**Jak rozpoznać oszustwa online?**

**Aż 38% Polaków[[1]](#footnote-1) padło ofiarą oszustwa podczas zakupów online. W łatwy sposób można stracić wiele czasu, nerwów a nawet pieniędzy. Oszuści nie są idealni i zostawiają ślady, dzięki którym łatwiej zorientować się, że ktoś próbuje przejąć nasze konto, ukraść nam cyfrową tożsamość czy po prostu pieniądze.**

Duża część oszustw wykorzystuje wiadomości tekstowe. Ten typ ataku jest tak częsty, że aż otrzymał swoją nazwę – smishing. SMS ma uśpić naszą czujność oraz sprawić wrażenie, że sprawa jest pilna na przykład zatrzymanie przesyłki, która wymaga dopłaty. Każdy taki sms zawiera link do bramki płatności, na której możemy zapłacić niewielką opłatę, aby nasza paczka została do nas doręczona czy też rzekomą dopłatę za prąd. Taka strona jest oczywiście fałszywa. Jej celem jest wyłudzenie danych naszych kart płatniczych lub zapisanie do usługi, która cyklicznie będzie pobierać opłatę. Nie jest to jedyna opcja mająca skłonić osoby do wykonania płatności. Podobny mechanizm miały ataki sugerujące niedopłatę do rachunku za prąd, usługi telekomunikacyjne, a nawet niedopłatę za sprawę sądową.

Link do fałszywej płatności w wiadomości SMS to nie jedyna opcja oszustwa. Mogą to być również wiadomości próbujące przekonać nas do pobrania aplikacji z niezaufanego źródła. Preteksty są różne: aplikacja do śledzenia przesyłki czy rzekoma aktualizacja aplikacji bankowej. Cel oszustów jest prosty: przejęcie kont bankowych oraz kradzież pieniędzy. Taka złośliwa aplikacja może działać w tle, przechwytywać dane wpisywane przy użyciu klawiatury lub emulować wciskanie elementów interfejsu ekranowego czy też klawiszy na wirtualnej klawiaturze.

Kolejnym typem oszustw są fałszywe e-maile. Wiadomość, której nadawca podszywa się na przykład pod Netflixa kopiując również całą szatę graficzną może spowodować, że ofiara szybciej uwierzy w wiarygodność takiego maila, niż gdyby dostała smsa. Ten rodzaj oszustwa niewiele różni się od wcześniej wspomnianych wiadomości sms. Po kliknięciu w link znajdujący się w wiadomości, ofiara jest nakłaniana do zapłaty rzekomo należnej kwoty. Kolejnym typem złośliwych wiadomości e-mail to te, które mają zainfekowany załącznik. Po pobraniu oraz otworzeniu takiego pliku, na urządzeniu instalowany jest wirus, który pozwala uzyskać oszustowi pełną kontrolę nad urządzeniem.

Wiadomości sms oraz e-mail to niestety nie jedyne metody oszustów. Portale ogłoszeń takie jak Allegro czy OLX walczą z plagą wyłudzeń. Ze sprzedającym kontaktuje się potencjalny kupiec, który próbuje przekonać, że jest zainteresowany zakupem. Następnie wysyła sprzedającemu linka do fałszywej bramki płatniczej. Rzekomo zapłata za towar ma wpłynąć na rachunek karty, której dane poda sprzedający. Skradzione w ten sposób dane karty płatniczej posłużą oczywiście do kradzieży wszystkich pieniędzy, jakie znajdowały się na koncie. Inny możliwy scenariusz to potwierdzenie sprzedaży poprzez zalogowanie się na stronie, do której link otrzymujemy mailowo. Logujemy się podając dane pozwalające na dostęp do naszego konta bankowego.

**Jak nie zostać oszukanym?**

Zawsze należy zwracać uwagę kto jest nadawcą wiadomości. Firmy do kontaktu z klientami zazwyczaj używają jednego adresu, numeru telefonu czy nazwy. Istnieją niestety narzędzia, które pozwalają oszustom spreparować wiadomość tak, aby wyglądała na wysłaną z prawdziwego i prawidłowego adresu czy numeru telefonu. Kolejną wskazówką mogą być błędy językowe. Oszuści często używają narzędzi do automatycznego tłumaczenia, które sprawiają, że tekst nie wygląda na napisany przez osobę, dla której dany język jest ojczysty. Nie powinno się klikać w żadne linki, których nie jesteśmy pewni. Łącze wykorzystujące skracacz linków z wielkim prawdopodobieństwem prowadzi do fałszywej strony lub aplikacji. Należy także upewnić się, że w łączu nie ma literówek – wykupowanie domen przypominających te prawdziwe (tzw. typosquatting) to częsta metoda cyberprzestępców. W przypadku podejrzanych wiadomości mailowych, warto sprawić adres nadawcy. Jeśli link, który otrzymaliśmy jest podejrzany, możemy go zgłosić do [CERT](https://incydent.cert.pl/#!/lang=pl). W przypadku wiadomości sms wystarczy skorzystać z funkcji przekaż. Dostaniemy możliwość wpisania numeru odbiorcy (799-448-084), a następnie wysyłamy jak każdy inny sms. Powinniśmy po chwili otrzymać potwierdzenie przyjęcia zgłoszenia.

Pomocne informacje można także znaleźć w [Encyklopedii Cyberoszustw Surfshark](https://surfshark.com/research/data-breach-impact/cybercrimes). Serwis opisuje typowe oszustwa – jak działają i w jaki sposób je rozpoznać.

**O Surfshark**

*Surfshark to globalna firma zajmująca się rozwiązaniami w zakresie ochrony prywatności założona na Litwie. Surfshark jest jednym z trzech najlepszych na świecie dostawców VPN i jednym z niewielu uznanych przez niezależnych ekspertów ds. cyberbezpieczeństwa. W 2021 w konkursie Cybersecurity Excellence Awards Surfshark zdobył złoty medal i tytuł najbardziej innowacyjnej usługi cyberbezpieczeństwa roku. W 2022 Surfshark po połączeniu się z Nord Security, został drugim oficjalnym jednorożcem na Litwie.*

**Więcej informacji udzielą:**

Paulius Udra

PR Manager Surfshark

[paulius@surfsharkpress.com](mailto:paulius@surfsharkpress.com)

+370 645 26125

Arkadiusz Sęga

Senior Account Executive, Grayling Poland

arkadiusz.sega@grayling.com

+48 601 960 875

1. <https://nordvpn.com/pl/blog/online-shopping-survey-results/> [↑](#footnote-ref-1)