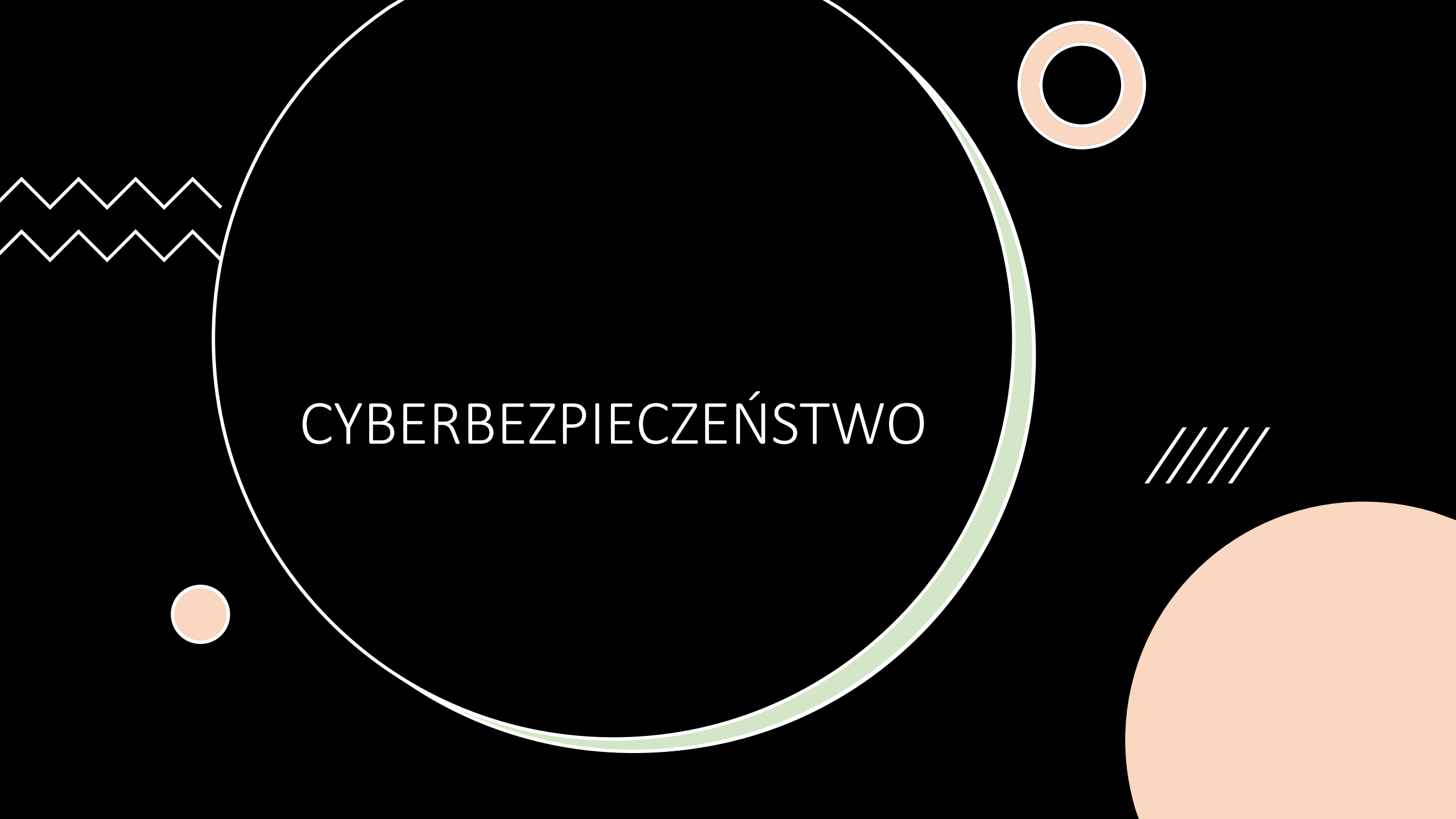


The image features a dark background with various geometric elements. A large, thin white circle is centered, with a thick light green arc on its right side. To the left of the circle are two white zigzag lines. In the top right corner is a small orange circle with a white outline. In the bottom left corner is a small solid orange circle. In the bottom right corner is a large solid orange circle. To the right of the main circle are four parallel white diagonal lines. The text 'CYBERBEZPIECZEŃSTWO' is centered within the white circle.

CYBERBEZPIECZEŃSTWO



BEZPIECZEŃSTWO

Bezpieczeństwo jest to stan systemu informatycznego, w którym poziom ryzyka jego aplikacji jest zredukowany do akceptowalnego poziomu, poprzez zastosowanie odpowiednich środków.



CYBERTERRORYZM

Ośmieszenie

Zdobycie informacji zastrzeżonych

Wyłączenie systemów
informacyjnych

Fizyczne uszkodzenie

RODZAJE ATAKÓW

Phishing

Man in the
middle; sniffin i
spoofing

Socjotechnika

Deface

Smishing

Wirusy i
pokrewne

Błąd
oprogramowania

PHISHING

odnosi się do procesu zbierania (kradzieży) danych przez przestępców.

PHISHING



W typowym ataku phishingowym cyberprzestępca tworzy **prawie idealną replikę strony WWW** dowolnej instytucji lub portalu.



Następnie przy użyciu **technik spamowych** wysyłane są wiadomości e- mail imitujące prawdziwą korespondencję wysyłaną przez różne instytucje.



Wszystkie takie wiadomości mają jeden cel: **nakłonienie odbiorców do kliknięcia zawartego w liście odsyłacza.**



Stworzone przez phisherów odsyłacze kierują użytkowników bezpośrednio do fałszywej strony WWW, na której "schwyta ryba" wprowadza poufne informacje



Aby odblokować Twoje konto w Allegro wyślij SMS o treści SKT na nr 73070 z numeru telefonu przypisanego do Twojego konta.

Lub zeskanuj kod:



Ponieważ wykryto włamanie, powyższy krok jest niezbędny do zweryfikowania czy jesteś właścicielem konta.
(Koszt wysłania wiadomości SMS wg. stawki operatora (0,55PLN))
Po wysłaniu wiadomości wpisz kod do formularza i kliknij "Odblokuj Konto" aby odblokować Twoje konto allegro.

Podaj Kod SMS:

Kod SMS:

Odblokuj konto

Drogi Użytkowniku

Ta wiadomość została do Ciebie automatycznie, przez system rozpoznawania niebezpieczeństw platformy allegro.

Dnia 29-04-2015 wykryto nieautoryzowany dostęp do Twojego konta w portalu. W związku z wykrytym niebezpieczeństwem Twoje konto zostało tymczasowo zawieszone.

Aby odblokować swoje konto przejdź pod adres : <http://odblokuj.allegro.pl?6846713>

*Grupa Allegro Sp. z o.o.
ul. Grunwaldzka 182
60-166 Poznań*

Firma wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy Poznań - Nowe Miasto i Wilda w Poznaniu,
Wydział VIII Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000268796, NIP 527-25-25-995, REGON [140762508](#),
Kapitał zakładowy 33 976 500,00 PLN

Kurier nie dostarczył przesyłkę do numeru zgłoszenia **RR6536886973PL** na adres **05.07.2015**, ponieważ nikt w tym czasie. Proszę [zobaczyć informacje](#) na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

[Zobacz informacje](#)

Uwaga

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.

To jest generowany automatycznie e-mail, kliknij jeżeli chcesz się [wypisać](#)

Phishing z wykorzystaniem mediów społecznościowych to rodzaj ataku przeprowadzany za pośrednictwem takich platform, jak Instagram, LinkedIn, Facebook lub Twitter. Celem takiego ataku jest kradzież danych osobowych lub przejęcie kontroli nad kontem w mediach społecznościowych.

PHISHING METODY OCHRONY



FORMA – niechlujna



TREŚĆ – alarmująca, nakazowa, ofertowa

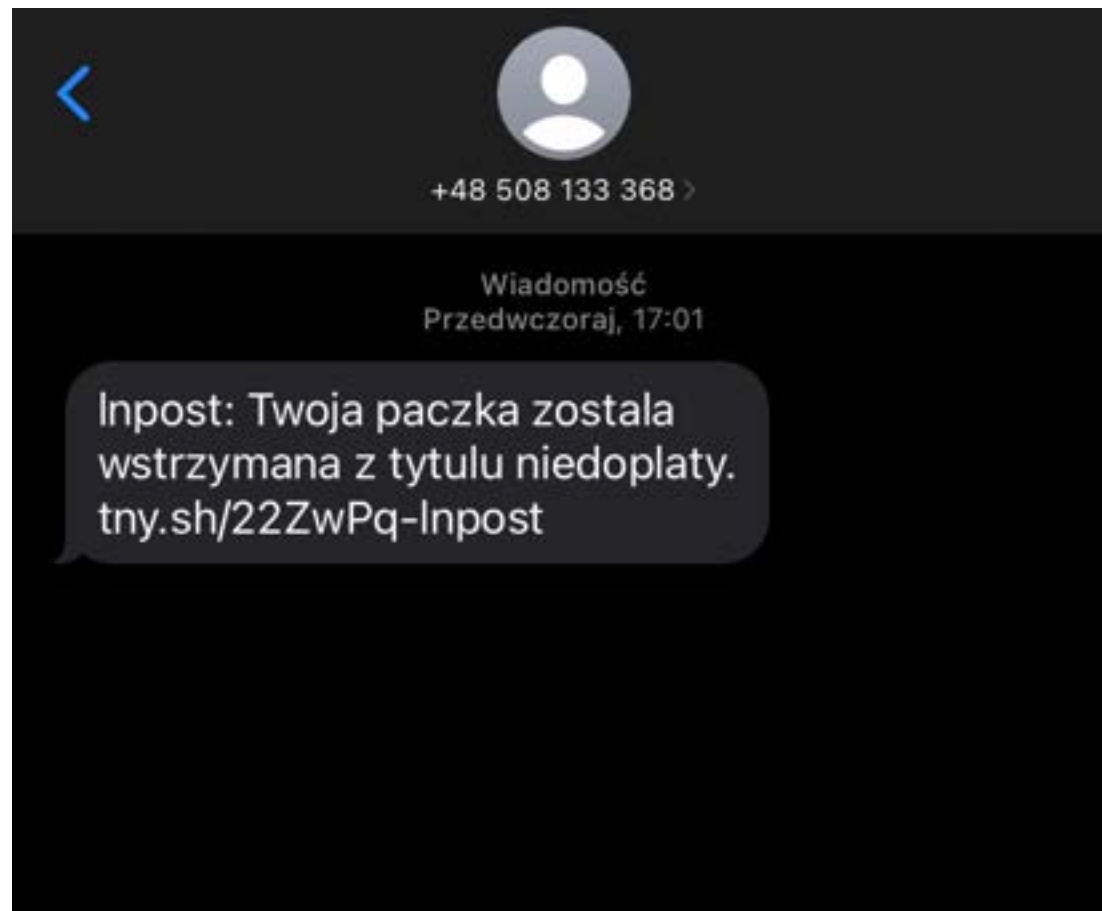


NADAWCA – nieznany, podszywający się



ODNOŚNIKI - inna nazwa, inne miejsce docelowe

Smishing = atak przez SMS



17:33



Aktywny(a) teraz



Jesteście znajomymi na Facebooku
Mieszka w: Tymowa, Tarnow, Poland
Pracuje w: Straż Pożarna

16:41

Hej Katarzyna jak masz chwile
możesz odebrać sobie bon na
zakupy do Rosmann na stronie
prezent-rossman.24.eu To
nowa akcja świąteczna sklepu i
można wygrać 2000zł, ale
zostało już tylko kilka sztuk do
zgarnięcia, powodzenia!



Aktywny(a) teraz



Jesteście znajomymi na Facebooku
Mieszka w: Kraków

22:19

mam pytanie może ty znasz
tego chłopaka na zdjęciu ,
wypisuje do mnie i twierdzi że
zna ciebie ? znasz go

[http://facebook-
profile65241445996.5v.pl](http://facebook-profile65241445996.5v.pl)

Naciśnij i przytrzymaj 😊 , aby zareagować

18:33



Jesteście znajomymi na Facebooku
Mieszka w: Bochnia
adwokat w: Kancelaria Adwokacka

06.12, 18:42

Hej Katarzyna! Przeczytaj
zanim usuną [przechwycone-
zdjecia.eu](http://przechwycone-zdjecia.eu)

06.12, 19:07

Wirus uwaga nie klikać



SOCJOTECHNIKA

Zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę.

Hackerzy często wykorzystują niewiedzę bądź łatwowierność użytkowników systemów informatycznych, aby pokonać zabezpieczenia odporne na wszelkie formy ataku.

Wyszukują przy tym najslabszy punkt systemu bezpieczeństwa, którym najczęściej jest człowiek.

METODY ATAKU SOCJOTECHNICZNEGO



Z pozoru nieszkodliwa informacja

Czasem wystarczy po prostu poprosić

Budowanie zaufania

Może pomóc?

Potrzebuję pomocy

Współczucie, wina i zastraszenie

JAK WYGLĄDA ATAK?

Udawanie pracownika tej samej firmy.

Udawanie przedstawiciela dostawcy, firmy partnerskiej lub agencji rządowej.

Udawanie kogoś, kto ma władzę.

Udawanie nowego pracownika proszącego o pomoc.

Udawanie przedstawiciela producenta systemu operacyjnego zalecającego pilną aktualizację.

Oferowanie pomocy w razie wystąpienia jakiegoś problemu.

Podrzucenie w okolicach stanowiska pracy ofiary dyskietki lub płyty CD-ROM zawierającej niebezpieczny kod.

Używanie wewnętrznej terminologii i żargonu w celu zbudowania zaufania.

Podrzucenie dokumentu lub pliku w pomieszczeniu poczty wewnętrznej firmy, aby dotarł do miejsca przeznaczenia jako korespondencja wewnętrzna.

ATAK- ZNAKI OSTRZEGAWCZE

Odmowa podania
numeru zwrotnego.

Nietypowa prośba.

Okazywanie
posiadania władzy.

Podkreślanie pilności
sprawy.

Groźenie
konsekwencjami
niepodporządkowania
się prośbie.

Okazywanie niechęci w
przypadku zadawania
pytań.

Wymienianie wielu
nazwisk.

Komplementy lub
pochlebstwa.

Flirtowanie.

MAN-IN-THE-MIDDLE

- Przerwanie przesyłania danych – informacja nie dociera do odbiorcy



- Przechwycenie danych – informacja dochodzi do odbiorcy, ale odczytuje ją również strona trzecia



- Modyfikacja danych – informacja zostaje przejęta, zmodyfikowana i w fałszywej postaci dostarczona do odbiorcy

MAN-IN-THE-MIDDLE



Każde podłączenie niezaufanego sprzętu do komputera może skutkować atakiem MIM



Ataki MIM:

Kopiowanie numeru

konta bankowego

Atak na karty zbliżeniowe

MAN-IN-THE-MIDDLE – JAK SIĘ CHRONIĆ?

Inne kanały komunikacyjne

- Telefon
- Kontakt bezpośredni

Potwierdzenie wiadomości

- E-mail zwrotny

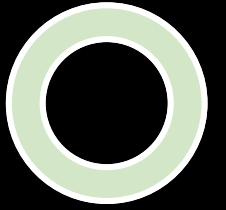
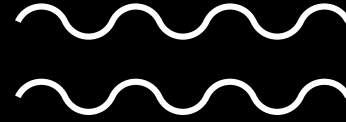
Bezpieczny podpis

- Algorytmy komputerowe zapewniające tożsamość nadawcy

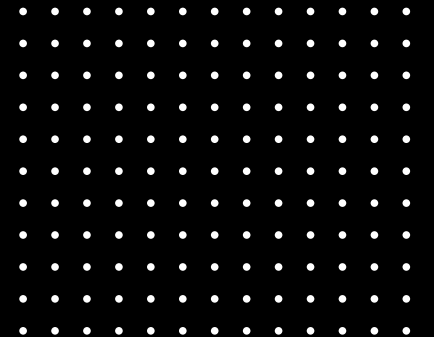
Zdrowy rozsądek

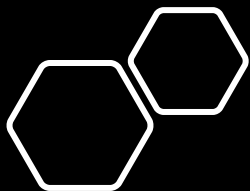
- Publiczna infrastruktura jest niebezpieczna

- „Oczernienie” jest typowym atakiem na stronę internetową zmieniającą jej wygląd zewnętrzny. Zwykle jest skutkiem ataku osób mniej obeznanych technicznie, nowicjuszy w świecie hackerskim.



DEFACE





WIRUSY I POKREWNE

IP:
lokalizacja: Polska

Język: Polski

Ten komputer został zablokowany

Jan Kowalski,

Ten komputer został zablokowany przez system automatycznej kontroli informacyjnej

Dlaczego?

To mogło nastąpić wskutek jednej z następujących przyczyn:

1. Ten komputer był używany w celu odtwarzania zakazanych stron internetowych
2. Ten komputer był używany w celu odtwarzania stron internetowych, zawierających elementy pornografii dziecięcej
3. Ten komputer był używany w celu przekazania informacji zakazanej
4. Ten komputer był używany w celu przechowywania/odtwarzania treści niecenzurowanego

Jak to naprawić?

Według przepisu o "kontroli informacyjnej oraz zabezpieczenia informacji" z dnia 02.01.2012 jest Pan(i) zobowiązany(a) do zapłaty kary w wysokości 500 złotych. W celu ułatwienia procesu płatności udzielamy zabezpieczonej formy płatności za pomocą voucherów Ukash. Wystarczy kupić voucher(y) o wartości 500złotych, wpisać je do formy płatności po czym kliknąć "Wysłać kod".

Co nastąpi po wpisaniu kodu?

Po sprawdzeniu kodu przez nasz system komputer zostanie odblokowany natychmiast. W przypadku wpisania 2 kodów o wartości 250 złotych, proszę wpisać najpierw jeden kod, po otrzymaniu potwierdzenia - następny.

Jak postępować w przypadku powstania problemów?

Jeżeli z jakichś przyczyn nie udało się zapłacić karą za pomocą zabezpieczonej formy płatności, trzeba napisać list na e-mail info@online-cyber-police.com, zaznaczając w treści maila swój adres IP oraz kod(-y) voucheru(-ów) Ukash o wartości 500złotych.

Po sprawdzeniu kodu przez nasz system komputer zostanie odblokowany natychmiast.



Proszę go odblokować za pomocą Ukash

Wpiszcie swój kod "Ukash" o wartości 500 zł

1	2	3	4	5	6	7	8
9	0	Delete					

Proszę wpisywać kod, używając wirtualnej klawiatury



WYŚLAĆ KOD ▶

Co to jest Ukash?

Gdzie mogę kupić Ukash?

Możesz nabyć Ukash w jednym z tysięcy punktów na świecie, przez Internet, przez portfel, w kiosku oraz bankomacie.



Ukash możesz kupić w każdym sklepie z logo eBay.



Zakup kuponu w serwisie dotpay.

WIRUSY I POKREWNE – METODY OCHRONY

Antywirusy

Firewalle (Zapory)

Poprawki systemowe