rodzica, krok po kroku

Przykładowa odpowiedź: 1) nowy PIN, 2) sprawdzenie aktualizacji i włączenie automatycznych, 3) uprawnienia aplikacji, 4) nowe hasło do poczty i drugi etap, 5) trzy numery w kontaktach. Na później: zmiana haseł w sklepie i przegląd aplikacji. Sprawdź swoją odpowiedź: czy Michał zaczyna od poczty albo blokady ekranu i część zmian zostawia na później?

Lekcja 8.3. Karta na lodówkę „Zanim klikniesz” i zasada „dzwon przed przelewem”

Przykładowa odpowiedź: pani Krystyna mówi „Oddzwonię”, kończy rozmowę i czyta kartę. Dzwoni do córki Joanny na numer wpisany na karcie, a potem do banku na numer z tyłu karty płatniczej. Bank potwierdza, że nie ma takiej procedury. Moja karta: „Nic nie robię w pośpiechu”, „Zanim zapłacę, dzwonię”, „Gdy jest groźnie, dzwonię pod 112”, numer córki i numer banku. Sprawdź swoją odpowiedź: czy pani Krystyna dzwoni na numer z karty i ignoruje numer podany przez rozmówcę?

Moduł 9. Wdrożenie i egzamin końcowy

Lekcja 9.1. Plan na jedno popołudnie: co zrobić dziś, a co w tym miesiącu

Przykładowa odpowiedź: godzina 1: nowe hasło do poczty, drugi etap i kody zapasowe, osobne hasło do Allegro. Godzina 2: powiadomienia w banku, numer infolinii na karcie, PIN inny niż „0000”, aktualizacje telefonu. Godzina 3: Facebook i rozmowa z bliskimi. Na później: BIK, PESEL, przegląd starych kont. Sprawdź swoją odpowiedź: czy plan zaczyna się od poczty i czy ma wpisaną datę?

Lekcja 9.2. Po oszustwie: wstyd, złość i kiedy poprosić o wsparcie

Przykładowa odpowiedź: dzwoni do banku i blokuje kartę, zapisuje, co się stało, a potem mówi żonie: „Dałem się oszukać i potrzebuję, żebyś mnie wysłuchała. Dziś nie szukam winnych.” Jeśli przez kilka dni nie może spać, dzwoni pod 116 123. Moje zdanie: „Zdarzyło mi się coś trudnego, usiądź ze mną na chwilę.” Sprawdź swoją odpowiedź: czy pan Andrzej najpierw załatwia bank i dopiero potem rozmowę, a numer 116 123 traktuje jako pomoc na kolejne dni?

Lekcja 9.3. Projekt końcowy: Twój plan ochrony i egzamin

Przykładowa odpowiedź: zrobione: hasło do poczty i drugi etap (data). Na miesiąc: powiadomienia w banku, blokada ekranu telefonu, „Ustawiamy telefon razem” z mamą. Numery: bank, numer żony, 112, 116 123. Przegląd: pierwszy dzień następnego miesiąca. Sprawdź swoją odpowiedź: czy kartka ma datę przeglądu i trzy konkretne czynności, nie ogólne postanowienia?