

## Internetowe oszustwa, czyli gra na EMOCJACH!

Internet stał się nieodłączną częścią naszej codzienności. Jest niezbędny do nauki czy pracy, pomaga w komunikacji, jest również pewną formą rozrywki. Jak zawsze jednak istnieje druga strona medalu. W natłoku codziennych obowiązków i pewnych przyzwyczajzeń nie wolno zapominać, że w internecie, tak jak w świecie rzeczywistym, również może pojawić się niebezpieczeństwo, przed którym należy się chronić. Sieć jest idealnym narzędziem dla cyberprzestępców, którzy znajdują nowe sposoby, aby kogoś oszukać.

Jednym z nich jest gra na emocjach, dlatego warto zachować zasadę ograniczonego zaufania i być wyczulonym na sytuacje, w których ktoś prosi nas w sieci o wsparcie finansowe, pamiętając o tym, że nie musi być tym, za kogo się podaje. Istnieje kilka konkretnych metod, o których powinieneś wiedzieć.

Jedną z najbardziej znanych jest **metoda „na wnuczka”**, która ma także swój internetowy odpowiednik. Złodziej może np. włamać się na komunikator internetowy bliskiej Ci osoby w mediach społecznościowych i podszywając się pod nią, prosić o środki finansowe. Prawdopodobnie dostaniesz wiadomość z linkiem do fałszywej strony internetowej z płatnościami, która może do złudzenia przypominać autentyczny serwis. Jeśli podasz tam swój login i hasło, oszust będzie mógł wykorzystać te dane do logowania w prawdziwym serwisie. Niestety kod SMS potrzebny do autoryzacji przekażesz złodziejowi sam, kiedy wpiszesz go niczego nieświadomy na fałszywej stronie.

Powinieneś skontaktować się z daną osobą w inny sposób, np. zadzwonić pod jej numer i upewnić się, że to faktycznie ona prosi Cię o przelew.

Więcej na temat linków do płatności i zachowywania czujności w internecie znajdziesz w filmie kampanii „Bankowcy dla Edukacji” pt. „Bądź CYBERBEZPIECZNY!: Nie klikaj w linki do płatności i nie ściągaaj załączników” – link: <https://youtu.be/aUdO0VDhEUK>

**Kolejnym sposobem jest metoda „na kod”**, zwana także **metodą „na znajomego”**.

Płatności przy użyciu kodu BLIK to bardzo wygodny sposób na wykonywanie transakcji za pomocą telefonu, możesz zapłacić nim zarówno w sklepie stacjonarnym jak i internetowym. W specjalnej bankowej aplikacji należy wygenerować 6-cyfrowy kod, który zachowuje ważność tylko przez kilka minut, wpisać go w odpowiednim miejscu, a następnie zatwierdzić transakcję w aplikacji przy użyciu PIN-u. Niestety, ta prosta forma płatności również została dostrzeżona przez cyberprzestępców. Oszuści wysyłają do jak największej liczby znajomych wiadomość, w której pytają czy dana osoba ma możliwość płacenia BLIKiem, jeżeli „ofiara” odpowie twierdząco to przestępca prosi o pomoc w uregulowaniu jakiegoś rachunku poprzez podanie kodu na czacie, jednak szybko okazuje się, że z konta zniknęła duża kwota, a nasz znajomy, którego tożsamość została wykorzystana przez złodzieja, nie wie nic o całym zajściu...

Pamiętaj, zanim podejmiesz decyzję skontaktuj się ze znajomym w inny sposób, np. zadzwoń do niego. Jeżeli jednak podasz taki kod oszustowi, od razu skontaktuj się ze swoim bankiem. W przypadku, gdy ktoś włamie się na Twoje konto na mediach społecznościowych i zacznie rozsyłać podobne wiadomości natychmiast poinformuj o tym całą swoją sieć kontaktów. Następnie zmień hasło w tym portalu oraz w innych serwisach, jeśli używasz w nich tego samego hasła.

Więcej o metodach podszywania się pod inne osoby w internecie dowiesz się, oglądając filmy: „Nie daj się oszukać: Oszustwa na BLIKa” – link: <https://youtu.be/vEemlZolAQ> i „Bądź CYBERBEZPIECZNY: Zanim cokolwiek zrobisz, ZWERYFIKUJ informacje!” – link: <https://youtu.be/N0xYooUHesQ>

Trzecią metodą jest **metoda „na znajomości”**. Obecnie wiele osób poznaje się przez internet i ten fakt potrafili wykorzystać także cyberprzestępcy. Poprzez zawieranie nowych znajomości, budowanie pozornie silnych więzi wyłudniają od innych pieniądze. Założmy, że od pewnego czasu z kimś piszesz, wydaje Ci się, że jesteście pokrewnymi duszami, wiecie o sobie wszystko, jednak ta osoba nie chce spotkać się w realu, wykorzystuje różne wymówki np. że nie ma czasu, ponieważ przygotowuje bardzo ważny projekt do pracy. Pewnego dnia prosi Cię o pożyczkę, Ty się zgadzasz, po czym ten ktoś przestaje odpisywać i okazuje się, że taka osoba nigdy nie istniała...

Pamiętaj, że dopóki nie poznasz znajomego osobiście, nie możesz mieć pewności, kto jest po drugiej stronie.

W Internecie możesz wierzyć tylko w to, co da się zweryfikować!

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę [www.bde.wib.org.pl](http://www.bde.wib.org.pl)

