Spam

W każdym ze scenariuszy zdecydujcie, czy wiadomość jest spamem i czy należy udostępnić informacje osobie, która o nie prosi. W odpowiednim polu wpiszcie odpowiedź na każde pytanie.

Scenariusz 1

Odbierasz e-mail od prawnika, który informuje Cię, że daleki krewny wskazał Cię jako spadkobiercę dużej sumy pieniędzy. W e-mailu czytasz „Aby odebrać pieniądze, proszę o przesłanie mi numeru konta bankowego oraz numeru rozliczeniowego banku, które są potrzebne do przelewu”.

Scenariusz 2

Znajomy przesyła Ci SMS-a, w którym informuje, że chce zobaczyć zdjęcie, które oglądaliście razem, ale teraz nie ma do niego dostępu. Nie masz teraz dostępu do komputera, aby wysłać mu zdjęcie. Odpowiada: „Mogę się szybko zalogować na Twoje konto i ściągnąć zdjęcie. Jakie masz hasło?”.

Scenariusz 3

Dostajesz e-mail z adresu szkoły z informacją o tym, że dokonano włamania na konta wielu uczniów. Czytasz w nim: „Wykryliśmy ostatnio włamania na konta uczniów. Przepraszamy, że do tego doszło. Staramy się wyeliminować ten problem. Aby zresetować konto, odpowiedz na ten e-mail, podając nazwę użytkownika i hasło”.

Scenariusz 4

Otrzymujesz e-mail z banku, w którym rzeczywiście masz konto. W e-mailu czytasz, że doszło do włamania do systemu banku i trzeba jak najszybciej się zalogować, aby zmienić hasło do konta bankowego, oraz zmienić hasła na wszelkich innych kontach, jeżeli były takie same.

Spam: Tekst dla prowadzącego

W każdym ze scenariuszy zdecydujcie, czy wiadomość jest spamem i czy należy udostępnić informacje osobie, która o nie prosi. W odpowiednim polu wpiszcie odpowiedź na każde pytanie.

Scenariusz 1

Odbierasz e-mail od prawnika, który informuje Cię, że daleki krewny wskazał Cię jako spadkobiercę dużej sumy pieniędzy. W e-mailu czytasz „Aby odebrać pieniądze, proszę o przesłanie mi numeru konta bankowego oraz numeru rozliczeniowego banku, które są potrzebne do przelewu”.

Ten e-mail to najprawdopodobniej spam. Nawet jeżeli imię i nazwisko krewnego się zgadza, nadawca może udawać prawnika. O Waszym pokrewieństwie mógł się dowiedzieć w inny sposób. Udostępnianie informacji o koncie bankowym jest zawsze ryzykowne i należy zachować ostrożność. Nigdy nie wysyłaj takich informacji bez uprzedniego kontaktu, a nawet wtedy trzeba zachować dużą ostrożność. Na przykład lepiej nie wysyłać takich informacji w e-mailu, ponieważ nie jest szyfrowany. Dlatego właśnie wiele szpitali, firm prawniczych i banków ma specjalne witryny internetowe do komunikacji z klientami czy pacjentami.

Scenariusz 2

Znajomy przesyła Ci SMS-a, w którym informuje, że chce zobaczyć zdjęcie, które oglądaliście razem, ale teraz nie ma do niego dostępu. Nie masz teraz dostępu do komputera, aby wysłać mu zdjęcie. Odpowiada: „Mogę się szybko zalogować na Twoje konto i ściągnąć zdjęcie. Jakie masz hasło?”.

Choć nie jest to spam, nie należy podawać hasła innym osobom. Kiedy poznają Twoje hasło, będą mogły zablokować Ci dostęp do konta lub uzyskać dostęp do innych kont internetowych, na których masz takie samo hasło. Co więcej, jeżeli wiadomość zobaczy ktoś inny lub przechwyci ją haker, jeszcze więcej osób zyska dostęp do Twojego konta bez Twojej wiedzy.

Scenariusz 3

Dostajesz e-mail z adresu szkoły z informacją o tym, że dokonano włamania na konta wielu uczniów. Czytasz w nim: „Wykryliśmy ostatnio włamania na konta uczniów. Przepraszamy, że do tego doszło. Staramy się wyeliminować ten problem. Aby zresetować konto, odpowiedz na ten e-mail, podając nazwę użytkownika i hasło”.

Z zasady nie prosi się użytkowników o podawanie takich informacji. Nawet jeżeli nadawca nie budzi poza tym podejrzeń, trzeba założyć, że każdy e-mail z prośbą o podanie hasła to spam.

Scenariusz 4

Otrzymujesz e-mail z banku, w którym rzeczywiście masz konto. W e-mailu czytasz, że doszło do włamania do systemu banku i trzeba jak najszybciej się zalogować, aby zmienić hasło do konta bankowego, oraz zmienić hasła na wszelkich innych kontach, jeżeli były takie same.

W takim przypadku należy otworzyć nowe okno przeglądarki i przejść do witryny banku tak jak zwykle. Informacja tego typu (o włamaniu na konta) powinna być zamieszczona w portalu dla klientów banku lub innej firmy. Czynności opisane w instrukcji zamieszczonej w portalu powinny być bezpieczne do wykonania. Podobnie jak w scenariuszu 3 żadna uczciwa osoba nie powinna Cię prosić o podanie danych konta w e-mailu.