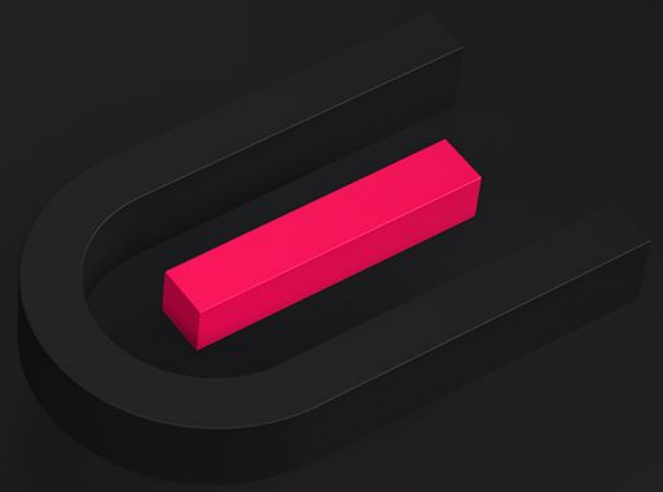


Bezpieczeństwo w sieci.
Oszustwa z wykorzystaniem telefonu

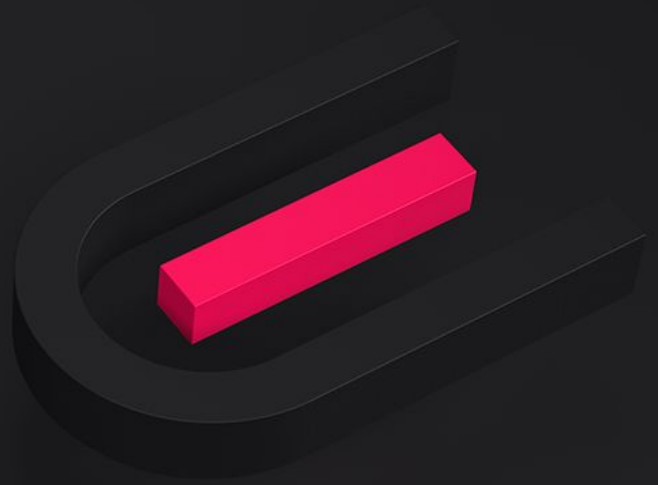
Najpopularniejsze oszustwa i jak się przed nimi bronić.

Robert Wach - r.wach@core.com.pl - 668 072 232

Avast AVG CORE

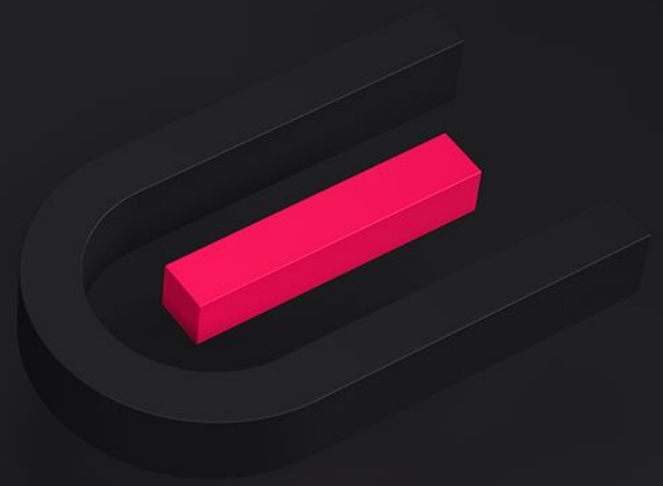
Smishing

Czym jest, jak działa i jak się przed nim chronić?



Avast AVG CORE

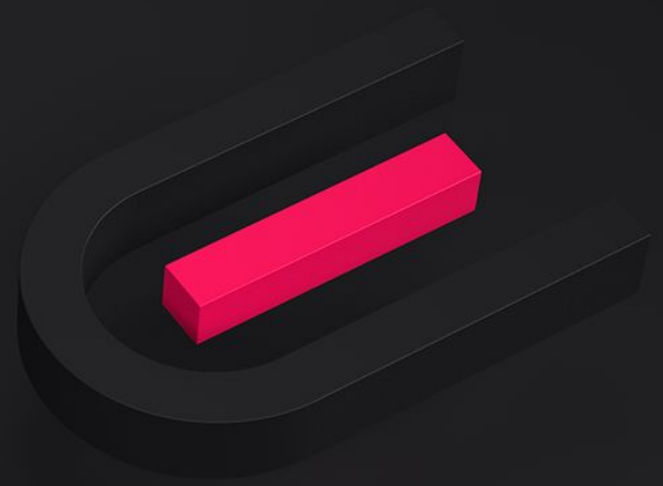
Smishing
Czym jest smishing?



Cyberprzestępcy coraz śmielej w swoich działaniach wykorzystują smishing. Czym jest ten atak? To rodzaj phishingu rozprzestrzenianego za pomocą wiadomości SMS, skąd wzięła się zresztą jego nazwa (SMS + phishing = SMiShing).

Oszuści próbują w ten sposób wyłudzić od swoich ofiar wrażliwe dane. Mogą to być numery karty płatniczej, dowodu osobistego czy dane logowania do bankowości internetowej.

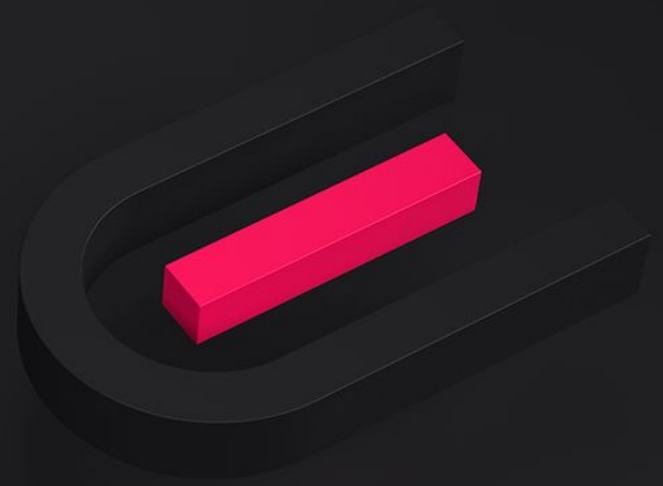
Smishing
Czym jest smishing?



Dlaczego wykorzystują w tym celu wiadomości SMS, choć wydawałoby się, że takie ataki są łatwiejsze do przeprowadzenia za pomocą wiadomości e-mail?

W Polsce numer telefonu komórkowego składa się z zaledwie 9 cyfr. Wygenerowanie tysięcy losowych numerów i wysłanie na nie wiadomości nie jest zatem zbyt trudne – oszust nie musi nawet pozyskiwać bazy kontaktów.

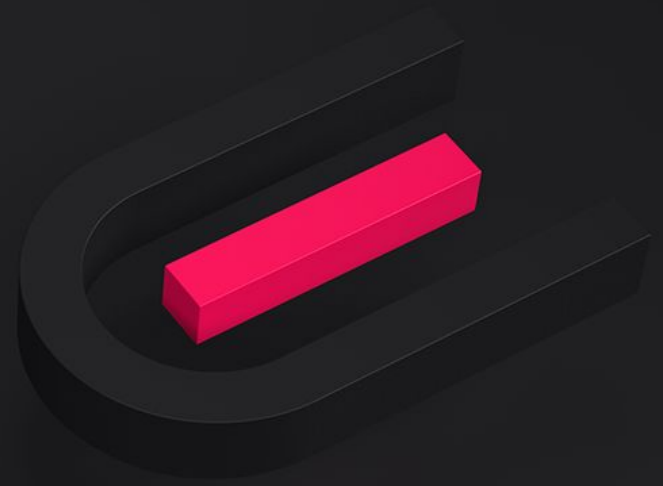
Smishing
Czym jest smishing?



SMS-y mają w phishingu kilka przewag nad e-mailami. Przede wszystkim cieszą się znacznie większym zaufaniem wśród użytkowników i obecnie nie są jeszcze zbyt mocno kojarzone z oszustwami. Co za tym idzie – odbiorca chętniej uwierzy w treść SMS-a niż wiadomości otrzymanej na skrzynkę e-mail.

Znacznie większy jest też współczynnik otwierania takich wiadomości. Zazwyczaj przekracza on 90%. Oszust może być zatem niemal pewny, że jego SMS zostanie przeczytany przez ofiarę.

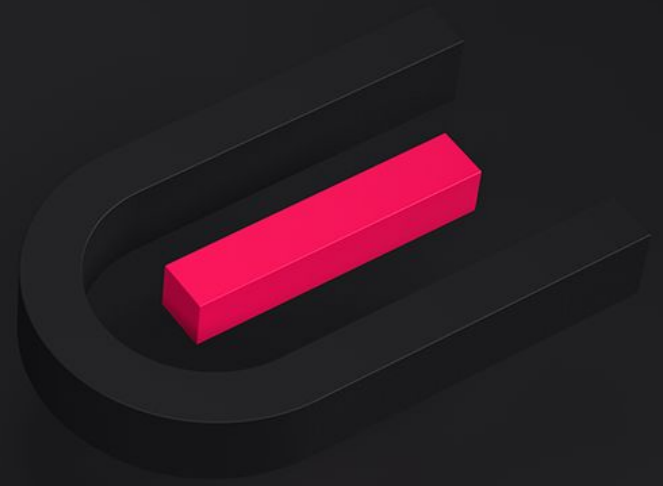
Smishing
Jak działa smishing?



Cyberprzestępcy chcą poprzez smishing wyłudzić wrażliwe dane. W tym celu zaszywają w wiadomości np. link rzekomo prowadzący do strony internetowej banku. W rzeczywistości jest to podstawiona witryna – wpisanie tam swoich danych logowania sprawi, że przekażemy je oszustom i zyskają dostęp do naszego konta bankowego.

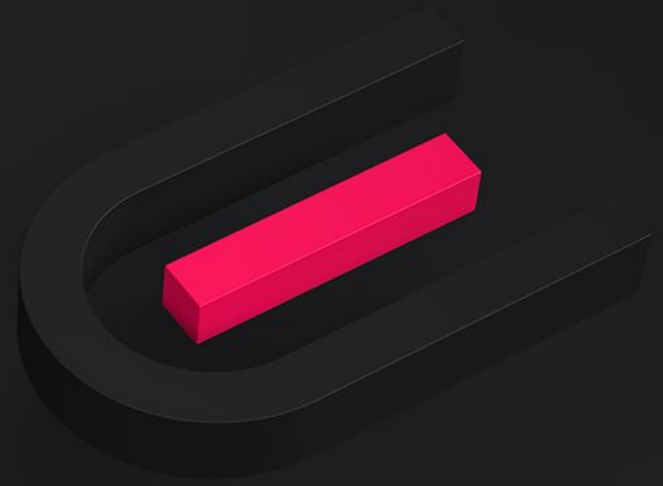
Smishing często dotyczy wyłudzenia numerów kart płatniczych, danych logowania do bankowości internetowej czy dokumentów tożsamości. Cyberprzestępcy mogą też po prostu wyłudzać pieniądze, podsyłając link do płatności w celu rzekomego uregulowania zaległych należności. Pod fałszywym odnośnikiem może się też kryć złośliwe oprogramowanie, które zainfekuje nasze urządzenie.

Smishing
Przykłady smishingu



Praktycznie każdy posiadacz telefonu komórkowego zetknął się ze smishingiem. Cyberprzestępcy zazwyczaj dopasowują się do obecnych wydarzeń czy pory roku. Podczas pandemii rozsyłali fałszywe informacje o możliwości zapisania się na szczepienie. Osoba, która kliknęła link i wprowadziła na podstawionej stronie swoje dane, przekazała je oszustom.

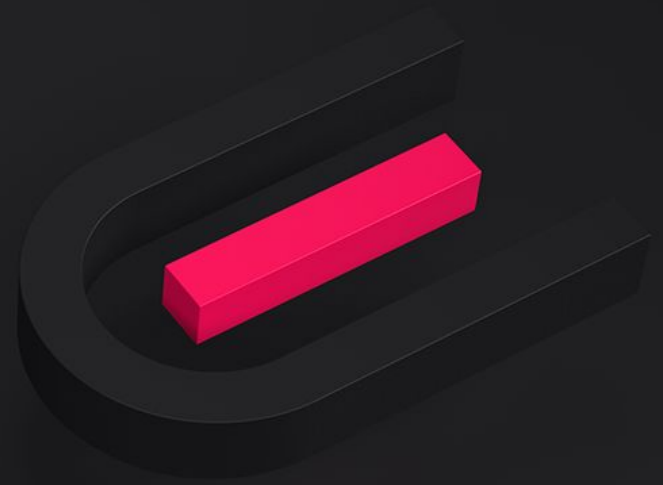
Smishing
Przykłady smishingu



Popularne są też wiadomości z prośbą o dopłatę do paczki, by kurier mógł ją dostarczyć. Tego typu ataki pojawiają się szczególnie w okresie przedświątecznym, gdy zamawiamy dużo przesyłek.

Smishing może również dotyczyć rzekomego nieuregulowanego rachunku za prąd czy gaz, blokady konta bankowego, a nawet fałszywej informacji o konieczności rozliczenia PIT.

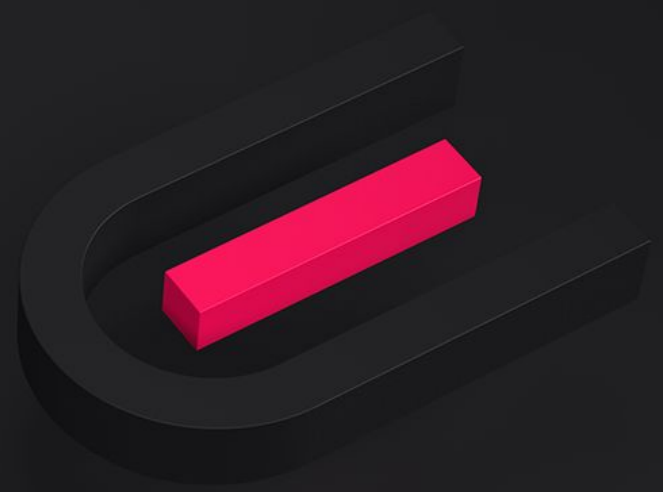
Smishing
Jak chronić się przed smishingiem?



- Nie klikaj w odnośniki znajdujące się w wiadomości SMS. Jeśli ktoś prosi Cię o zalogowanie do banku, sam wpisz witrynę w przeglądarce.
- Nie reaguj na prośby o drobną dopłatę za usługę. Jeśli nie jesteś pewny, czy rzeczywiście z czymś nie zalegasz, skontaktuj się bezpośrednio z usługodawcą, np. firmą energetyczną.
- Korzystaj z uwierzytelniania dwuskładnikowego wszędzie, gdzie to możliwe. Nawet jeśli Twoje dane gdzieś wycieką, oszust nie wykorzysta ich bez dodatkowego potwierdzenia logowania z Twojej strony.
- Nie odpowiadaj na otrzymane wiadomości smishingowe.
- Korzystaj z oprogramowania antywirusowego na telefonie, takiego jak Avast Mobile Security. Może ono automatycznie blokować wiadomości z próbą oszustwa. Niektóre smartfony mają tę funkcję wbudowaną w system.

Spoofing telefoniczny

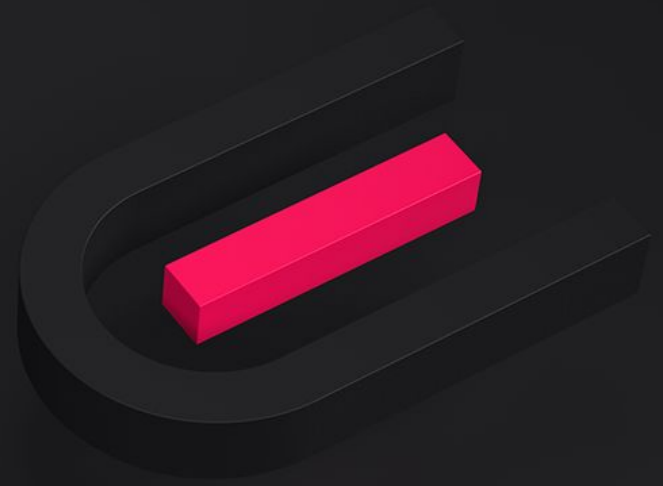
Czym jest i jak się przed nim bronić?



Avast AVG CORE

Spoofing telefoniczny

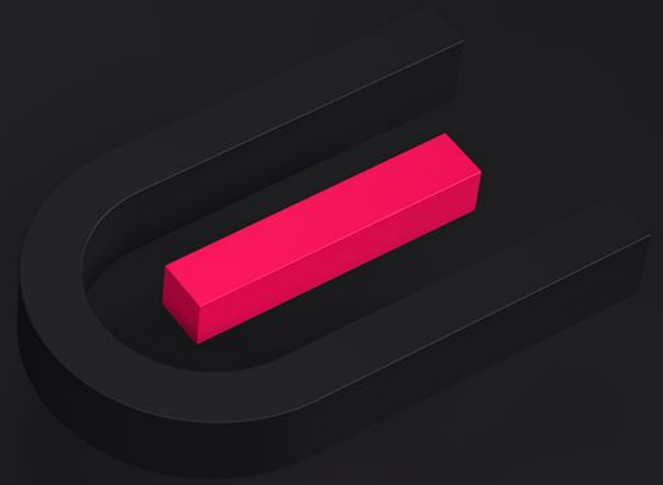
Czym jest spoofing?



Cyberprzestępcy dysponują obecnie narzędziami, które pozwalają im podszyć się pod wybrany numer telefonu. Dzięki temu ofiara będzie widziała na wyświetlaczu, że dzwoni do niej np. bank, a w rzeczywistości będzie to oszust. Jak to możliwe? Najczęściej wykorzystuje się w tym celu telefonię VoIP, gdzie można zdefiniować numer, jaki ma się wyświetlać na ekranie. Podszycie się pod konkretny numer jest obecnie banalnie proste i poradzi sobie z tym nawet amator.

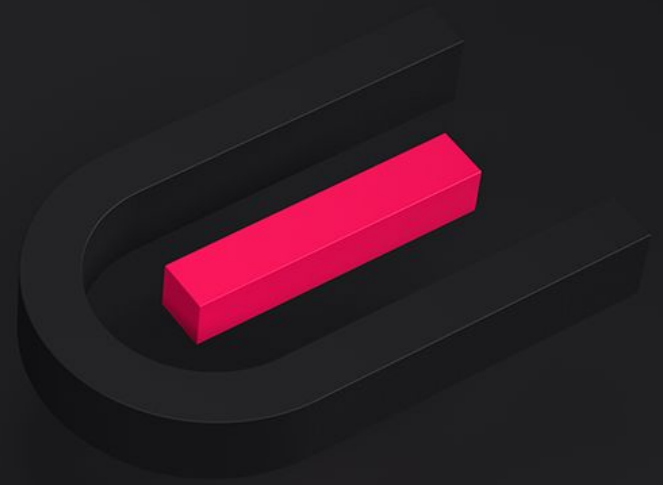
Spoofing telefoniczny

Czym jest spoofing?



Celem takiego działania jest najczęściej wyłudzenie wrażliwych danych. Oszuści mogą podszywać się pod przedstawicieli banków, by zdobyć np. imię i nazwisko, adres oraz numer PESEL. Dane te mogą posłużyć do kradzieży tożsamości, wyrobienia fałszywego dowodu czy nawet zaciągnięcia pożyczki.

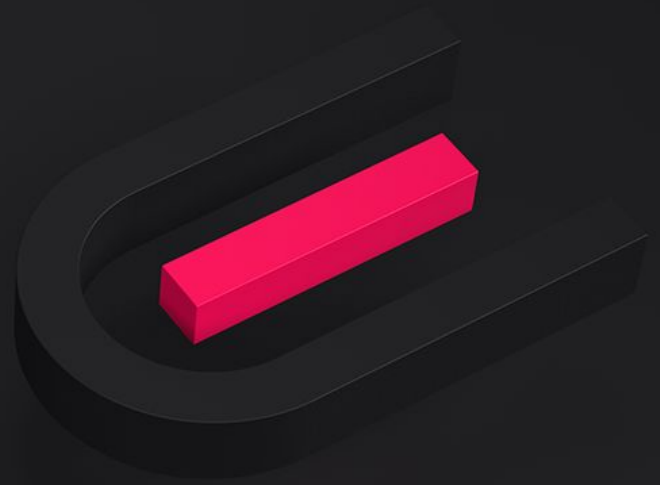
Spoofing telefoniczny
Jak się bronić przed spoofingiem?



- Przemyśl, gdzie podajesz swój numer telefonu. Jeśli jest on łatwo dostępny w internecie, to prędzej czy później zainteresuje się nim oszust.
- Bądź podejrzliwy podczas rozmów telefonicznych, nawet jeśli rozmówca podaje się np. za pracownika banku.
- Jeśli nie jesteś pewny, czy rozmawiasz z pracownikiem wybranej instytucji, rozłącz się, a następnie samodzielnie zadzwoń na infolinię.
- Nie zdradzaj nikomu przez telefon swoich danych logowania do banku czy innych serwisów.
- Jeśli podczas rozmowy zostaniesz poproszony o zainstalowanie dodatkowego oprogramowania lub kliknięcia odnośnika przesłanego SMS-em, nie rób tego.
- Jeśli obawiasz się, że nieumyślnie podałeś komuś przez telefon swoje dane, skontaktuj się z bankiem i zastrzeż swoje konto.

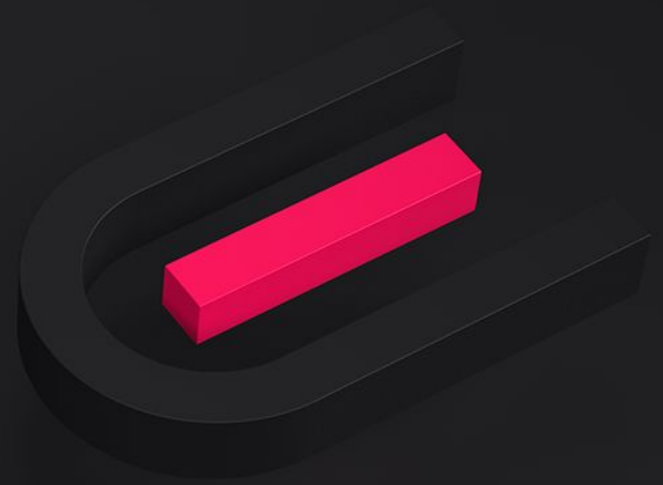
Wyrobienie duplikatu SIM

Na czym polega i jak się chronić?



Avast AVG CORE

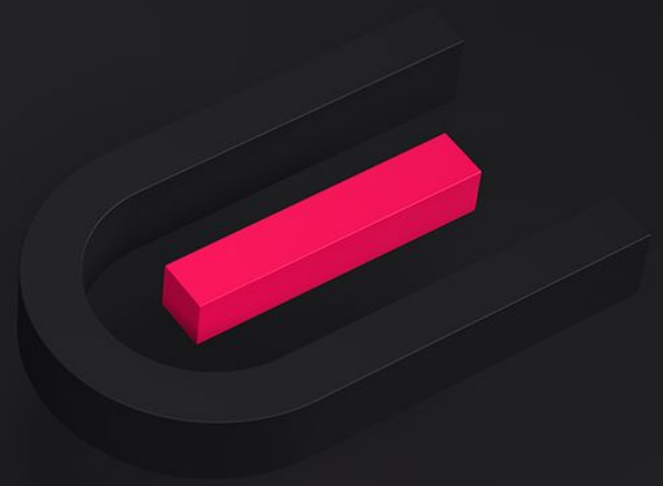
Wyrobienie duplikatu SIM
Na czym polega?



Popularnym zjawiskiem jest też wyrabianie przez oszustów duplikatu karty SIM do telefonu w celu autoryzacji przelewów w banku ofiary. W 2018 roku szajka złodziei działająca według tego schematu wyłudziła w Polsce przynajmniej kilkaset tysięcy złotych.

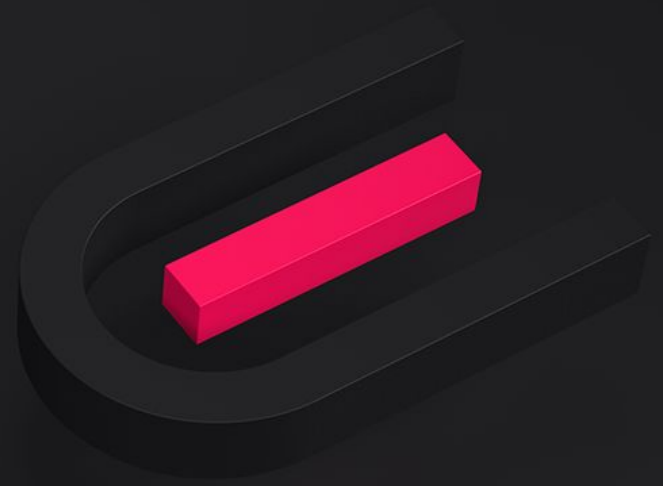
Na czym dokładnie polega ten przekręt? Oszust udaje się do salonu operatora telekomunikacyjnego i wyrabia duplikat karty SIM swojej ofiary, identyfikując się np. podrobionym dokumentem tożsamości.

Wyrobienie duplikatu SIM
Na czym polega?



Następnie loguje się na konto bankowe ofiary i zleca przelew na dużą kwotę – zazwyczaj dotyczy to wszystkich zgromadzonych środków. Operację autoryzuje kodem SMS, który otrzymał na wyrobiony duplikat karty. W tym czasie ofiara pozostaje nieświadoma, bowiem jej karta SIM przestała działać.

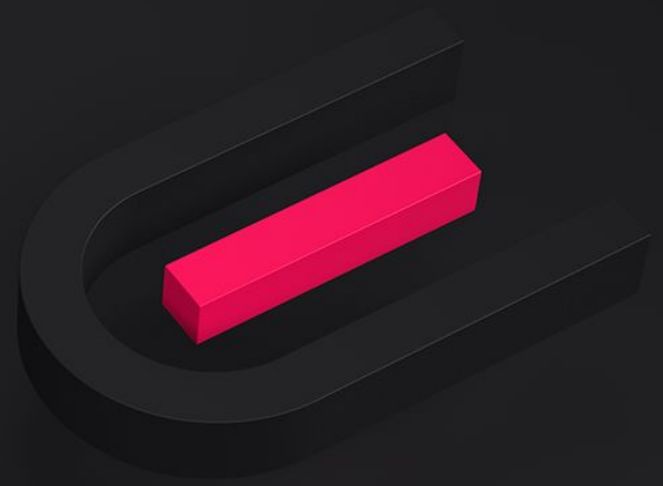
Wyrobienie duplikatu SIM
Na czym polega?



Aby przeprowadzić całą operację, ofiara już wcześniej musiała być na celowniku oszustów. W jakiś sposób pozyskali oni dane logowania do bankowości online, a także dane służące do wyrobienia fałszywego dokumentu tożsamości.

Jest to więc atak wieloetapowy, który może się zacząć od phishingu czy też smishingu. Oszustwo wycelowane jest jednak w konkretną osobę.

Wyrobienie duplikatu SIM
Jak się przed tym uchronić?

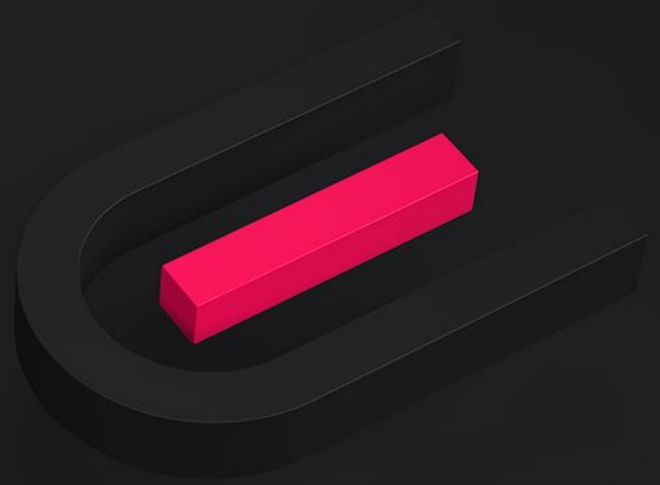


Nie ma jednoznacznego sposobu na ochronę przed tym oszustwem. Wszystko zależy w głównej mierze od tego, czy cyberprzestępcom uda się wyrobić duplikat karty SIM u operatora i pozyskać dane logowania do banku. Co można jednak zrobić?

- Monitoruj kartę SIM. Jeśli nagle przestanie działać, może to oznaczać, że ktoś wyrobił jej duplikat. W takim przypadku zweryfikuj operację u operatora i poinformuj bank o możliwej aktywności na Twoim koncie.
- Jeśli obawiasz się tego ataku, używaj innego numeru telefonu do obsługi konta bankowego – najlepiej takiego, który nie jest udostępniony w internetowych bazach, np. w KRS.

Połączenia z zagranicznych numerów

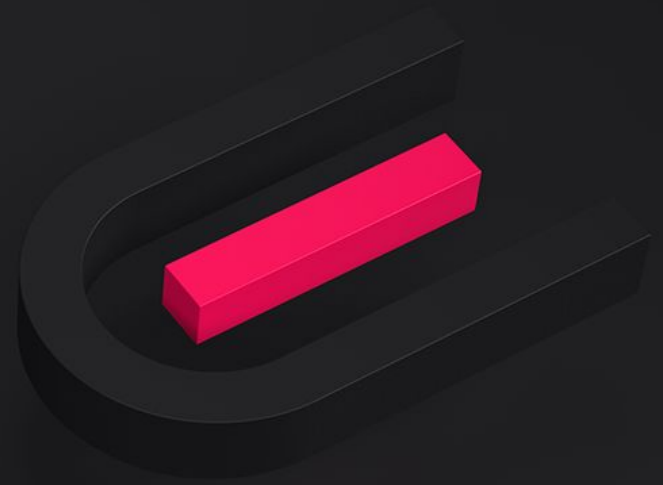
Na czym polegają i jak się chronić?



Avast AVG CORE

Połączenia z zagranicznych numerów telefonów

Na czym polegają?

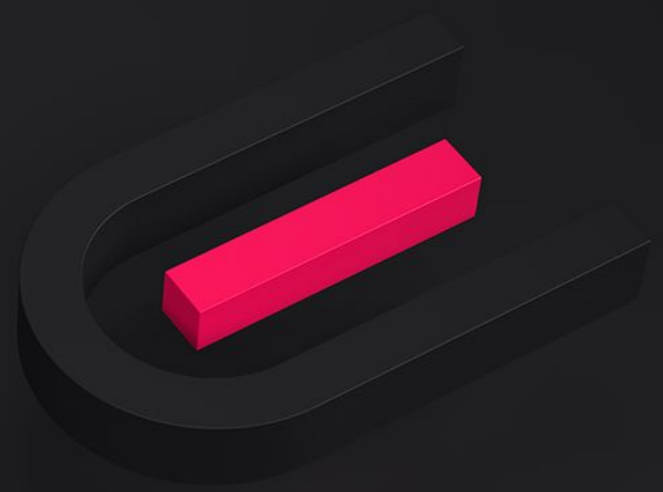


Naciąganie na zagraniczny numer telefonu to jedno ze starszych, ale wciąż aktualnych oszustw. Polega ono na wykonaniu krótkiego połączenia na numer ofiary. Na tyle krótkiego, by nie zdążyć go odebrać.

Oszuści liczą na to, że ofiara oddzwoni na zagraniczny numer, nacinając się tym samym na wysoki koszt połączenia, który może wynosić nawet kilkadziesiąt złotych za minutę. Część tych pieniędzy operator przekazuje właścicielowi numeru i w ten sposób oszust zarabia na swojej działalności.

Połączenia z zagranicznych numerów telefonów

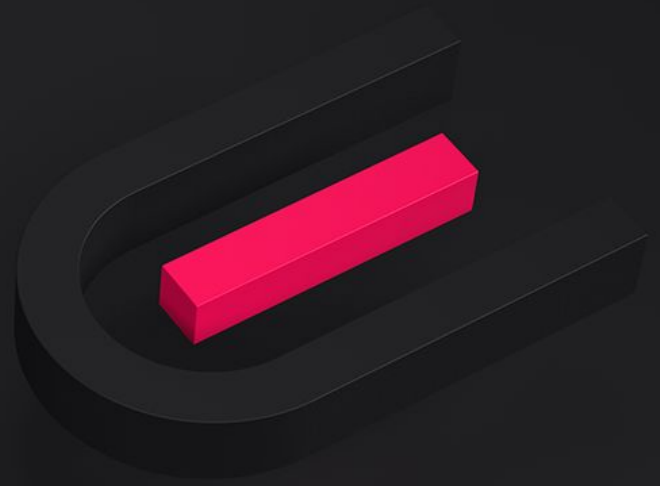
Jak się bronić przed tym bronić?



- Najprostsza i najskuteczniejsza rada – jeśli nie znasz numeru, nie oddzwaniaj. Jeśli ktoś ma do Ciebie ważną sprawę, zadzwoni ponownie.
- Weryfikuj numer kierunkowy. W przypadku Polski jest to +48. Jeśli początek numeru jest inny, to numer pochodzi zza granicy. Niektóre telefony automatycznie rozpoznają państwo pochodzenia numeru i wyświetlają na ekranie.

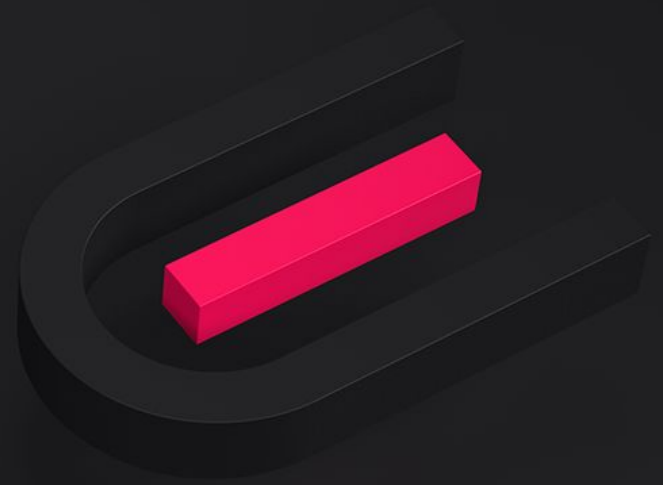
Stalkerware – szpieg w telefonie

Jakie informacje zbiera i jak się chronić?



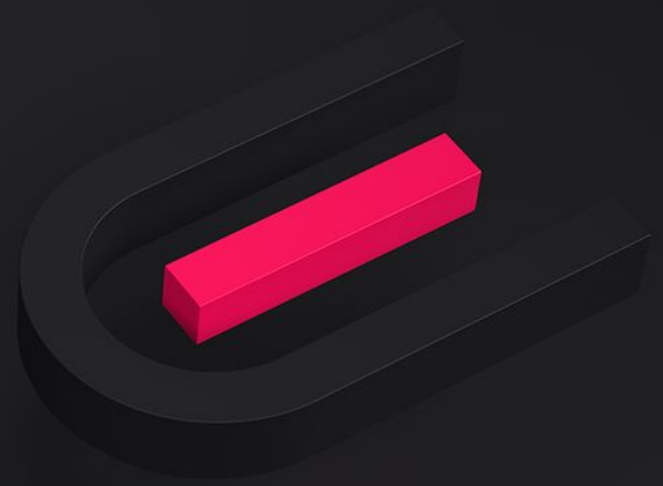
Avast AVG CORE

Stalkerware – szpieg w telefonie
Czym jest?



Aplikacje stalkerware to oprogramowanie, które pozwala śledzić każdy ruch użytkownika na jego telefonie. Programy tego typu zazwyczaj są reklamowane jako narzędzia do kontroli rodzicielskiej, a niektóre z nich są w pełni legalne, choć korzystanie z nich bez informowania o tym kontrolowanej osoby uważane jest za nieetyczne.

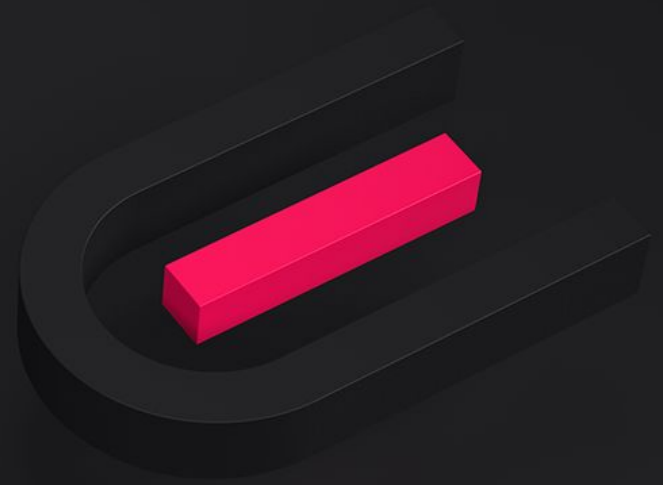
Stalkerware – szpieg w telefonie
Czym jest?



Aby je zainstalować, wystarczy jednorazowy dostęp fizyczny do smartfona. Instalacji może więc dokonać nieufny partner lub np. rodzic, nie informując o tym właściciela telefonu.

Stalkerware może być również instalowane w wyniku infekcji złośliwym oprogramowaniem. Wtedy dostęp do naszych danych zyskuje osoba z zewnątrz, co może być jeszcze groźniejsze w skutkach.

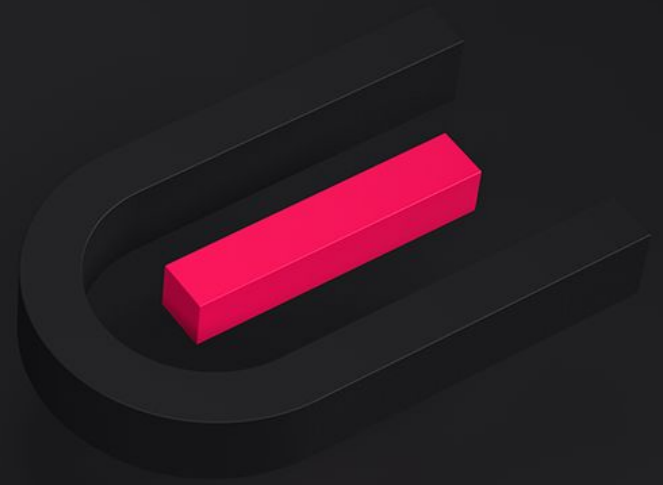
Stalkerware – szpieg w telefonie
Jakie informacje zbiera?



Osoba szpiegująca, która korzysta ze stalkerware, może:

- widzieć aktualną lokalizację ofiary,
- mieć wgląd w wiadomości i komunikatory,
- przeglądać zdjęcia i filmy zrobione telefonem,
- mieć dostęp do plików na urządzeniu,
- widzieć, co ofiara wpisuje za pomocą klawiatury,
- podsłuchiwać rozmowy telefoniczne.

Stalkerware – szpieg w telefonie
Jak się chronić?

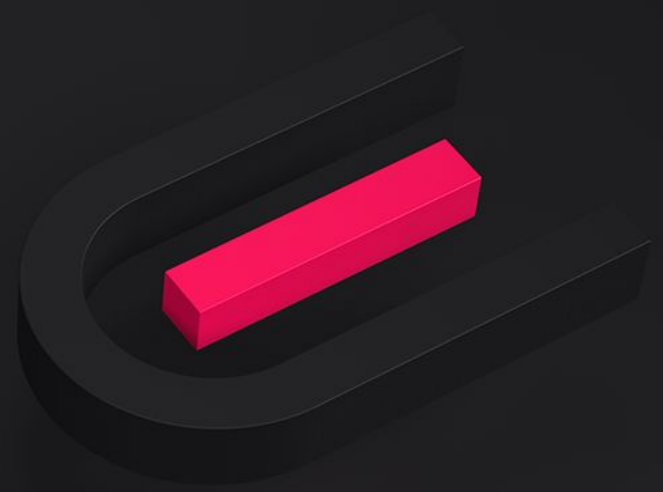


- Zabezpiecz fizyczny dostęp do swojego telefonu. Stosuj blokadę ekranu, autoryzację biometryczną za pomocą twarzy lub odcisku palca i nie zostawiaj urządzenia bez opieki.
- Zainstaluj oprogramowanie antywirusowe. Dobra aplikacja, taka jak np. Avast Mobile Security, potrafi wykryć większość stalkerware i poinformować o jej obecności. Część programów tego typu oznaczana jest jako potencjalnie niechciane oprogramowanie.
- Monitoruj zużycie baterii i transfer danych. Stalkerware wydatnie wpływa na zużycie baterii i danych. Sprawdzaj, czy nieznane Ci aplikacje nie zużywają zbyt dużo energii lub pakietu danych i im przeciwdziałaj.
- Sprawdź uprawnienia aplikacji. Jeśli nieznany Ci program ma dostęp np. do geolokalizacji, telefonu czy odczytywania wiadomości, może to być stalkerware.

Avast AVG CORE

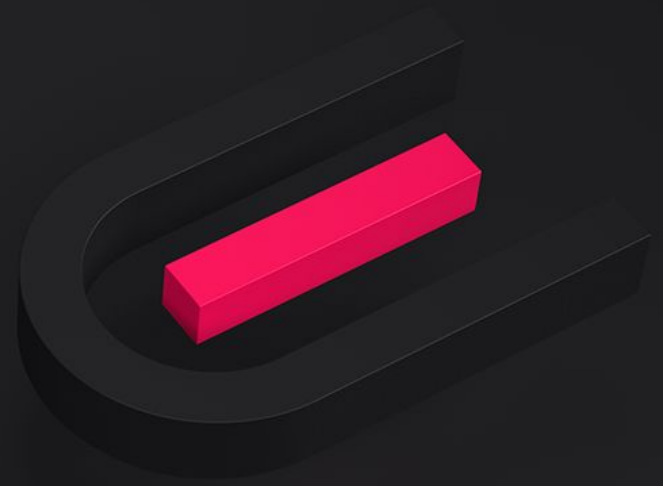
Oszustwa przez WhatsApp

Na portalach aukcyjnych i przez Booking.com



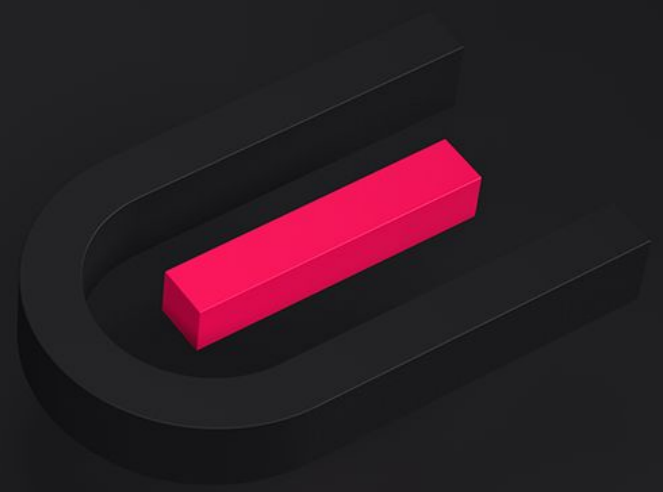
Avast AVG CORE

Oszustwa przez WhatsApp
Na portalach aukcyjnych



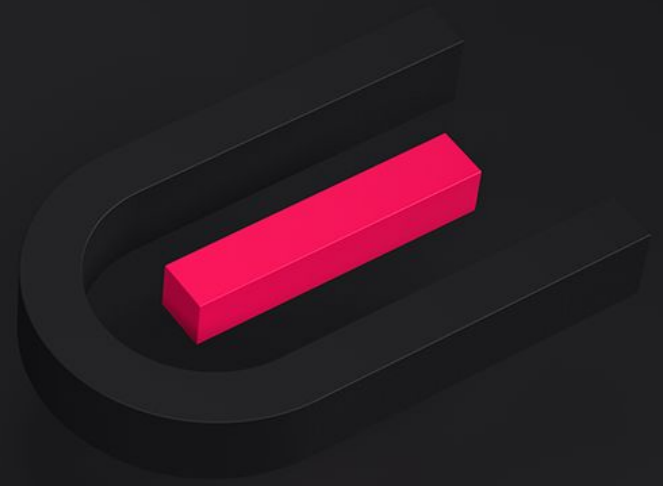
Ofiarą może być osoba, która chce coś sprzedać. Rzekomo zainteresowany kupujący kontaktuje się ze sprzedawcą przez WhatsApp i informuje, że opłacił już zamówienie. Przesyła też fałszywy link do strony, która łudząco przypomina witrynę popularnego przewoźnika (np. DPD, inPost) i informuje, że sprzedawca może tam odebrać swoje pieniądze za przedmiot, podając numer karty lub dane logowania do banku. W ten sposób nieświadomy sprzedający udostępnia wrażliwe dane oszustowi lub wręcz wpłaca pieniądze na jego konto.

Oszustwa przez WhatsApp
Na portalach aukcyjnych



Oszustwa te mogą przybierać różne warianty, ale mają wspólny mianownik – chęć rozliczenia płatności/przesyłki poza serwisem aukcyjnym. Aby się przed tym ochronić, należy korespondować z potencjalnymi kupcami tylko za pośrednictwem portalu aukcyjnego.

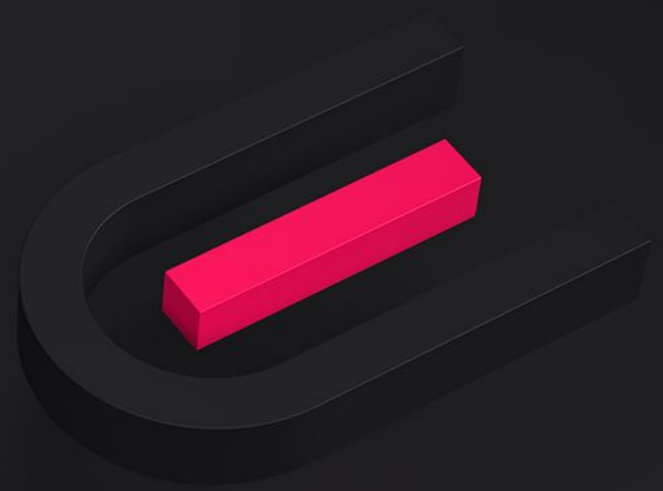
Oszustwa przez WhatsApp
Przez Booking.com



Oszuści kontaktują się na WhatsAppie z osobą, która złożyła rezerwację noclegu przez Booking.com. Informują, że pojawił się problem z płatnością kartą i należy ją w tym momencie autoryzować. Jeśli przekażemy dane karty przez komunikator, narazimy się na utratę pieniędzy.

Należy pamiętać, by z hotelem korespondować wyłącznie oficjalnymi kanałami, czyli bezpośrednio przez Booking.com lub inny portal służący do rezerwacji noclegów.

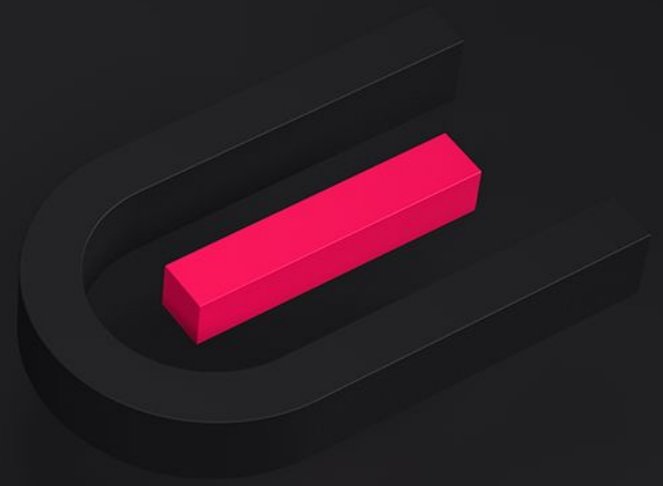
Podsumowanie



Przede wszystkim ostrożność

Avast AVG CORE

Kontakt



Robert Wach - r.wach@core.com.pl - 668 072 232

Kod rabatowy na rozwiązania Avast Ultimate Mutlidevice:
https://avtrade.pl/avast-ultimate
kod - ngo2022 - 65% zniżki

Avast AVG CORE