

Bezpieczny Miesiąc - Kampania ECSM

<https://bezpiecznymiesiac.pl/bm/baza-wiedzy/546,Kampania-Europolu-quotCyberScamsquot.html>

2023-05-30, 03:51

Kampania Europolu "CyberScams"

OSZUSTWA INWESTYCYJNE

Typowe oszustwa inwestycyjne zawierają kuszącą obietnicę zysku poprzez inwestycje w akcje, obligacje, kryptowaluty, rzadkie metale, zagraniczne inwestycje gruntowe lub alternatywne źródła energii.

JAK ROZPOZNAĆ SCAM?

- Wielkośćnie otrzymujesz podgrzane telefony.
- Rozmowa obciąża Ci szybkie zyski i zapewnienia, że inwestycja jest bezpieczna.
- Oferta jest ograniczona czasowo.
- Oferta jest dostępna tylko dla Ciebie i jest przesyłana, aby nie udostępnić jej innym osobom.

CO MOŻESZ ZROBIĆ?

- Zastępnij bezstronne porady finansowej, zanim przeleżesz pieniądze na jakikolwiek inwestycję.
- Nie ufaj telefonom zachęcającym do inwestycji, szczególnie gdy nie znasz rozmówcy.
- Bądź podejrzliwy, gdy ktoś oferuje Ci bezpieczne inwestycje lub gwarancję dużych zysków.
- Uważaj na oszustów, szczególnie jeśli kiedyś padłeś ofiarą scamu. Możesz być osławiany za łatwy cel.
- Jeśli masz jakikolwiek wątpliwość, skontaktuj się z policją.

EUROPOL ECSM NASK #CyberScams

Oszustwa inwestycyjne

OSZUSTWA MATRYMONIALNE

Oszuści kontaktują się z ofiarami na serwisach randkowych, a także przez media społecznościowe lub e-mail.

JAK ROZPOZNASZ SCAM?

- Niezapomnij: Młodego chłopca rozmawiaj osobiście, ponieważ to bardzo mu się podoba i namawia do prywatnych rozmów.
- Wiadomości często są inspirowane i zredagowane.
- Profil nieznanego jest niepełny i niezgodny z tym, co da Ci osoba prywatna.
- Niezapomnij: proszą Cię o wysłanie intymnych zdjęć lub wideo.
- Zdobywa Twoje zaufanie. Potem proszą o pieniądze, podarunki lub szczegóły Twojego konta bankowego.

CO MOŻESZ ZROBIĆ?

- Uważaj jako informację udostępniasz w sieciach społecznościowych i na serwisach randkowych.
- Zachowaj czujność. Oszuści są obecni nawet na renomowanych stronach.
- Nie postępuj pochopnie i zadawaj pytania, gdy masz wątpliwości.
- Przeanalizuj zdjęcie i profil nieznanego, aby sprawdzić, czy nie zostały użyte w innym miejscu.
- Bądź wyczulony na błędy ortograficzne i gramatyczne, niedokładne odpowiedzi i wymówki, takie jak niedziałająca kamera.
- Nie udostępniaj kompromitujących materiałów, które mogłyby zostać użyte do szantażu.
- Jeśli zgodzisz się na spotkanie, powiedz rodzinie oraz przyjaciółm, z kim i gdzie się umawiasz.
- Uważaj na próby o pieniądze. Nigdy nie wysyłaj pieniędzy, danych karty kredytowej, hasła do konta czy kopii dokumentów.
- Unikaj wysyłania płatności z góry.
- Nie przesyłaj pieniędzy nieznanym osobom, ponieważ przesyłanie pieniędzy jest przestępstwem.

JESTEŚ OFIARĄ?

- Nie wstydz się! Należy natychmiast zerwać wszelki kontakt. Jeśli to możliwe, zachowaj historię konwersacji.
- Zawiadom policję.
- Zgłoś władowanie w serwisie, w którym oszust nawiązał z Tobą pierwszy kontakt.
- Jeśli udostępniłeś dane konta bankowego, niezwłocznie skontaktuj się z bankiem.

EUROPOL ECSM NASK #CyberScams

Oszustwa matrymonialne

FAŁSZYWE STRONY INTERNETOWE

Phishing to rozsyłanie wiadomości e-mail, zawierających linki do fałszywej strony internetowej, która do złudzenia przypomina witrynę Twojego banku. Tam jesteś proszony o ujawnienie danych logowania do konta.



JAK ROZPOZNAĆ SCAM?

Fałszywe strony banków wyglądają niemal identycznie jak ich prawdziwe odpowiedniki. Takie witryny często zawierają wyskakujące okienko z prośbą o podanie danych logowania. Prawdziwe banki nie używają takich okien.

Fałszywe witryny:

- Wymuszają natychmiastowe działanie: logowanie, podanie hasła. Bank nie stosuje takiego przemyślenia.
- Wyglądają pokręconie, mają wady techniczne, a także błędy ortograficzne i gramatyczne.
- Używają wraskających okien, które próbują wyłudzić od Ciebie poufne informacje. Nie klikaj w nie, unikaj podawania swoich danych i haseł logowania.

CO MOŻESZ ZROBIĆ?

- Nigdy nie klikaj w linki przesyłane w mailach, które prowadzą do strony Twojego banku.
- Ręcznie wpisz adres strony banku albo korzystaj z linku zapisanego na łacie ulubionych.
- Używaj przeglądarki, która blokuje wyskakujące okna.
- Ważny komunikat z banku nigdy nie jest wysyłany jedynie przez e-mail. Jeśli bank ma dla Ciebie naprawdę ważną wiadomość, zostanie o tym poinformowany po zalogowaniu na swoje konto.



Fałszywe strony internetowe

PHISHING - WYŁUDZANIE INFORMACJI

Phishing to rozsyłanie e-maili, które oszukują odbiorców i namawiają do udostępnienia danych osobowych, finansowych lub dotyczących bezpieczeństwa.

JAK TO DZIAŁA?

Fałszywe wiadomości e-mail mogą wyglądać idealnie tak, jak standardowa korespondencja z banku.

- zawierają dane banku, który widać i tekst przypominający prawdziwe e-maile
- zawierają dołączone załączniki lub linki do stron, które mają wywrzeć na Ciebie presję i nakłonić do działania

Oszuści wykorzystują fakt, że ludzie są zajęci i nie weryfikują się z uwagą w otrzymaną korespondencję.

Bądź szczególnie ostrożny, gdy korzystasz ze smartfona i tableta. Na urządzeniach mobilnych trudniej zorientować się, że jesteś oszukiwany.

CO MOŻESZ ZROBIĆ?

- Przebiegaj o aktualizacji oprogramowania w tym przeglądarki, programu antywirusowego i systemu operacyjnego.
- Zachowaj szczególną czujność, jeśli wiadomość e-mail od banku wymaga podania poufnych informacji (np. danych do logowania).
- Przeprawy się dokładniej wiadomości: porównaj adres z adresem korespondencji z bankiem. Sprawdź, czy nie ma błędów w pisowni i gramatyce.
- Nie odpowiadaj na podejrzane wiadomości e-mail. Przetnij je do swojego banku ręcznie w oficjalnym serwisie.
- Nie ściągaj załączników i nie klikaj w podejrzane linki. Zmniejsz tego samodzielnego wpisu podany adres w wyszukiwarce.
- Jeśli masz wątpliwości, sprawdź informację na stronie swojego banku, lub zadzwoń na infolinię.



Phishing


OSZUSTWA W SKLEPACH INTERNETOWYCH

Oferty sklepów internetowych mogą być świetną okazją nie tylko dla Ciebie, ale również dla oszustów.

CO MOŻESZ ZROBIĆ?

- Korzystaj z najlepszych sklepów internetowych, gdy masz taką możliwość. Bądź świadomy, z kim się kontaktujesz, jeśli zgadzasz taką potrzebę.
- Sprawdź opinie o sklepie, zanim cokolwiek w nim kupisz.
 - Płać kartą kredytową - będziesz mieć większe szanse odzyskania pieniędzy.
 - Płać używając bezpiecznej usługi płatniczej - uważaj na sklepy, które akceptują jedynie przelewy.
 - Płać przez internet tylko, gdy jesteś połączony z bezpieczną siecią - unikaj bezpłatnego lub publicznego Wi-Fi.
 - Używaj do płatności bezpiecznego urządzenia - aktualny system operacyjny i oprogramowanie zabezpieczające.
- Sprzedz się reklamami oferującymi cudowne produkty i podejrzane przeceny - jeśli coś brzmi zbyt pięknie, raczej nie jest prawdziwe!
- Wyskakujące okno informuje, że wygrałeś nagrodę? Zastanów się zanim klikniesz - możesz wygrać wirusa.
- Jeśli nie otrzymasz produktu, skontaktuj się ze sprzedawcą. Nie odpowiadaj? Zadzwoń do banku.

Zawsze zgłaszaj policji wszelkie próby oszustwa, nawet jeśli ostatecznie nie padłeś ofiarą.



Fałszywe sklepy internetowe

VISHING - WYŁUDZENIE PRZEZ TELEFON

Vishing (kombinacja słów Voice - głos i Phishing) to telefoniczne wyłudzenie informacji osobistych/finansowych. Vishing może być powiązany z namową do przekazania pieniędzy.



CO MOŻESZ ZROBIĆ?

- > **Być ostrożny**, gdy odbierasz połączenia z nieznanymi numerami.
- > **Poproś dzwoniącego o numer telefonu** i powiedz, że oddzwonisz.
- > **Sprawdź wiarygodność organizacji**, wyszukaj w internecie ich numer telefonu i zaadresuj bezpośrednio.
- > **Nie sprawdzaj dzwoniącego za pomocą numeru telefonu, który Ci podał** (to może być fałszywy numer).
- > **Ostrzeżenie** mogą wykorzystywać informacje znalezione w internecie i mediach społecznościowych. Nie zakładaj, że są uczciwi tylko dlatego, że dużo o Tobie wiedzą.
- > **Nigdy nie udostępniaj numeru PIN do karty kredytowej i hasła do konta**. Twój bank nigdy nie zapytałby o takie informacje przez telefon.
- > **Nie dokonuj przelewu na ich prośbę**. Twój bank nigdy by Cię o to nie poprosił.
- > **Jeśli wydaje Ci się, że odebrałeś telefon od oszusta, powiadom swój bank.**



Logo: EURPOL ECR, NASK, #CyberScams

Vishing

WYŁUDZANIE INFORMACJI SMSEM

Smishing (kombinacja słów SMS i Phishing) to próba wyłudzenia informacji poufnych, firmowych lub dotyczących bezpieczeństwa za pośrednictwem SMS.



JAK TO DZIAŁA?

Otrzymujesz SMS, w którym nadawca prosi Cię o kliknięcie linku lub telefon pod wskazany numer, aby "zweryfikować", "zaktualizować" lub "poprawnie aktywować" konto. Odszczepki prowadzą do fałszywej strony/telefonu oszusta, który podaje się za usługodawcę.

CO MOŻESZ ZROBIĆ?

- > **Nie klikaj linków, załączników ani obrazów** otrzymanych w SMS nie wiadomego pochodzenia, bez wcześniejszego sprawdzenia nadawcy.
- > **Nie spiesz się**. Sprawdź źródło wiadomości zanim udzielicz odpowiedzi.
- > **Nigdy nie odpowiadaj na SMS**, który prosi o podanie Twojego numeru PIN, hasła do konta bankowego lub innych poufnych informacji.
- > **Jeśli podałeś swoje dane w odpowiedzi na SMS**, który mógł być wyłudzeniem, niezwłocznie skontaktuj się z bankiem.

Logo: EURPOL ECR, NASK, #CyberScams

Wyłudzenie przez SMS

BIZNESOWE OSZUSTWO "NA DYREKTORA"

Oszuści podszywają się pod dyrektora, żeby skłonić pracownika do zapłaty fałszywej faktury lub wykonania nieautoryzowanego przelewu z konta firmowego.

JAK TO DZIAŁA?

- Oszuści często lub wręcz e-mail podszywają się pod osobę wysoko postawioną w firmie (np. dyrektora, dyrektora ds. finansów).
- Jest dobrze poinformowany o strukturze organizacji.
- Domaga się decyzyjnych natychmiastowego przelewu.
- Gra na emocjach, używa zwrotów takich jak "poufność", "tęma Ci, jak", "pilnie obecnie niedostępny".
- Jako argumentu używa wyjątkowej sytuacji (kontrola podatkowa, przejęcie firmy, fuzja).
- Często prośba dotyczy płatności na konto w banku spoza Europy.
- W efekcie pracownik przelewa pieniądze na konto oszusta.
- Informuje, że dalsze instrukcje pracownik otrzyma później, mailowo albo za pośrednictwem innych osób.
- Prosi, aby pracownik pomógł standardowe procedury autoryzacji płatności.

JAK ROZPOZNAĆ SCAM?

- Otrzymujesz niespodziewany e-mail/telefon.
- Wyczaszaj presję. Zadanie ma być wykonane jak najszybciej.
- Kontaktuje się z Tobą osoba wysoko postawiona w firmie, z którą na co dzień nie współpracujesz.
- Otrzymujesz niecodzienne zadanie, które jest niezgodne z procedurami wewnętrznymi.
- Jesteś przestany o zachowanie całkowitej poufności.
- Słyszysz pochwały, groźby albo obietnice nagrody.

CO MOŻESZ ZROBIĆ?

JAKO FIRMA	JAKO PRACOWNIK
<p>Bądź świadomy ryzyka i ostrzeż o nim swoich pracowników.</p> <p>Poproś, aby pracownicy traktowali podjęcie przelewu z najwyższą ostrożnością.</p> <p>Stwórz wewnętrzne procedury dotyczące płatności.</p> <p>Wprowadź procedury sprawdzania płatności, które są decyzyjne mailowo.</p> <p>Stwórz procedury raportowania scamów i oszustw.</p> <p>Sprawdź, czy na stronie internetowej firmy nie ma informacji, które umożliwiają poznanie struktury przedsiębiorstwa. Uwaga! Nie publikuj w mediach społecznościowych.</p> <p>Zaktualizuj zabezpieczenia techniczne.</p> <p>Zawsze informuj policję o próbach oszustwa, nawet jeśli nie zostalś ofiarą scamu.</p>	<p>Skonfiguruj do procedur bezpieczeństwa, szczególnie tych związanych z płatnościami. Nigdy nie udaj się na stronę, nie otwieraj procedury autoryzacji.</p> <p>Uważnie sprawdzaj adres e-mail, szczególnie gdy wiadomość zawiera informacje poufne/decyzyjne przelewu.</p> <p>Gdy masz wątpliwości, skontaktuj się z innym pracownikiem.</p> <p>Nigdy nie otwieraj podejrzanych załączników i linków otrzymywanych w e-mailu. Zachowaj szczególną ostrożność, gdy sprawdzasz prywatną pocztę na firmowym komputerze.</p> <p>Nie podawaj zbyt wiele informacji i zachowaj ostrożność w mediach społecznościowych.</p> <p>Nie udostępniaj informacji o strukturze firmy, hierarchii, bezpieczeństwie i obowiązujących procedurach.</p> <p>Jeśli otrzymasz podejrzana wiadomość albo telefon – zawsze skontaktuj się z działem IT.</p>

Oszustwa na dyrektora

WYŁUDZENIA "NA FAKTURĘ"

JAK TO DZIAŁA?

- Z firmą kontaktuje się osoba, która podaje się za reprezentanta dostawcy i usługodawcy / wierzyciela.
- Oszust może kontaktować się osobiste telefonem, mailowo albo listownie.
- Oszust informuje o zmianie danych do płatności przyrzecz faktur. Podaje numery na nowo, kontrolowane przez siebie konta.

CO MOŻESZ ZROBIĆ?

JAKO FIRMA	JAKO PRACOWNIK
<p>Uperwij się, że pracownicy są poinformowani o możliwości oszustwa i będą potrafili go unikać.</p> <p>Stwórz procedurę weryfikacji danych do płatności.</p> <p>Sprawdź badania rzekomo pochodzące od Twójch wierzycieli, zwłaszcza jeśli pojawiła się o zmianę danych bankowych dotyczących przyszłych faktur.</p> <p>Nie korzystaj z danych kontaktowych umieszczonych w podejrzanej wiadomości. Używaj wyłącznie wykorzystywanych we wcześniejszej korespondencji.</p> <p>W każdej ze współpracujących firm ustal jedną osobę kontaktową w sprawie płatności. Domagaj się jej adresowania w przypadku jakichkolwiek zmian.</p>	<p>Przejdź zespół odpowiedzialny za płatności, aby zawsze uważnie sprawdzał dane.</p> <p>Przejrzyj stronę internetową firmy, jeśli to możliwe usiłuj z niej informacje o dostawcach i usługodawcach. Zwracaj uwagę jakie informacje o firmie umieszczają pracownicy w mediach społecznościowych.</p> <p>Dla płatności powyżej wyznaczonego pułapu, utwórz procedurę potwierdzającą prawidłowe dane do przelewu oraz odbiorcę (np. spotkanie z firmą).</p> <p>Po opłaceniu faktury wyślij potwierdzenie e-mailem. Dla bezpieczeństwa podaj nazwę banku beneficjenta i cztery ostatnie cyfry z numeru konta.</p>

Ogranicz informacje, które udostępniasz o swoim pracowniku w mediach społecznościowych.

Skontaktuj się z policją, jeżeli podejrzewasz oszustwo, nawet jeśli nie padłeś jego ofiarą.

Oszustwo "na fakturę"

PLIKI DO POBRANIA

Fałszywe strony banków (mp4, 9.57 MB) 04.06.2019 14:14

Oszustwa matrymonialne (mp4, 13.15 MB) 04.06.2019 14:14

Phishing, Smishing oraz Vishing (mp4, 14.74 MB) 04.06.2019 14:15

Oszustwa na dyrektora (mp4, 13.81 MB) 04.06.2019 14:15

Oszustwa inwestycyjne (mp4, 14.09 MB) 04.06.2019 14:15

Oszustwo "Na fakturę" (mp4, 13 MB) 04.06.2019 14:16

Kradzież danych osobowych (mp4, 14.36 MB) 04.06.2019 14:16

[Drukuj tą stronę](#)
[Generuj PDF z tej stronie](#)

[Poprzedni Strona](#)
[Następny Strona](#)