



QUIZ WIEDZY DLA DOROSŁYCH

1. Wyłudzenie jakiejś kwoty pieniędzy lub pozyskanie danych osoby wraz z numerem konta rachunku bankowego to:
 - a) trolling
 - b) phishing
 - c) sexting
2. Co robisz, gdy ktoś dzwoni z banku i prosi cię o login i hasło:
 - a) informuję rozmówcę o tym o co pyta, bo przedstawił się i dzwoni zapewne z numeru banku
 - b) nigdy na telefon takich informacji nie podaję, bo oszuści potrafią nawet podszywać się pod telefony pochodzące rzekomo z banku
 - c) „Kodeks bankowy” wymaga tego, by udzielić na pytania pracownika banku wszelkich informacji telefonicznie
3. Aby nie paść ofiarą oszustwa podczas transakcji internetowych warto:
 - a) przeczytać komentarze o sprzedającym
 - b) sprawdzić nr KRS, NIP i REGON sklepu internetowego
 - c) obie odpowiedzi są prawidłowe
4. Program przechytujący wszystkie dane przepływające pomiędzy komputerem a siecią, z którą jest on podłączony to:
 - a) sniffer
 - b) Excel
 - c) GIMP
5. Numer MSISDN to:
 - a) numer na karcie bankomatowej
 - b) numer abonenta sieci komórkowej
 - c) numer rachunku bankowego

6. Jak zareagujesz po otrzymaniu smsa dotyczącego bankowości internetowej, który wydaje Ci się podejrzany:
- a) dokładnie czytasz smsa i zawsze wykonujesz wszystkie podane w nim polecenia
 - b) niezwłocznie kontaktujesz się z bankiem i informujesz o niepokojących sygnałach oraz zmieniasz hasła lub sposób logowania na innym sprzęcie
 - c) nie robisz nic, przecież oszuści aż tak się nie wyspecjalizowali
7. Wykonywanie połączeń telefonicznych z wykorzystaniem zmienionego identyfikatora inicjującego połączenie to:
- a) grooming
 - b) hejting
 - c) spoofing
8. Logując się na stronę, poprzez którą dokonuje się płatności, należy sprawdzić, czy opiera się ona na bezpiecznym połączeniu szyfrowanym oznaczonym skrótem:
- a) https
 - b) http
 - c) vpn
9. Elektroniczna portmonetka to:
- a) konto bankowe, z którego możemy korzystać bez ograniczenia
 - b) rodzaj karty płatniczej wraz z numerem konta w celu późniejszego ich doładowania
 - c) portmonetka, która zamykana jest na kod PIN
10. Jeśli twoje nastoletnie dziecko ma założone konto:
- a) pozwalasz mu nim dysponować w sposób dowolny
 - b) nie rozmawiasz z nim o zagrożeniach dotyczących transakcji płatniczych, bo ten problem nieletnich nie dotyczy
 - c) obie odpowiedzi są błędne.
11. Osoba starsza wypłacająca dużą sumę pieniędzy z konta w banku może być potencjalną ofiarą:
- a) tzw. oszustwa na wnuczka
 - b) tzw. oszustwa na policjanta CBS
 - c) obie odpowiedzi są prawidłowe

12. W przypadku zagubienia dowodu osobistego zapobiegiesz podpisaniu umowy kredytu na twoje nazwisko, jeśli:
- a) zastrzeżesz swój dowód osobisty w dowolnym banku
 - b) powiesz o tym znajomemu policjantowi
 - c) złożysz wniosek o wydanie nowego dowodu osobistego
13. Popularny kilka lat temu skimming polega na kopiowaniu z karty płatniczej:
- a) paska magnetycznego
 - b) numeru rachunku bankowego
 - c) kodu CVC/CVV
14. Gdy otrzymasz smsa z informacją o tym, że twoja paczka została przejęta przez służby celne:
- a) przesyłasz go do wszystkich znajomych, którzy robią zakupy za granicą
 - b) kasujesz wiadomość
 - c) automatycznie klikasz w link zawarty w wiadomości sms
15. Ofiarą tzw. child groomingu może paść:
- a) senior
 - b) dziecko
 - c) kobieta
16. Sms, który otrzymujesz z banku może być cyfrowym atakiem gdy:
- a) informacja dotyczy zmiany danych osobowych lub numeru telefonu
 - b) zauważysz na stronie internetowej bankowości internetowej, że ostatnie udane logowanie było w czasie, w którym nie korzystałeś z bankowości internetowej
 - c) obie odpowiedzi są prawidłowe
17. Aby sprawdzić, czy strona bankowości internetowej jest właściwą stroną danego banku należy:
- a) wejść na stronę internetową i sprawdzić, czy wyświetlają się informacje o banku,
 - b) kliknąć w grafikę kłódki i sprawdzić, kto jest wystawcą certyfikatu,
 - c) żadne z powyższych
18. Korzystając z bankowości mobilnej (aplikacji) należy pamiętać, aby:
- a) autoryzować aplikację tylko na urządzeniu, którego jesteś wyłącznym posiadaczem,
 - b) przynajmniej raz na kwartał autoryzować aplikację,
 - c) autoryzować aplikację na dowolnym urządzeniu, które jest dostępne publicznie,

19. Ustalając hasło do bankowości internetowej należy pamiętać, aby:
- a) hasło było krótkie i łatwe do odgadnięcia, np. lato1234,
 - b) hasło zawierało tylko cyfry, np. 2022,
 - c) hasło było odpowiednio długie, składało się z minimum 8 znaków, posiadało duże litery i znak specjalny, np. L@t02022@#
20. Kiedy dzwoni do Ciebie osoba, podająca się za pracownika banku i prosząca Ciebie o zainstalowanie programu do zabezpieczania bankowości internetowej:
- a) postępujesz zgodnie z zaleceniami osoby dzwoniącej – przecież to pracownik banku,
 - b) weryfikujesz pracownika banku pytając go z jakiej instytucji dzwoni, jaki jest cel instalacji oprogramowania; po weryfikacji instalujesz program,
 - c) dziękujesz za rozmowę, rozłączasz połączenie, informujesz swój bank o zaistniałej sytuacji
21. Korzystając z bankowości internetowej należy pamiętać, aby:
- a) oprogramowanie telefonu/komputera/tabletu było zawsze aktualizowane na bieżąco,
 - b) oprogramowanie antywirusowe było aktualizowane za każdym razem, kiedy wymaga tego program,
 - c) odpowiedź a i b są poprawne
22. Kiedy Twój znajomy, z którym masz stały kontakt, za pomocą mediów społecznościowych prosi Cię o podanie kodu BLIK, aby opłacić ważną dla niego transakcję, to:
- a) podajesz kod bez wahania
 - b) dzwonisz do znajomego i dopytujesz szczegóły, czy to aby na pewno on prosi Ciebie o kod,
 - c) żadna odpowiedź nie jest prawidłowa
23. Które transakcje dokonane kartą w internecie są bezpieczne?
- a) autoryzowane za pomocą 3D Secure/aplikacji mobilnej,
 - b) podając dane z karty (numer karty, data ważności karty, kod CVC/CVV)
 - c) żadne z powyższych
24. Którą rocznicę swojej działalności obchodzi w tym roku Bank Spółdzielczy w Inowrocławiu?
- a) 145
 - b) 150
 - c) 155