InternetowyKantor.pl

Poradnik

Jak nie wpaść w pułapkę cyberoszustów?

Wstęp

Przeniesienie do sieci znacznej części naszej aktywności – od zarządzania finansami, przez zakupy, aż po rozrywkę – nie oznacza jedynie samych korzyści. Wraz z nowymi możliwościami i udogodnieniami rośnie również liczba cyberzagrożeń, które mogą się wiązać ze stratami finansowymi, ujawnieniem wrażliwych informacji, utratą naszych danych czy kradzieżą tożsamości.

Jakie pułapki zastawiają na nas oszuści? Mogą to być fałszywe strony internetowe podszywające się pod zaufane instytucje (np. banki czy firmy kurierskie). Coraz częściej stosowane są także phishingowe wiadomości e-mail i SMS, które mogą wyglądać jak autentyczne powiadomienia o problemach z rachunkiem lub paczką, na którą czekasz. Naszą czujność powinny też wzbudzić obietnice łatwego zarobku lub inwestycje „gwarantujące" szybki zwrot pieniędzy – w rzeczywistości takie „okazje" mają na celu wyłudzenie środków lub danych osobowych.

Jak chronić się przed zagrożeniami online? W tym e-booku przedstawiamy najpopularniejsze rodzaje ataków oraz skuteczne sposoby na obronę. Piszemy o profilaktyce i edukacji z zakresu cyberbezpieczeństwa – z perspektywy indywidualnych użytkowników i firm. Bądźmy razem bezpieczni w sieci.

Zachęcamy do lektury!

Spis treści

5 zasad bezpieczeństwa w internecie

1

Korzystaj z dwustopniowej weryfikacji

Używanie dwustopniowego uwierzytelniania (2FA – *Two-Factor Authentication*) dodaje warstwę ochrony do logowania na konta. Nawet jeśli oszust uzyska dostęp do Twojego hasła, nie będzie mógł zalogować się bez drugiego czynnika, np. kodu SMS lub aplikacji uwierzytelniającej.

2

Twórz unikatowe, silne hasła

Stosowanie długich, skomplikowanych haseł, które zawierają różne znaki (duże i małe litery, cyfry, znaki specjalne) i używanie unikalnych haseł dla różnych kont utrudnia cyberprzestępcom przejęcie dostępu do wielu usług jednocześnie. Ważne jest również zmienianie haseł, jeśli mamy podejrzenie, że ktoś je poznał.

3

Ostrożnie w publicznych sieciach wi-fi

Publiczne, niezabezpieczone sieci i hotspoty są podatne na ataki. Logowanie się do wrażliwych usług w tych sieciach jest bardzo ryzykowne. Jeśli już musisz korzystać z publicznych sieci wi-fi, koniecznie używaj wirtualnej sieci prywatnej VPN (*Virtual Private Network*), która szyfruje połączenie.

4

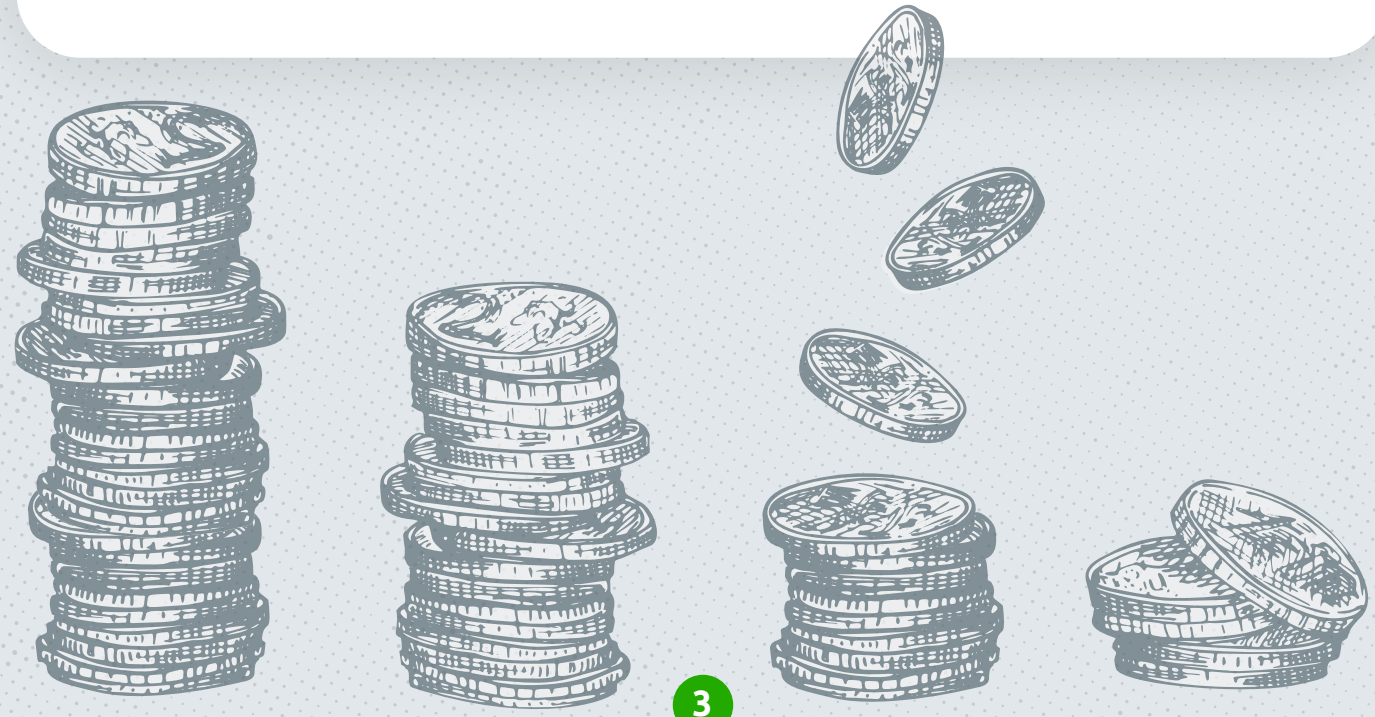
Sprawdzaj autentyczność stron internetowych

Przed wprowadzeniem danych poufnych, takich jak hasła czy informacje finansowe, upewnij się, że strona jest bezpieczna. Sprawdź czy adres strony jest prawidłowy, czy nie różni się choćby najdrobniejszym elementem, czy zaczyna się od https, co oznacza że transmisja jest szyfrowana. Dlaczego to takie ważne? Próba wymuszenia logowania, np. do banku, na fałszywej, podstawionej stronie to często stosowana taktyka we wspomnianych wcześniej publicznych sieciach wi-fi. Jeśli hotspot jest kontrolowany przez hackera, to może on podmieniać strony, bazując na literówkach w nazwach domen. Zamiast „m" w nazwie domeny może pojawić się „rn", a zamiast „www" – „wvvw" czy „wwww". Warto też zwracać uwagę na podejrzane elementy w przypadku jakości grafiki czy poprawności językowej.

5

Zachowaj ostrożność wobec podejrzanych wiadomości

Uważaj na nieznane e-maile i SMS-y, które mogą zawierać linki do fałszywych stron internetowych lub podejrzane załączniki. Nigdy nie klikaj w takie treści ani nie pobieraj plików pochodzących z niewiarygodnych źródeł. Cyberprzestępcy często podszywają się pod zaufane instytucje, dlatego zawsze należy sprawdzić autentyczność nadawcy przed udostępnieniem jakichkolwiek informacji.

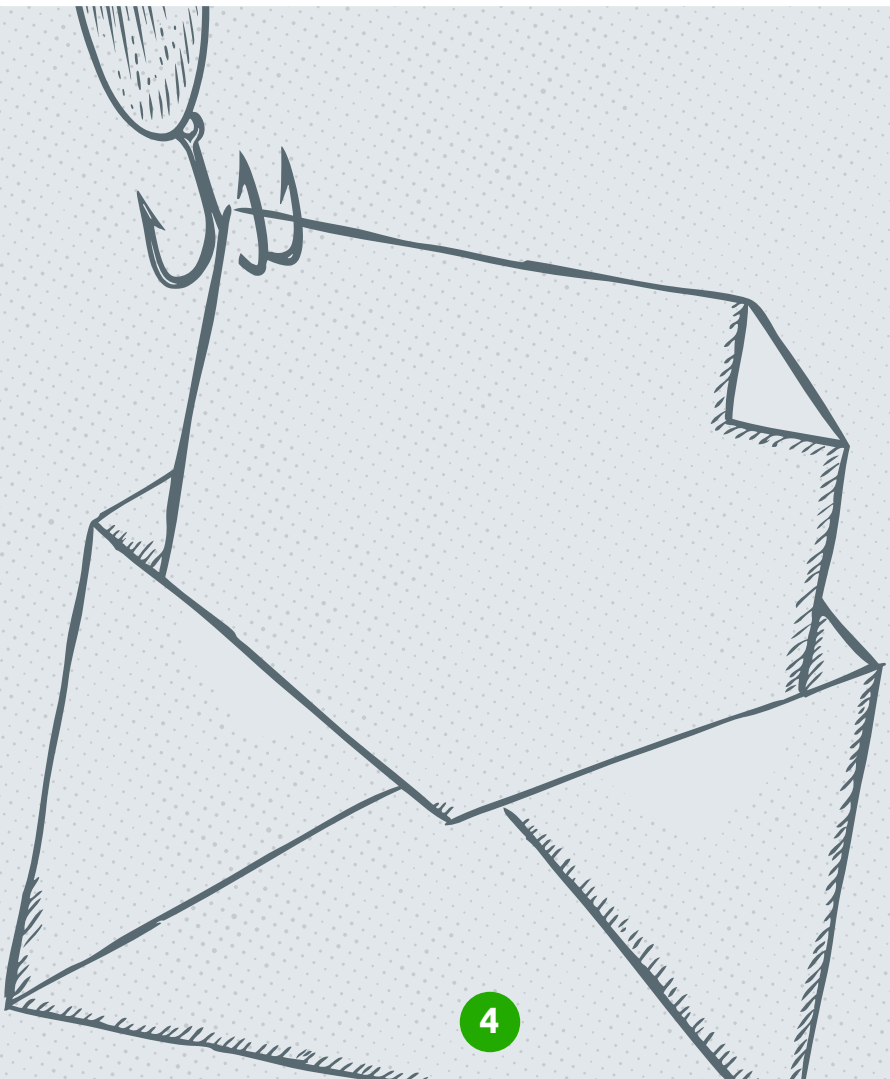


Krajobraz zagrożeń

najpopularniejsze rodzaje ataków

Phishing

To jeden z najczęstszych cyberataków. *Phishing* (skrót od ang. *password harvesting fishing* – łowienie haseł) polega na wysyłaniu m.in. fałszywych wiadomości e-mail lub SMS-ów, które podszywają się pod zaufane instytucje (banki, firmy, urzędy). Celem jest skłonienie ofiary do podania jak największej ilości poufnych informacji, takich jak dane logowania czy dane osobowe. Mają one uwiarygadniać dalsze etapy ataku.
Tradycyjny *phishing* jest obecnie coraz częściej wspierany przez AI (ang. *artificial intelligence* – sztuczna inteligencja), co pozwala na tworzenie o wiele bardziej przekonujących, spersonalizowanych wiadomości. AI może analizować preferencje ofiar i generować phishing, który wydaje się bardziej autentyczny, przez co trudniej go wykryć.

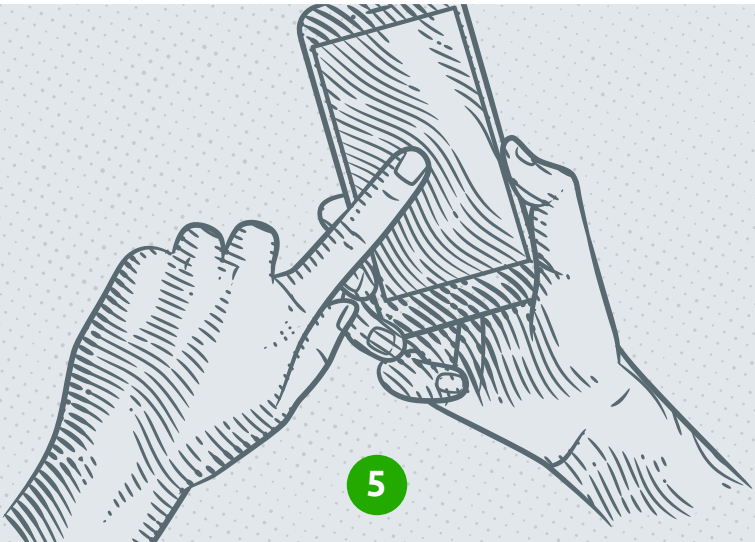


Spear phishing

Spear phishing to rodzaj *phishingu*, który jest bardziej wyrafinowany i spersonalizowany niż tradycyjne ataki. W tym przypadku cyberprzestępcy obierają za cel konkretne osoby lub organizacje i dostosowują swoje wiadomości – tak, aby były bardziej wiarygodne. Zamiast wysyłać masowe, ogólne wiadomości, oszuści zdobywają informacje o ofierze z różnych źródeł, takich jak media społecznościowe, publiczne rejestry czy nawet wcześniejsze interakcje online. AI może analizować dane ofiar zamieszczane w internecie, np. za pomocą social mediów, aby tworzyć wysoce spersonalizowane ataki *spear phishingowe*. Przestępcy, korzystając z tych informacji, mogą łatwiej przekonać ofiary do podania danych logowania, co prowadzi do przejęcia kont. Ponieważ wiadomość zawiera znane Ci szczegóły, wygląda bardziej wiarygodnie i przez to jest trudniejsza do rozpoznania jako oszustwo.

Skąd wiedzieli, że czekam na paczkę?

Cyberprzestępcy często wykorzystują informacje o naszych codziennych działaniach w internecie. Jeśli kupujesz coś online lub regularnie korzystasz z określonych usług, mogą wysłać fałszywego SMS-a lub e-maila w momencie, gdy rzeczywiście czekasz na paczkę lub właśnie zapłaciłeś rachunek. Mogą podszywać się pod kurierów lub dostawców energii, twierdząc, że jest problem z przesyłką lub płatnością. To zwiększa prawdopodobieństwo, że atakowana osoba kliknie w link i poda swoje dane. Te ataki są szczególnie skuteczne, gdy cyberprzestępcy uzyskają dane, które pozwalają im personalizować wiadomości.



Deepfake audio i wideo

Technologia deepfake wzmacnia zagrożenia związane z socjotechniką, ponieważ cyberprzestępcy mogą używać realistycznych, fałszywych nagrań audio i wideo, aby podszywać się pod znane i popularne osoby (np. polityków, celebrytów). Dzięki temu mogą wyłudzać pieniądze lub poufne informacje, oszukując ofiary w bardziej przekonujący sposób niż w klasycznych atakach socjotechnicznych.

Dlaczego znane osoby firmują oszustwa?

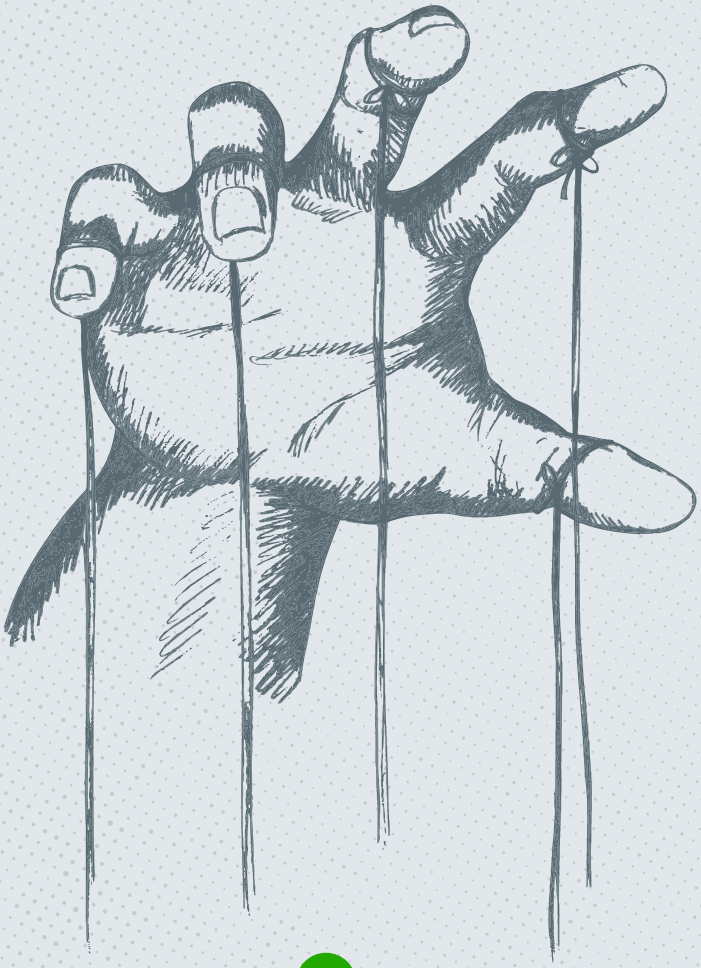
Wizerunki znanych osób są często wykorzystywane przez cyberprzestępców do wzbudzenia zaufania. Takie działania nie polegają już tylko na wysyłaniu wiadomości prywatnych pełnych błędów na Instagramie czy Facebooku. Obecnie piosenkarze, aktorzy czy politycy często padają ofiarą deepfake'ów – technologii umożliwiającej tworzenie fałszywych nagrań wideo i audio. Dzięki deepfake'owi przestępcy mogą stworzyć film, w którym np. powszechnie lubiany celebryta zachwala „zyskowne inwestycje" lub „bezpieczne produkty finansowe". Choć materiał wygląda bardzo wiarygodnie, w rzeczywistości jest to oszustwo.

Socjotechnika (*Social Engineering*)

Cyberprzestępcy są również w stanie skutecznie manipulować ofiarą, aby uzyskać od niej poufne informacje. Często oszuści dzwonią lub piszą jako „przedstawiciele techniczni” lub „pracownicy banku”, przekonując ofiarę do udostępnienia danych lub wykonania określonych czynności, takich jak przelanie pieniędzy.

Czas to pieniądz?

Manipulowanie ofiarami, aby uzyskać od nich poufne informacje, często odbywa się z wykorzystaniem socjotechniki. Jak to działa w praktyce? Oszuści próbują m.in. wywoływać presję czasu, np. strasząc blokadą konta. To sprawia, że ofiary działają impulsywnie, nie sprawdzają autentyczności wiadomości czy nie weryfikują danych osoby, która się z nimi kontaktuje.



Cyberbezpieczeństwo w firmie

Edukacja i świadomość cyberzagrożeń jest kluczowa nie tylko z punktu widzenia indywidualnych użytkowników, ale także całych organizacji. Jakie działania można podjąć, aby zwiększyć świadomość pracowników na temat cyberzagrożeń?

Regularne szkolenia z zakresu cyberbezpieczeństwa

Pracownicy powinni regularnie uczestniczyć w szkoleniach, które przedstawiają aktualne zagrożenia, techniki oszustów i najlepsze praktyki dotyczące bezpieczeństwa w sieci. Ważne jest, aby te szkolenia były interaktywne, obejmowały realistyczne przykłady phishingu, socjotechniki i innych form ataków.

Kampanie informacyjne

Warto organizować kampanie uświadamiające, które w przystępny sposób tłumaczą, jak rozpoznać różne rodzaje cyberzagrożeń. Można to zrobić za pomocą e-maili, plakatów w biurze, artykułów lub dedykowanych webinarów.

Symulacje phishingowe

Jednym z najskuteczniejszych sposobów na zwiększenie świadomości są symulowane ataki phishingowe. Dzięki nim pracownicy mogą na własnej skórze doświadczyć, jak wygląda „prawdziwy” atak. Po takiej symulacji można przeprowadzić analizę – wskazać, gdzie popełniono błędy i podzielić się wskazówkami, jak unikać takich pułapek w przyszłości.

Wdrażanie polityk bezpieczeństwa

Niezwykle ważne jest, aby firma wdrożyła i konsekwentnie egzekwowała polityki bezpieczeństwa IT. Pracownicy powinni być świadomi tych zasad i rozumieć, dlaczego są one ważne. Przykłady takich polityk to m.in. wymóg regularnej zmiany haseł, korzystanie z menedżerów haseł czy stosowanie dwustopniowej weryfikacji.

Przypomnienia i aktualizacje

Świadomość zagrożeń należy stale podtrzymywać. Regularne przypomnienia, newslettery lub alerty o nowych zagrożeniach pomogą utrzymać czujność pracowników. Edukacja na temat cyberbezpieczeństwa powinna być ciągłym procesem, a nie działaniem jednorazowym.

Zachęcanie do zgłaszania podejrzanych incydentów

Pracownicy powinni czuć się swobodnie, gdy zgłaszają podejrzane wiadomości, strony internetowe lub inne incydenty związane z bezpieczeństwem. Warto stworzyć prosty system zgłaszania zagrożeń i nagradzać pracowników za odpowiedzialne działania.

Dariusz Polaczyk, Risk & Security Manager, InternetowyKantor.pl

> Krajobraz zagrożeń w sieci zmienia się dynamicznie, tak jak nasz świat. Dlatego stawiamy na edukację pracowników i staramy się propagować wiedzę w taki sposób, aby była ona nie tylko użyteczna, ale również łatwa do przyswojenia. Przygotowywane przez nas kampanie, prezentacje i ostrzeżenia przestrzegają przed zagrożeniami, zachęcają do weryfikowania informacji w internecie, przypominają o konieczności tworzenia silnych haseł, czy informują o kolejnej kampanii phishingowej. Świadomość potencjalnych pułapek jest bardzo ważna. Tylko w ten sposób możemy zadbać o swoje bezpieczeństwo.

Eksperci ostrzegają

przegląd zagrożeń w 2024 r.

Strategie i metody wykorzystywane przez cyberoszustów zmieniają się bardzo szybko. Jak za nimi nadążyć? Warto śledzić ostrzeżenia publikowane w mediach społecznościowych przez CERT Polska, CSIRT GOV (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Agencję Bezpieczeństwa Wewnętrznego), Komisję Nadzoru Finansowego, policję oraz portale branżowe, takie jak niebezpiecznik.pl czy zaufanatrzeciastrona.pl.

Oto zjawiska i zagrożenia w obszarze cyberbezpieczeństwa, o których w ostatnim czasie informowali eksperci:

Fałszywe zbiórki dla powodzian

np. post o nieistniejącej kobiecie porwanej przez wodę

Spreparowane sensacyjne artykuły

aby zapoznać się z ich treścią, musisz podać swój adres e-mail oraz hasło

Podszywanie się pod firmy kurierskie

fałszywe maile informujące o rzekomych problemach z paczką i prośba o pobranie załączonego dokumentu, w którym znajduje się inny plik ze złośliwym oprogramowaniem

Fałszywe strony bankowości elektronicznej

niebezpieczne domeny, których nazwa do złudzenia przypomina domenę wybranego banku

Wezwania do zapłacenia nieprawdziwego mandatu

podawany w treści wiadomości link przekierowuje do fałszywej strony z formularzem logowania

Posty w social media przekierowujące do fałszywych stron z przecenami

celem jest wyłudzenie danych karty płatniczej

Fałszywe inwestycje

cyberprzestępcy w social mediach podszywają się pod znane firmy, zachęcają do inwestowania pieniędzy i kierują na niebezpieczne strony

Co robić, gdy dojdzie do najgorszego?

Nie zawsze udaje się uniknąć wszystkich zagrożeń. Jeśli doszło do wyłudzenia danych, pieniędzy lub haseł, przede wszystkim zachowaj spokój. Będzie Ci potrzebny do tego, by w pełni świadomie podjąć konieczne, następujące kroki:

zmień hasła do wszystkich kont, szczególnie jeśli używasz tego samego hasła na wielu platformach

zablokuj karty płatnicze i skontaktuj się z bankiem, jeśli podejrzewasz, że ktoś uzyskał dostęp do Twoich danych finansowych

zgłoś incydent odpowiednim instytucjom, takim jak Twój bank, policja czy CERT*

zainstaluj oprogramowanie antywirusowe i przeprowadź pełne skanowanie systemu, aby upewnić się, że nie masz złośliwego oprogramowania na urządzeniu

sprawdź swoje konta online pod kątem nietypowych logowań lub operacji

* CERT Polska to pierwszy w naszym kraju zespół reagowania na incydenty z zakresu bezpieczeństwa komputerowego, który powstał w 1996 r. Zespół CERT Polska działa w strukturach instytutu badawczego NASK (Naukowej i Akademickiej Sieci Komputerowej). Incydenty z dziedziny cyberbezpieczeństwa – np. domeny internetowe służące do wyłudzeń danych i środków finansowych – można zgłaszać na stronie cert.pl, wybierając przycisk „Zgłoś incydent". Wszystkie podejrzane wiadomości SMS z linkami można z kolei zgłosić używając funkcji „Przekaż", bezpośrednio na numer: 8080.


InternetowyKantor.pl