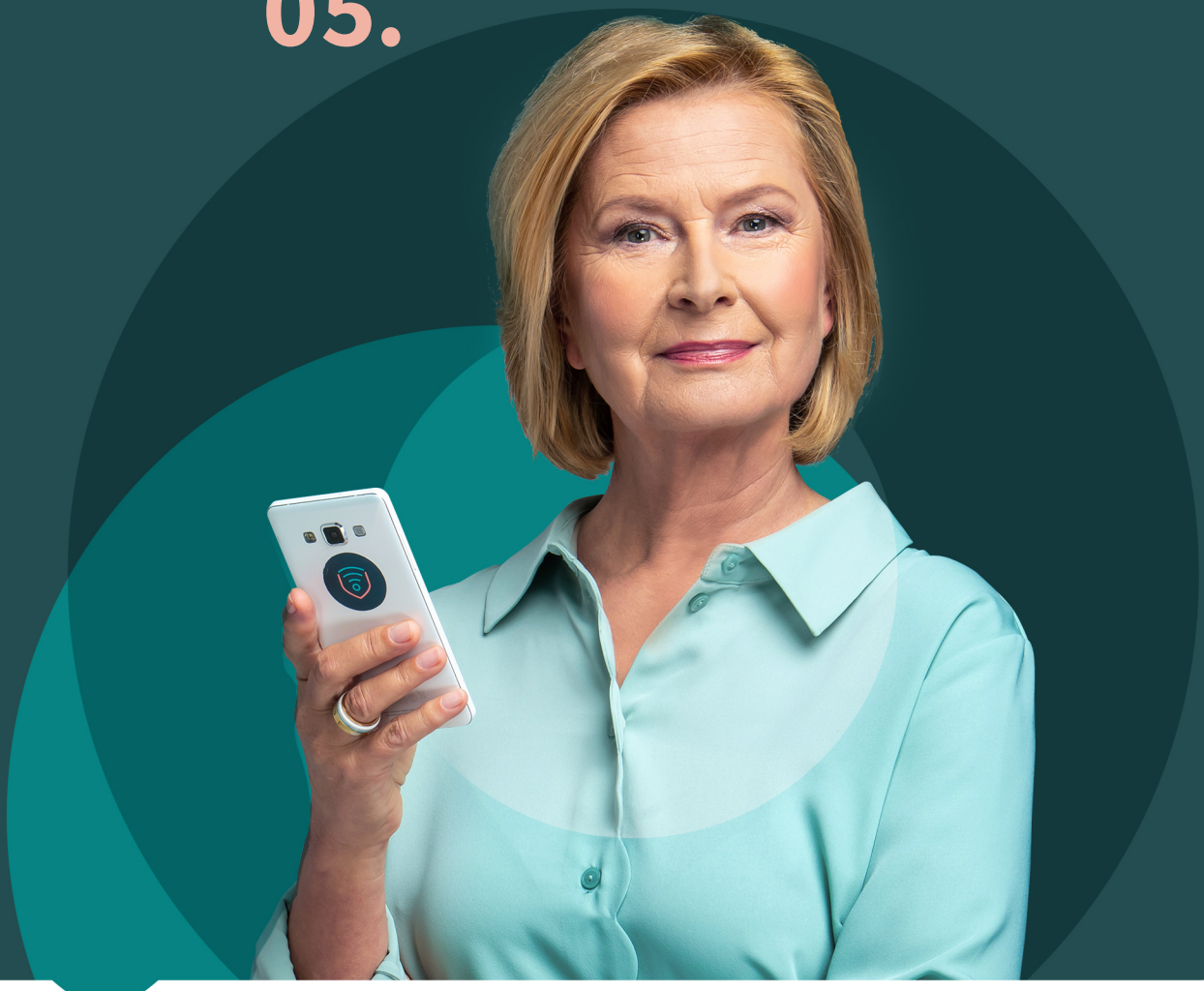
SENIORZE
spotkajmy się w sieci

#Metoda na...
czyli metody oszustw w sieci,
na które trzeba uważać.

Poradnik dla seniora

05.



Partner kampanii:

WARSZAWSKI INSTYTUT BANKOWOŚCI

Fundusze Europejskie Polska Cyfrowa

KPRM

NASK

Unia Europejska
Europejski Fundusz Rozwoju Regionalnego

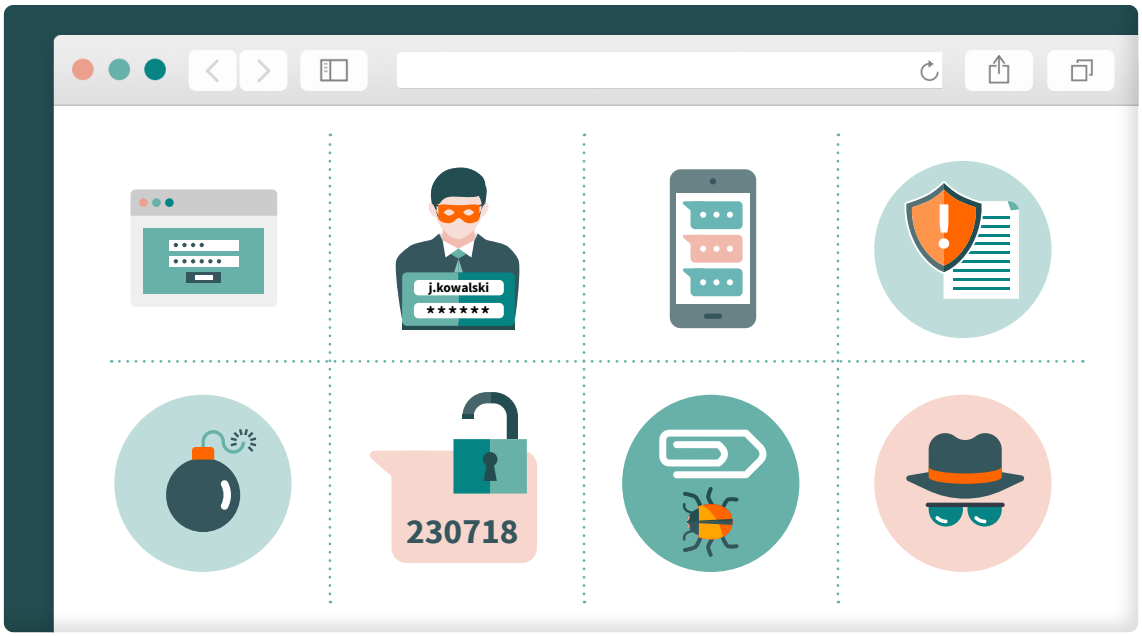
WITAJ!

W tym przewodniku wyjaśnimy Ci, jak rozpoznać powszechne metody oszustów w sieci oraz jak postępować, jeżeli na takie niebezpieczne sytuacje natrafisz.

Pamiętasz z filmu z Barbarą pt. *„Metoda na..., czyli na co powinien uważać w internecie bezpieczny senior”*, jak pewien mężczyzna przekazał swoje pieniądze złodziejowi, myśląc, że rozmawia z wnuczką? A jak znajoma naszej bohaterki dostała podejrzaną wiadomość e-mail, w której nadawca podawał się za urzędnika z ZUS? Niestety oszuści na wiele sposobów próbują wyłudzać pieniądze przez internet.

W tej broszurze omówimy różne **metody oszustw**. Skupimy się szczególnie na tych aktualnych oraz najbardziej powszechnych. Choć te sposoby są różne, opierają się na bardzo podobnych **mechanizmach**, takich jak **gra na emocjach** i **wykorzystanie zaufania do autorytetu**.

Jeżeli poznasz powszechne metody oszustów w internecie, staniesz się użytkownikiem bardziej wyczulonym na niepokojące zjawiska w sieci. Będziesz też ostrożniej korzystać z tego, co ona oferuje. Pamiętaj: internet będzie bezpiecznym miejscem, jeżeli tylko zachowasz ostrożność.



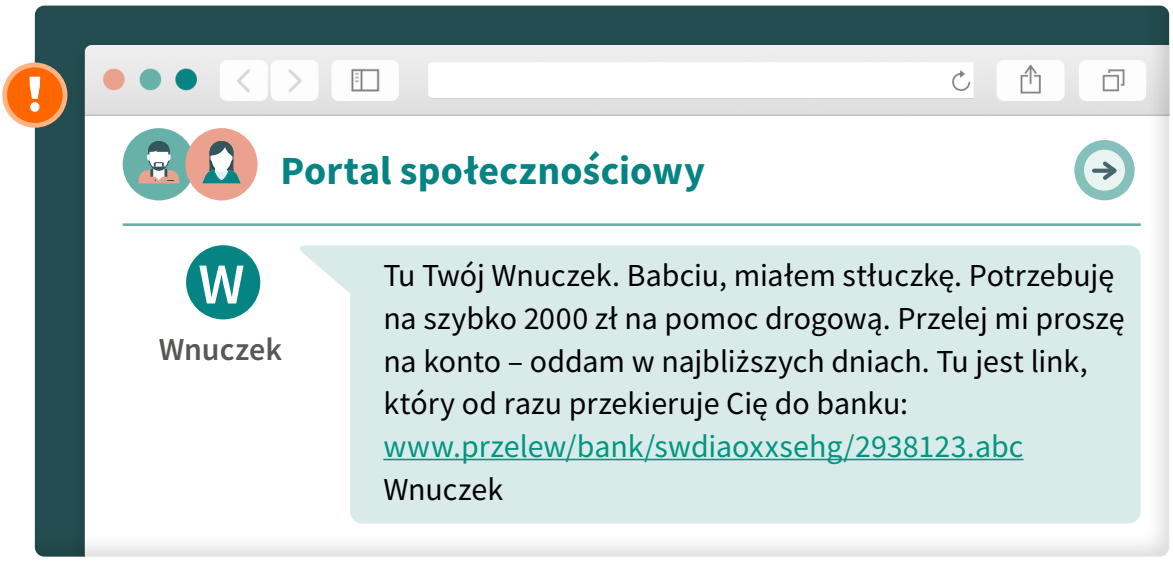
Gra na emocjach

Oszuści w internecie, żeby osiągnąć swój cel, często grają na emocjach. Nie oznacza to, że w sieci nie można polegać na własnej intuicji i odczuciach. Warto jednak 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**. Przyjrzyjmy się trzem popularnym metodom oszustw wykorzystywanym przez internetowych złodziei.

METODA „NA WNUCZKA”

Znana już chyba wszystkim z różnych doniesień medialnych metoda „na wnuczka” ma także swój **internetowy odpowiednik**. Mechanizm pozostaje niezmieniony – oszust podaje się za kogoś, kim nie jest, i usiłuje wyłudzić pieniądze.

Jak to działa? Złodziej może np. **włamać się** na **komunikator internetowy bliskiej nam osoby** np. w mediach społecznościowych i podszywając się pod nią, prosić nas o środki finansowe. W takim przypadku dostaniemy prawdopodobnie wiadomość z **linkiem** do nieprawdziwej strony internetowej z płatnościami, która może do złudzenia przypominać autentyczny serwis (Dowiedz się lub przypomnij sobie, czym jest phishing z broszury pt. *„E-mail i media społecznościowe? Wszystko, co musisz wiedzieć o bezpiecznej komunikacji w sieci”*). Gdy w niego klikniemy, nastąpi przekierowanie do **kolejnej fałszywej strony** – tym razem banku. Jeśli podamy tam nasz login i hasło, oszust będzie mógł wykorzystać te dane do logowania w prawdziwym serwisie. Niestety kod SMS potrzebny do **autoryzacji** podamy złodziejowi sami, kiedy wpiszemy go niczego nieświadomi na fałszywej stronie.



Łatwo dać się nabrać: nasza czujność osłabia się, gdy o pomoc prosi rzekomo własne dziecko czy wnuk...

Zawsze, gdy dostaniemy podejrzaną **wiadomość z prośbą o przelew**, pozwólmy sobie być **nieufni**. W takim przypadku należy **skontaktować się** z daną osobą w inny sposób, np. zadzwonić pod jej numer i upewnić się, że to faktycznie ona prosi nas o przelew. Więcej na temat linków do płatności i zachowywania czujności w internecie znajdziesz w filmie pt. *„Bądź CYBERBEZPIECZNY!: Odc. 7. Nie klikaj w linki do płatności i nie ściągaj załączników”*.

METODA „NA KOD”

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

Płatności przy użyciu kodu to bardzo wygodny sposób dokonywania bezgotówkowych transakcji. W specjalnej bankowej **aplikacji** możemy wygenerować **6-cyfrowy kod**, który zachowuje ważność tylko przez kilka minut. W tym czasie musimy **podać kod** na stronie internetowej, gdzie chcemy dokonać płatności (możemy tak też zapłacić w sklepie, wpisując go na terminalu płatniczym, kiedy płacimy za zakupy), a następnie **zatwierdzić transakcję w aplikacji** przy użyciu naszego **PIN-u**. Takiego kodu możemy używać również np. do wypłaty gotówki w bankomacie. Aby korzystać z płatności w takiej formie, wystarczy konto bankowe, odpowiednia aplikacja i wyrażona przez nas zgoda na zatwierdzanie transakcji przez telefon.

Także w tym przypadku musimy uważać na wiadomości, które za pośrednictwem komunikatora w mediach społecznościowych przesyła rzekomo bliska nam osoba.

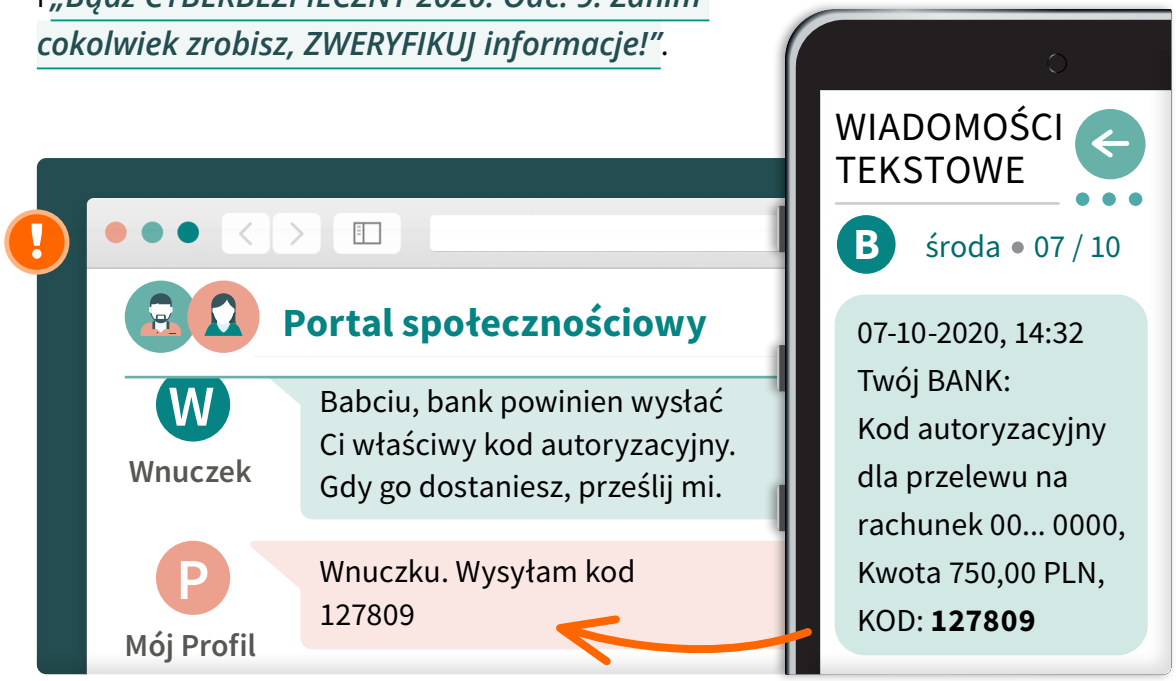
Wyobraź sobie, że

dostajesz wiadomość sms, w której znajomy napisał, że potrzebuje **jednorazowego, niewielkiego wsparcia finansowego** i prosi o przesłanie kodu ze specjalnej aplikacji bankowej, służącej do szybkich płatności. Gdy podamy mu kod, szybko okazuje się, że z konta zniknęła duża kwota, a nasz znajomy, którego tożsamość została wykorzystana przez złodzieja, nie wie nic o całym zajściu…

Co powinieneś zrobić, gdy otrzymasz wiadomość od kogoś znajomego z prośbą o np. 20 zł, które ta osoba może dzięki Tobie za chwilę wypłacić z bankomatu za pomocą przekazanego przez Ciebie kodu? Najpierw **skontaktuj się ze znajomym w inny sposób**, np. zadzwoń do niego. Tylko w ten sposób dowiesz się, czy o kod naprawdę poprosiła Cię właśnie ta osoba, czy może to złodziej chciał wyłudzić od Ciebie pieniądze.

Jeżeli pod wpływem emocji jednak podasz taki kod oszustowi, od razu **skontaktuj się ze swoim bankiem**. Może też zdarzyć się tak, że ktoś włamie się na Twoje konto w portalu społecznościowymi i wyśle z niego wiadomości z prośbą o kod do Twoich znajomych. Co wtedy zrobić? Przede wszystkim od razu **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: Odc. 1 – Oszustwa na BLIKa”* i *„Bądź CYBERBEZPIECZNY 2020: Odc. 9. Zanim cokolwiek zrobisz, ZWERYFIKUJ informacje!”*.



METODA „NA ZNAJOMOŚCI”

Oszuści w sprytny sposób wykorzystują fakt, że obecnie wiele osób **poznaje się online** i za pośrednictwem sieci tworzy często bliskie relacje. Złodzieje mogą wyłudzać pieniądze metodą „na znajomości”. Na czym ona polega? Jak czytamy na stronie *www.dokumentyzastrzezone.pl*: „ofiara poznaje kogoś przez internet, związuje się z tą osobą, a następnie jest proszona o przysłanie pieniędzy”.

Wyobraź sobie, że

od dłuższego czasu piszesz online z Tomkiem Kowalskim. Czujesz, że wszystko już o sobie wiecie, mimo że nie mieliście jeszcze okazji spotkać się „na żywo". Nic bardziej mylnego! Dopóki nie poznasz znajomego osobiście, nie możesz mieć pewności, kto jest po drugiej stronie. A co, jeśli przekażesz takiej osobie środki, a później na policji okaże się, że ktoś taki nie istnieje? No właśnie…

W internecie możesz wierzyć tylko w to, co da się zweryfikować. Gdy chcesz komuś zaufać, spotkaj się z tą osobą w prawdziwym świecie, jeżeli do tej pory rozmawialiście tylko przez internet.

PAMIĘTAJ

Po wnikliwym zapoznaniu się z tym podrozdziałem wiesz już, o czym musisz zawsze pamiętać.

1. Metody internetowych oszustów często opierają się na **grze na emocjach**.
2. Jeżeli bliska osoba prosi Cię w sieci o pieniądze, **zweryfikuj jej tożsamość**. W razie wyłudzenia – skontaktuj się ze swoim bankiem.
3. Ktoś rozsyła coś z Twojego konta w mediach społecznościowych? Powiadom o tym swoją sieć kontaktów i zmień hasło.
4. Nie przekazuj swoich pieniędzy osobom, które znasz tylko z sieci.

Wykorzystanie zaufania do instytucji

Internetowi oszuści często podają się za zaufane instytucje, np. ministerstwa, ZUS, Urząd Skarbowy czy banki komercyjne. Chcą **zainfekować złośliwym oprogramowaniem** nasze urządzenia lub, jak w przypadku metod związanych z grą na emocjach, **przejąć nasze dane dostępu** do różnych systemów. Dla użytkowników wiąże się to z koniecznością **zachowania ostrożności** w przypadku wiadomości, które uzyskujemy drogą mailową.

METODA „NA ZUS”

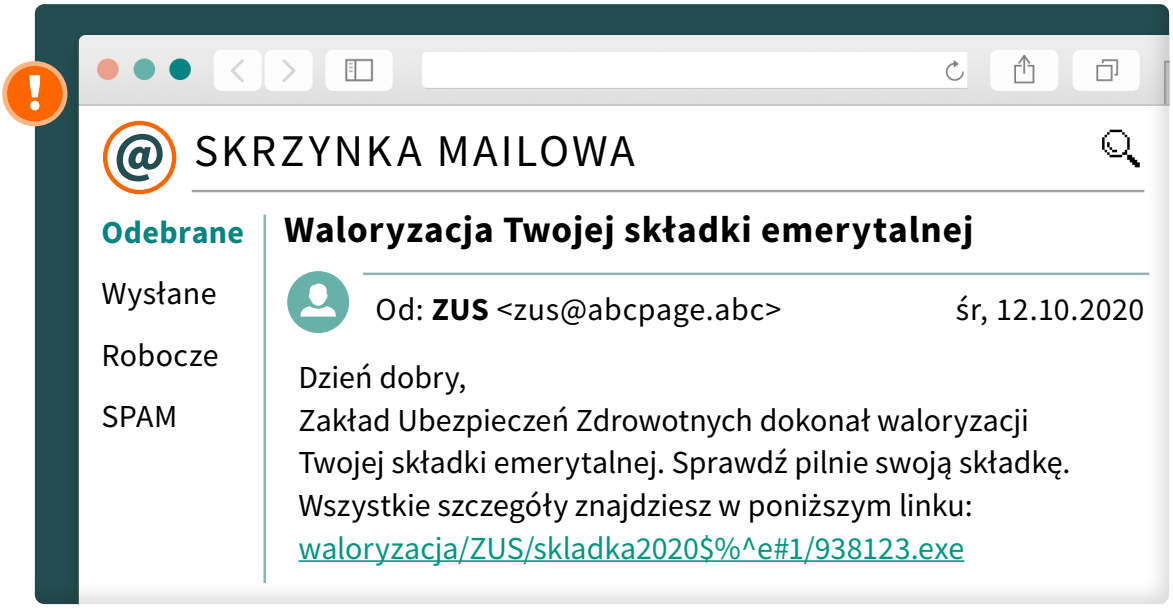
> ***METODA „NA ZUS”*** – za pomocą wiadomości e-mailowych, w których nadawca podaje się za Zakład Ubezpieczeń Społecznych, oszuści wysyłają niebezpieczne linki lub załączniki z jasnym wskazaniem, że należy w nie kliknąć lub pobrać je na swoje urządzenie.

Innymi słowy, dostajemy **e-mail z załącznikiem od jednostki administracji publicznej**, np. z tematem „Składki zdrowotne”, ale faktycznie nie jest to żadna instytucja, a podszywający się pod nią oszust. Załączone do wiadomości pliki, po ich otwarciu, otwierają im **dostęp do naszych urządzeń**. Zawierają one zwykle rozszerzenia (czyli końcówkę nazwy) takie jak: „js”, „vps”, „jse”, „exe”, „scr” i inne. Jeżeli klikniemy w taki plik celem pobrania, ściągniemy tym samym na nasze urządzenie złośliwe oprogramowanie, a cyberoszuści uzyskają dostęp do naszych plików i systemu.

Oszuści mogą też ukrywać prawdziwe rozszerzenia plików, a w ich nazwach zapisywać inne, znane i zaufane rozszerzenia, np. „pdf”. (Więcej na ten temat dowiesz się, oglądając film pt. *„Bezpieczeństwo działań w sieci: Odc. 1 – Mylące rozszerzenia plików”*). Co więc robić, gdy otrzymasz wiadomość od Zakładu Ubezpieczeń Społecznych z informacją, aby pobrać załącznik i potwierdzić zgodność rozliczeń? Oczywiście **w nic nie klikać**! Najpierw sprawdź **wygląd załącznika**, ale nawet jeżeli nie będzie budził Twoich podejrzeń, skontaktuj się **telefonicznie z daną instytucją i zweryfikuj**, czy taki e-mail jest prawdziwy i rzeczywiście zaufany. Pamiętaj też, aby w ustawieniach swojego urządzenia sprawdzić, czy masz odznaczoną funkcję „ukryj rozszerzenia plików” – pozwoli to nie dać się zwieść fałszywym nazwom plików.

Innym sposobem oszustwa może być **przesłanie nam linku**, po kliknięciu w który **przeniesiemy się na fałszywą stronę**. Może to być witryna do transakcji płatniczych lub do bankowości internetowej, gdzie – podobnie jak w przypadku metody na wnuczka – podajemy dane do logowania i kod SMS, a oszuści je przejmują.

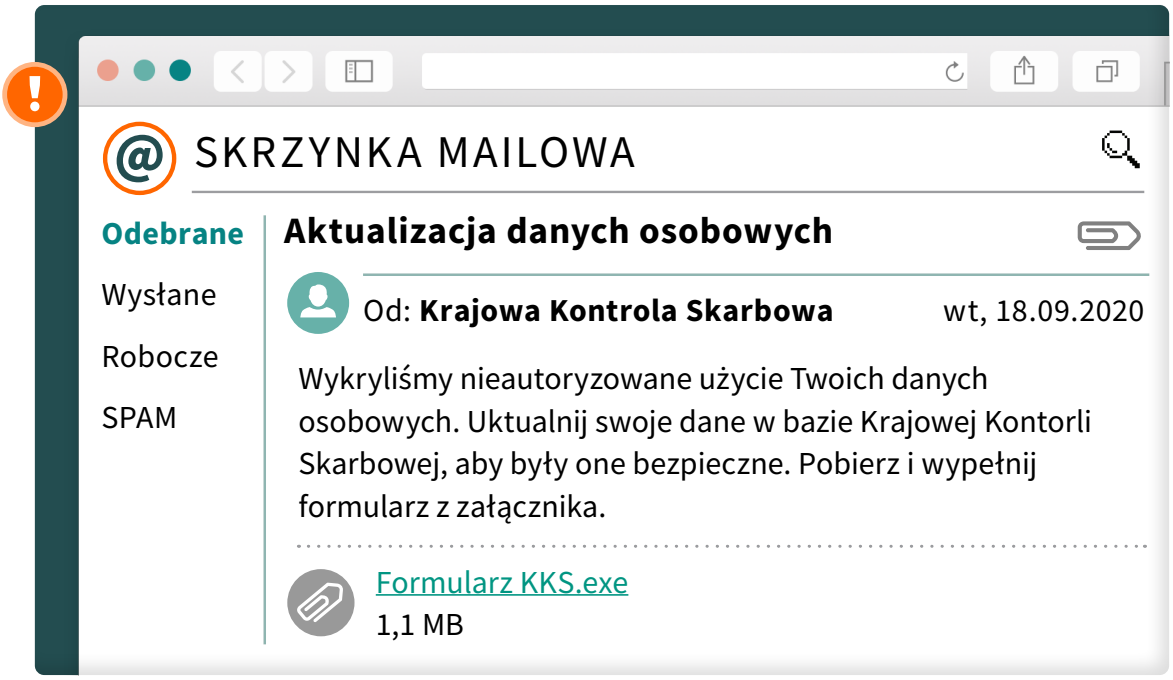
Ta technika jest wykorzystywana często także w innych odsłonach. Możemy np. dostać od banku wiadomość **SMS z linkiem do strony**, na której dowiadujemy się, że np. rzekomo widniejemy na liście zadłużeń na niewielką kwotę. Takie metody bywają również wykorzystywane przez oszustów podających się za komornika. (Obejrzyj film pt. *„Nie klikaj bezrefleksyjnie w linki przesłane mailem”*, aby dowiedzieć się więcej o niebezpiecznych linkach). W tym przypadku również nie klikajmy w żaden przesłany link, a zamiast tego zadzwońmy do danego banku lub instytucji celem zweryfikowania zaistniałej sytuacji. Więcej na temat tego typu zjawisk dowiesz się z filmu pt. *„Nie daj się oszukać: Odc. 3 – Cyberprzestępcy podszywają się pod różne instytucje”*.



METODA „NA KRAJOWĄ KONTROLĘ SKARBOWĄ”

METODA „NA KRAJOWĄ KONTROLĘ SKARBOWĄ” – sposób oszustwa polegający na rozsyłaniu wiadomości e-mail, w których adresat podaje się za zaufaną instytucję, w tym przypadku Krajową Kontrolę Skarbową. W wiadomościach tych oszuści zachęcają do pobrania i otworzenia załączników, informując, że jest to urzędowy (czyli zaufany) formularz do wypełnienia.

Ministerstwo Finansów przestrzegało niedawno przed e-mailami, których adresat podawał się za pracownika Krajowej Administracji Skarbowej i prosił o wypełnienie załączonych formularzy. Dowiedz się więcej na ten temat z artykułu pt. *„UWAGA na fałszywe wiadomości e-mail nt. Krajowej Kontroli Skarbowej”*.



Co powinieneś zrobić, gdy otrzymasz taką niepokojącą wiadomość e-mail?

1. Spójrz na **rozszerzenie załączonego pliku** – sprawdź, czy nic Cię nie niepokoi i najlepiej włącz opcję widocznych rozszerzeń.
2. **Zweryfikuj**, czy **adres e-mailowy** nie jest podejrzany, a w treści nie ma błędów i literówek.
3. **Zadzwoń do danej instytucji** w celu zweryfikowania zaistniałego zdarzenia.
4. **Zachowaj spokój** i do czasu uzyskania całkowitej pewności nie wykonuj żadnych pochopnych czynności.
5. **Skontaktuj się z kimś zaufanym** z rodziny, znajomych i opowiedz o zdarzeniu.

Jak widzisz, oszuści znajdują kolejne sposoby na wykorzystanie zaufania do instytucji państwowych. W jednym przypadku włamują się do naszych systemów przez pliki, które otwieramy z **załącznika**, w innych zdobywają nasze dane za pośrednictwem **linków** albo proszą o wypełnienie **formularza**. Dlatego, pomimo znajomości ogólnych zasad ochrony przed oszustami w sieci, warto raz na jakiś czas sprawdzać **aktualności** zamieszczane na stronach internetowych, które przestrzegają przed tego typu niebezpiecznymi zdarzeniami. Można to sprawdzić np. na stronie: *http://dokumentyzastrzezone.pl/category/aktualnosci/*.

METODA „SPYWINDOW"

Oszuści wykorzystują zaufanie nie tylko do **instytucji państwowych**, ale także do **bankowych**.

> ***METODA „SPYWINDOW"*** *(ang. „okno szpiegowskie")* polega na tym, że oszust, podając się za pracownika banku, zachęca do otworzenia teoretycznie bezpiecznego dokumentu. Żeby to zrobić, musimy podać nasze dane do logowania. SpyWindow przesyła te dane oszustowi, a do nas przychodzi fałszywe potwierdzenie autoryzacji.

Jak to rozumieć? Za namową oszustów, podających się za pracowników naszego banku, instalujemy złośliwe oprogramowanie, myśląc, że jest to bezpieczne. Następnie, aby otworzyć plik z dokumentem, podajemy nasze dane logowania, udostępniając je tym samym oszustom. Więcej na temat tego mechanizmu można dowiedzieć się, oglądając film pt. *„Bądź CYBERBEZPIECZNY 2020: Odc. 4. SpyWindow, czyli moc socjotechniki"*.

O czym więc trzeba pamiętać? **Nie przekazuj** swoich danych logowania oraz żadnych innych danych osobom podającym się za pracowników banku. **Nie wpisuj** ich również w miejscach, które nie są **oficjalną stroną logowania** do banku lub **oficjalną aplikacją bankową** – nawet jeżeli ktoś podaje się za pracownika banku i mówi Ci, że jest inaczej. Warto zawsze **zweryfikować**, czy osoba, z którą rozmawiamy, rzeczywiście jest pracownikiem danej instytucji.

PAMIĘTAJ

Po wnikliwym zapoznaniu się z tym podrozdziałem wiesz już, o czym zawsze musisz pamiętać.

1. Jeżeli otrzymasz e-mail od zaufanej instytucji państwowej, zwróć uwagę na **adres** i **treść wiadomości** – zastanów się, czy nic nie budzi Twoich podejrzeń. Sprawdź **rozszerzenie pliku**, zanim go otworzysz, ponieważ jego nazwa może posiadać wprowadzający w błąd skrót rozszerzenia.

2. Zanim otworzysz otrzymany plik, **skontaktuj się z daną instytucją telefonicznie**. Pozwoli to na weryfikację prawdziwości zdarzenia.

3. **Nie klikaj** również **w żadne linki** przesyłane w tego typu wiadomościach. Nie wpisuj swoich danych logowania i innych danych wrażliwych na stronach podanych w treści e-maila.

4. To, że ktoś podaje się za pracownika Twojego banku, nie znaczy, że nim jest. **Zweryfikuj** to.

5. **Nie przekazuj swoich danych logowania** do bankowości internetowej w żadnym innym miejscu niż oficjalna strona banku oraz jego oficjalna aplikacja – nawet jeśli prosi Cię o to ktoś, kto podaje się za zaufaną osobę.

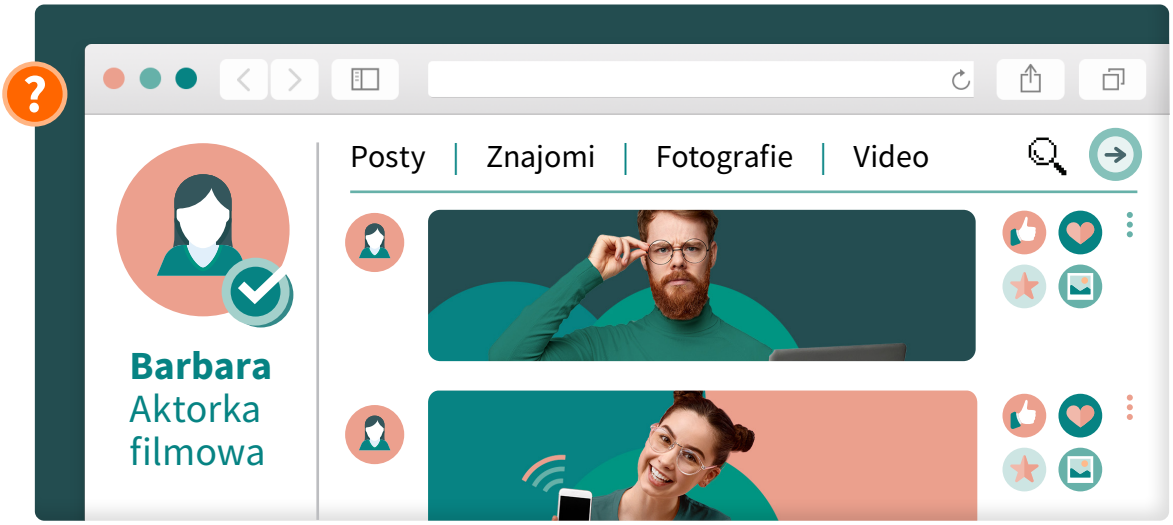
Zasada ograniczonego zaufania w internecie

Internetowi oszuści wykorzystują też inne mechanizmy, np. zaufanie do rozpoznawalnej osoby (lidera opinii), zaufanie do innych użytkowników czy też – wykorzystywanie aktualnych tematów, które dotyczą szerokich grup.

ZAUFANIE DO ZNANYCH OSÓB

METODA „NA ZNANE OSOBY” polega na tym, że oszuści podają się w mediach społecznościowych za sławne osoby i wykorzystując ich status, udostępniają linki, które mogą zawierać wirusy.

Wiemy już, że nie należy klikać w żadne linki automatycznie, tylko wcześniej **sprawdzić ich prawdziwość**. Warto też zwrócić uwagę, czy **profil**, z którego link został udostępniony, zawiera **oznaczenie**, że jest zweryfikowany jako bezpieczny. Jest to najczęściej specyficzny znak znajdujący się przy nazwie użytkownika, np. drobna ikona (przykład zobaczysz na grafice poniżej). Więcej na temat tego typu oszustwa dowiesz się, oglądając film pt. *„Bądź CYBERBEZPIECZNY 2020: Odc. 8. Uważaj na fałszywe konta!”*.

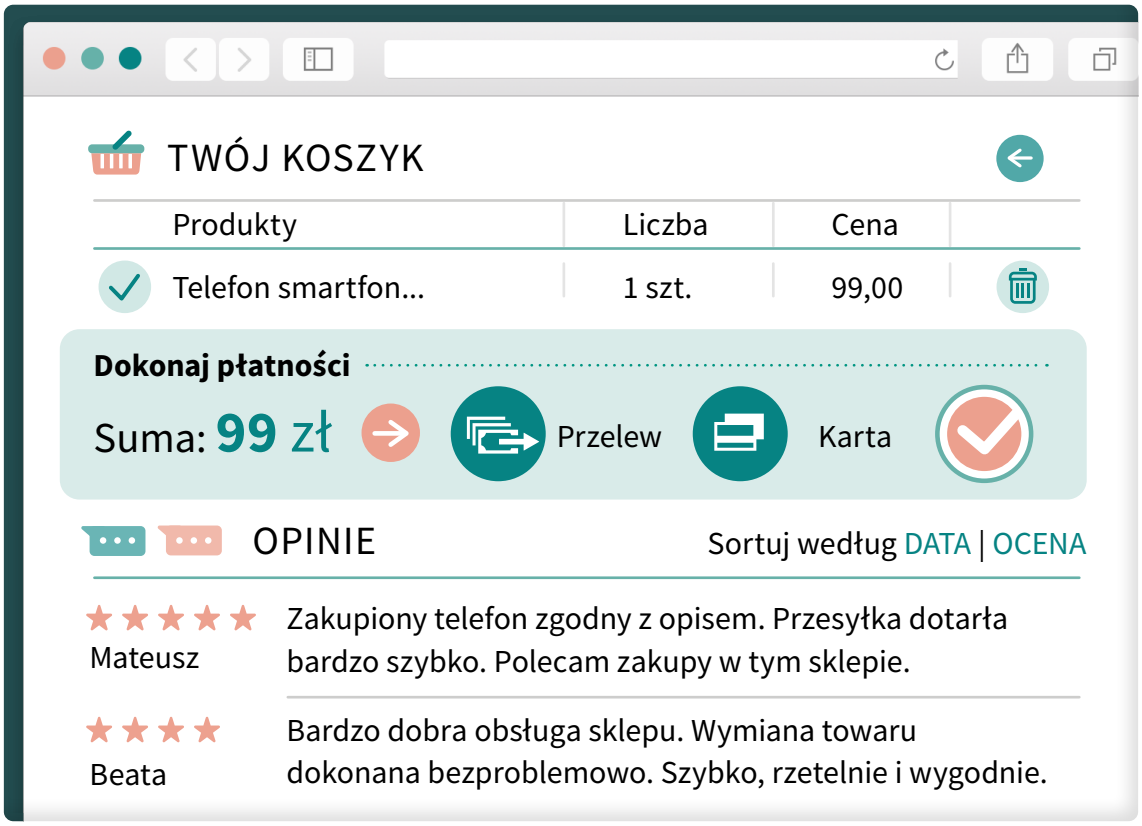


ZAUFANIE DO INNYCH UŻYTKOWNIKÓW

METODA „NA ZAKUPY PRZEZ INTERNET” to, jak czytamy na stronie *www.dokumentyzastrzezone.pl*: „prośba o przesłanie pieniędzy w celu zapłaty za produkt, przedmiot aukcji lub usługę reklamowaną przez internet”.

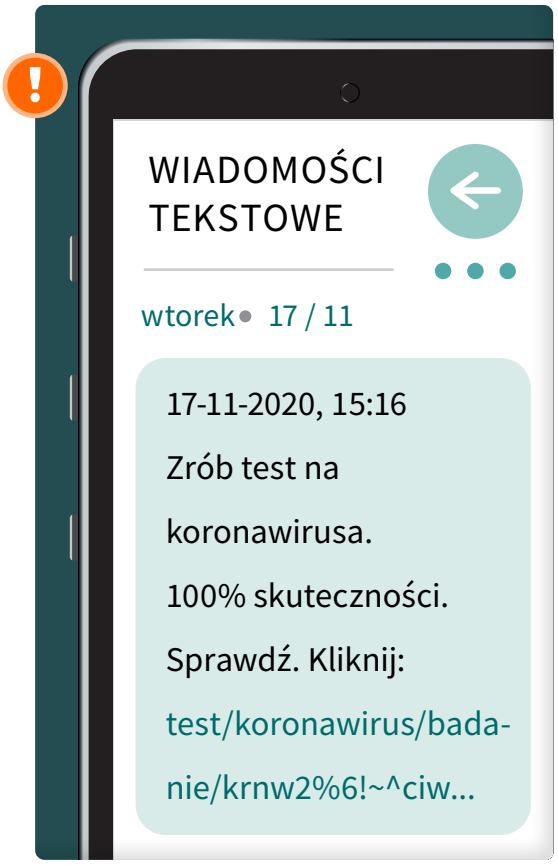
Istnieją portale, na których użytkownicy udostępniają innym osobom produkty lub usługi. Klient dokonuje płatności i czeka na swój zakup, ale kontakt ze sprzedawcą nagle się urywa, zaś pokrzywdzony zostaje z niczym.

Aby się uchronić przed oszustwem, transakcji dokonuj tylko **w pewnych i sprawdzonych miejscach**, u użytkowników, którzy są zaufani i mają dobre opinie. Niech Twoją podejrzliwość wzbudzą oferty produktów lub usług, które są np. znacznie tańsze, niż powinny być.



POCZUCIE BRAKU WYJŚCIA, CZYLI POTRZEBNE ŚRODKI MEDYCZNE

METODA „NA KORONAWIRUSA” pokazuje, że oszuści szybko reagują na aktualne wydarzenia i próbują wykorzystywać je do swoich działań.



Czasami złodzieje próbują się wzbogacić, wykorzystując poczucie niepewności i zagrożenia, jakie towarzyszy nam podczas pandemii koronawirusa. Oszuści rozsyłają wiadomości SMS z linkami, za pomocą których **wyłudzają dane logowania** do bankowości lub **zachęcają do pobierania na urządzenie złośliwego oprogramowania**. Przesyłane komunikaty przekazują nieprawdziwe informacje na temat COVID-19, np. związane z refundacją szczepionki. Więcej informacji na ten temat znajdziesz w artykule pt. *„Uwaga na oszukańcze ogłoszenia związane z epidemią koronawirusa (COVID-19) ”*.

PAMIĘTAJ

Po wnikliwym zapoznaniu się z tym podrozdziałem wiesz już, o czym musisz zawsze pamiętać.

1. Pamiętaj, że oszuści mogą zakładać **fałszywe konta w mediach społecznościowych**, aby podszywać się pod znane osoby. Niezależnie, kto publikuje dany link – nie klikaj w nic bez wcześniejszego sprawdzenia.
2. **Sprawdzaj sprzedawców w internecie** i dokonuj transakcji tylko u tych zaufanych.
3. Wszystkie informacje, jakie otrzymujesz w podejrzanych wiadomościach, **zawsze sprawdzaj w oficjalnych miejscach**.

Jak zgłosić incydent w sieci?

Widzisz zagrożenie w sieci? Reaguj, zgłoś je do **CERT Polska**. Jak już wiesz z broszury pt. *„Antywirus i zaślepka? Wszystko, co musisz wiedzieć o programach i narzędziach zwiększających Twoje bezpieczeństwo w sieci. Poradnik dla seniora”* na stronie **www.cert.pl** można nie tylko zapoznać się z aktualnościami na temat bezpieczeństwa w sieci oraz dowiedzieć się o najważniejszych cyberzagrożeniach. Portal daje też możliwość zgłaszania różnego rodzaju niebezpiecznych zdarzeń w sieci. Jeśli trafiłeś na oszusta – wejdź na **https://incydent.cert.pl/** i zgłoś incydent.

Co już wiesz o metodach oszustów w sieci?

- Wiesz, że metody „na wnuczka”, „na kod” i „na znajomości” opierają się na **grze na emocjach**. Znasz ich mechanizm i wiesz, jak się przed nimi uchronić.
- Wiesz, że metody „na ZUS”, „na Krajową Kontrolę Skarbową” i „SpyWindow” opierają się na **zaufaniu do różnych instytucji** państwowych, bankowych i innych. Znasz ich mechanizm i wiesz, jak się przed nimi uchronić.
- Wiesz, że istnieje też wiele innych metod, które oszuści stale dostosowują do **aktualnych wydarzeń**. Znając mechanizmy i działania profilaktyczne, dużo łatwiej jest Ci wyłapać zagrożenie w gąszczu informacji.

Zobacz pozostałe filmy instruktażowe i broszury na temat bezpiecznego korzystania z internetu:

- **na stronie internetowej kampanii** „Seniorze – spotkajmy się w sieci”:

  https://www.gov.pl/seniorze-spotkajmy-sie-w-sieci

Po więcej informacji na temat bezpieczeństwa w sieci możesz się udać:

- **na stronę gov.pl**, na której znajduje się dużo ciekawych materiałów na temat korzystania z sieci oraz cyberbezpieczeństwa:

  https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

- **na stronę cert.pl**, gdzie można dowiedzieć się o najważniejszych cyberzagrożeniach i zgłosić różnego rodzaju niebezpiecznych zdarzeń w sieci:

  https://www.cert.pl/

- **na stronę System DOKUMENTY ZASTRZEŻONE**, z której możesz czerpać informacje o aktualnych zjawiskach związanych z bezpieczeństwem dokumentów – w tym bankowości internetowej:

  https://dokumentyzastrzezone.pl/category/aktualnosci/

- **na kanał Fundacji Warszawski Instytut Bankowości**, na którym znajdziesz bardzo dużo edukacyjnych filmów, związanych między innymi z bezpieczeństwem seniora w sieci:

  https://www.youtube.com/channel/UC0hP7yAJ58bkWJnsnf-hHhw

Seniorze

– spotkajmy się w sieci i korzystajmy z niej **bezpiecznie**.
Teraz widzisz, jakie to proste!

Publikacja powstała w ramach kampanii „Seniorze – spotkajmy się w sieci”.
Kampania została zrealizowana przez Ministerstwo Cyfryzacji (obecnie: KPRM) i Państwowy Instytut Badawczy NASK we współpracy z Warszawskim Instytutem Bankowości – laureatem konkursu pt. „(Nie)Bezpieczni w sieci – konkurs dla NGO na najlepszą kampanię edukacyjną”. Jest ona współfinansowana ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa.

Konsultacja merytoryczna:
Fundacja Warszawski Instytut Bankowości
Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji (obecnie: KPRM)

Redakcja i korekta językowa:
Zespół Programów Edukacyjno-Informacyjnych,
Państwowy Instytut Badawczy NASK

Layout, projekt okładki i skład:
Bringmore Advertising

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne 4.0 Międzynarodowa Licencja Publiczna (CC BY-NC)

Państwowy Instytut Badawczy NASK
ul. Kolska 12
01-045 Warszawa

Wydanie I
Warszawa 2020

Partner kampanii:

WARSZAWSKI INSTYTUT BANKOWOŚCI

Fundusze Europejskie Polska Cyfrowa

KPRM

NASK

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

SENIORZE
spotkajmy się w sieci

Zobacz i pokaż bliskim

www.gov.pl/seniorze-spotkajmy-sie-w-sieci

Partner kampanii:

WARSZAWSKI INSTYTUT BANKOWOŚCI

Fundusze Europejskie Polska Cyfrowa

KPRM

NASK

Unia Europejska
Europejski Fundusz Rozwoju Regionalnego