Jak łatwo okraść Cię w sieci?

AGENDA

01

Dlaczego mamy do czynienia z hackerami? Jakie są powody przeprowadzania takich działań, oraz dlaczego możemy stać się celem.

02

Rodzaje ataków.
W jaki sposób hackerzy zdobywają nasze loginy, hasła, konta bankowe. Jak sami ułatwiamy im to zadanie. Jak się przed tym chronić.

03

Co zrobić, gdy jednak staniemy się ofiarą ataku. Jakie działania wdrożyć i jak wyjść z tego cało.

04

Bezpieczeństwo w Social Mediach.
Dlaczego w dużej mierze to od nas zależy czy hackerzy obiorą nas za cel. Przyklady „what could go wrong”.


TIME
Dlaczego

5 powodów

Dlaczego

Motywacje hakerów są złożone i różnorodne, a jednostki działające w obszarze cyberprzestępczości mogą mieć różne cele i powody. Omówimy sobie kilka głównych motywacji.

Działania Finansowe

Jednym z głównych motywów jest uzyskiwanie korzyści finansowych. Ataki na systemy bankowe, kradzież tożsamości, szantaże lub wymuszanie opłat w zamian za odblokowanie danych - to tylko kilka przykładów działań skierowanych na osiągnięcie zysku materialnego.

Uznanie Reputacja

Niektórzy działają z chęci udowodnienia swoich umiejętności technicznych, udowodnienia zdolności lub po prostu zaspokojenia własnej ambicji.

Ataki te mogą być prowadzone dla zwiększenia prestiżu w społeczności hakerskiej.

Działania Społeczne

“We Do Not Forgive.
We Do Not Forget.
Expect Us.”

Anonymous

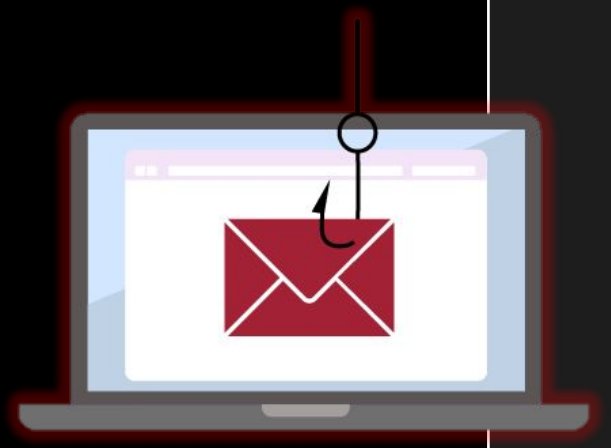
My nie wybaczamy.
My nie zapominamy.
Spodziewaj się nas.

Działania Makro

Państwa, organizacje międzynarodowe mogą przeprowadzać ataki w celu pozyskania poufnych informacji.

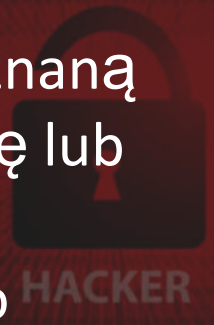
Szpiegostwo przemysłowe i polityczne to motywacje, które prowadzą do infiltracji systemów w poszukiwaniu tajemnic handlowych, danych badawczych lub poufnych informacji.

Rodzaje ataków

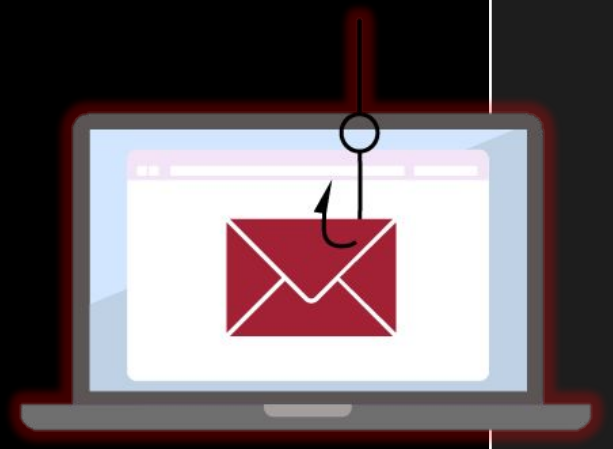


Phishing

…sposób wyłudzanie osobistych informacji podszywanie się pod znaną użytkownikowi z nazwy instytucję lub osobę, w celu późniejszego wykorzystania tych informacji do nieuprawnionych działań.



Phishing - statystyki



25 625 incydentów

64% wszystkich incydentów hakerskich

Najczęstsze podszycia: InPost, FB, Vinted

dane za rok 2023

Bnp paribas <david.shears@bellaliant.net>

Drogi Kliencie,

Nasz system wykryje, że nie aktywowałeś jeszcze naszej nowej usługi bezpieczeństwa Hsbc Secure Key, dzięki czemu możesz łatwo kontrolować swoje konto

Otrzymany SMS-em kod zniknie z
r., teraz korzystaj z nowych, darmo
kontrolowania zakupów internetow

Aktywuj usługę:

https://goonline.bnpparib

1. Zidentyfikuj się za pomocą s
bankowych.
2. Wpisz kod wysłany do Ciebi
telefonu podany w Twoim ba

Zauważ, że ten komunikat jest g
Nie używaj funkcji „odpowiedz d

Dziękuję za twoje zaufanie.

Grupa BNP Paribas.

https://anacetina.com/readme.php

https://sportquillesespalionnais.fr/wp-includes/certificates/thems/web/

OVHcloud.pl <5a2fd@ambulances-boularand.fr>
to aj

Szanowny Kliencie!

Jesteśmy zobowiązani poinformować o tym, aby uniknąć zawieszenia nazwy domeny [redacted].pl.

Zadłużenie należy uregulować w wysokości 10.00 euro przed 07/09/2022, pod następującym linkiem:

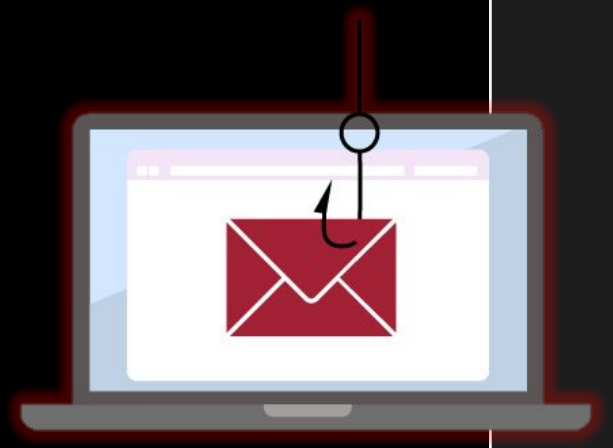
Uspokoić się teraz

Dziękujemy za Twoją wierność

Z poważaniem,

Obsługa klienta OVHcloud

Phishing - jak się chronić?



Wprowadź uwierzytelnianie dwuskładnikowe

Weryfikuj adresatów wiadomości oraz linki

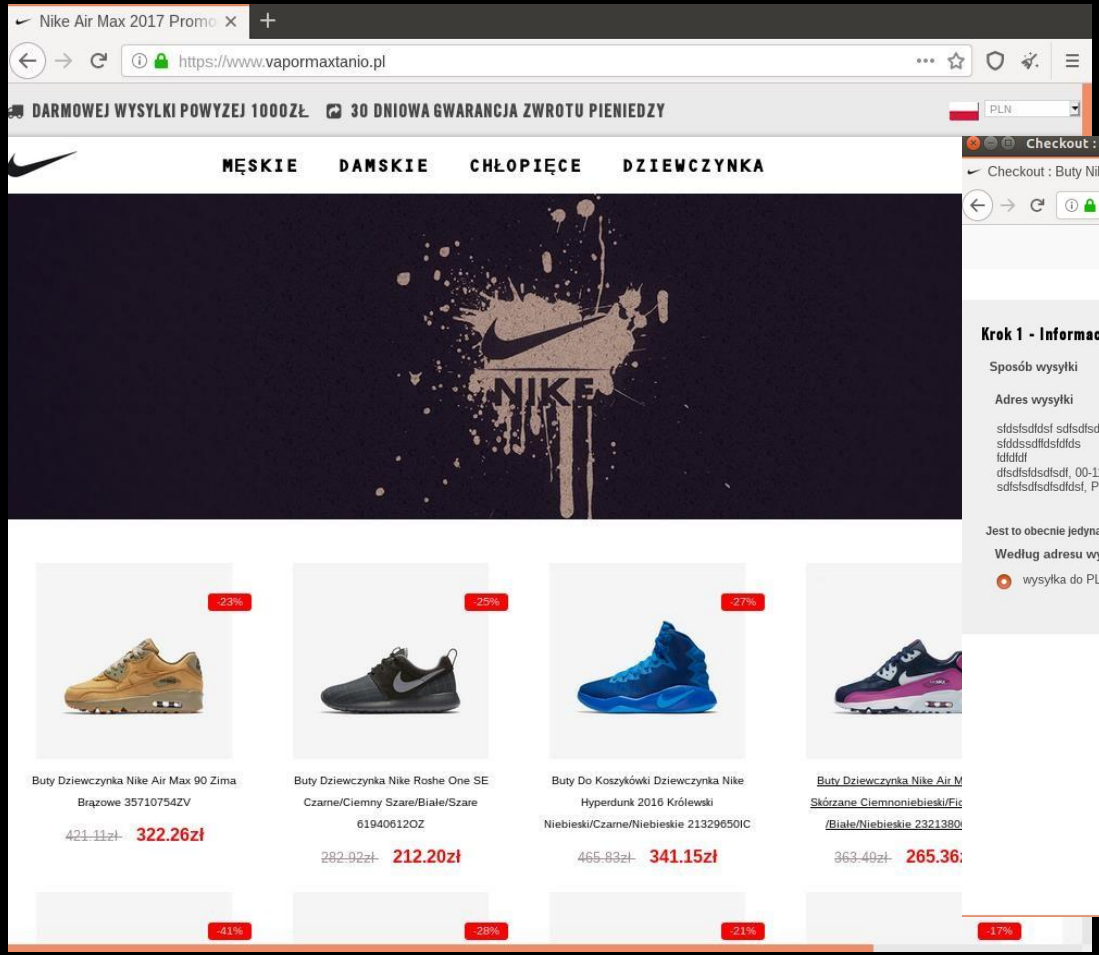
Podchodź do sprawy na chłodno

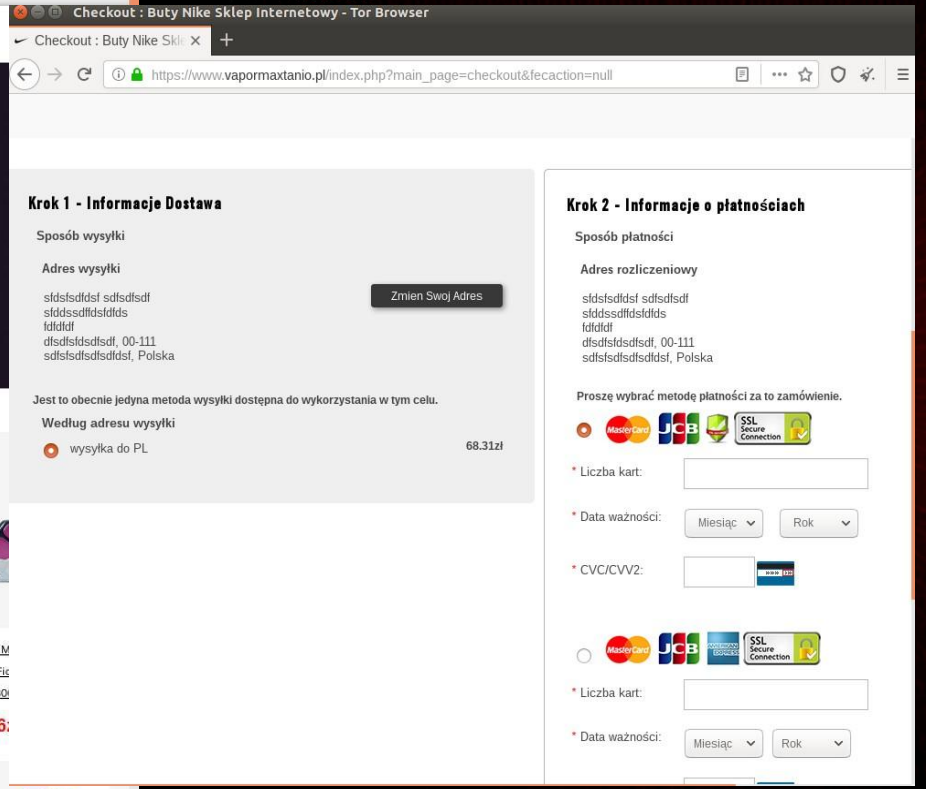
Fake Shop

Fałszywe sklepy z produktami detalicznymi

Fałszywe giełdy kryptowalut lub papierów

Fałszywe zbiórki


Nike Air Max 2017 Promo
https://www.vapormaxtanio.pl
DARMOWEJ WYSYLKI POWYZEJ 1000ZŁ
30 DNIOWA GWARANCJA ZWROTU PIENIEDZY
PLN
MĘSKIE
DAMSKIE
CHŁOPIĘCE
DZIEWCZYNKA
NIKE
-23%
Buty Dziewczynka Nike Air Max 90 Zima Brązowe 35710754ZV
421.11zł
322.26zł
-25%
Buty Dziewczynka Nike Roshe One SE Czarne/Ciemny Szare/Białe/Szare 61940612OZ
282.92zł
212.20zł
-27%
Buty Do Koszykówki Dziewczynka Nike Hyperdunk 2016 Królewski Niebieski/Czarne/Niebieskie 21329650IC
465.83zł
341.15zł
Buty Dziewczynka Nike Air M
Skórzane Ciemnoniebieski/Fi
/Białe/Niebieskie 2321380
363.40zł
265.36
-41%
-28%
-21%
-17%


Checkout : Buty Nike Sklep Internetowy - Tor Browser
Checkout : Buty Nike Skl
https://www.vapormaxtanio.pl/index.php?main_page=checkout&fecaction=null
Krok 1 - Informacje Dostawa
Sposób wysyłki
Adres wysyłki
sfdsfsdfdsf sdfsdfsdf
sfddssdffdsfdfds
fdfdfdf
dfsdfsfdsdfsdf, 00-111
sdfsfsdfsdfsdfdsf, Polska
Zmien Swoj Adres
Jest to obecnie jedyna metoda wysyłki dostępna do wykorzystania w tym celu.
Według adresu wysyłki
wysyłka do PL
68.31zł
Krok 2 - Informacje o płatnościach
Sposób płatności
Adres rozliczeniowy
sfdsfsdfdsf sdfsdfsdf
sfddssdffdsfdfds
fdfdfdf
dfsdfsfdsdfsdf, 00-111
sdfsfsdfsdfsdfdsf, Polska
Proszę wybrać metodę płatności za to zamówienie.
SSL Secure Connection
* Liczba kart:
* Data ważności:
Miesiąc
Rok
* CVC/CVV2:
SSL Secure Connection
* Liczba kart:
* Data ważności:
Miesiąc
Rok

Fake Shop - jak rozpoznać?

Podejrzanie zaniżone ceny

Duża ilość literówek, niepoprawna odmiana

Brak lub złe opinie w Google

Fake Shop - jak rozpoznać?

Jeden sposób płatności, tylko kartą

Reklamy Google nie świadczą o zaufanym sklepie

Sca
m

Chociaż są różne odmiany, to istota tego oszustwa zazwyczaj polega na próbie wciągnięcia ofiary w kłamliwą transakcję finansową. Tego rodzaju działania są nielegalne i mają na celu wyłudzenie pieniędzy od ofiar poprzez manipulację i wprowadzenie ich w błąd.

Scam

Nie wysyłać swoich oszczędności księciom ...

... ani astronautom, policjantom, ...

... ani innym cwaniakom.

Phishing

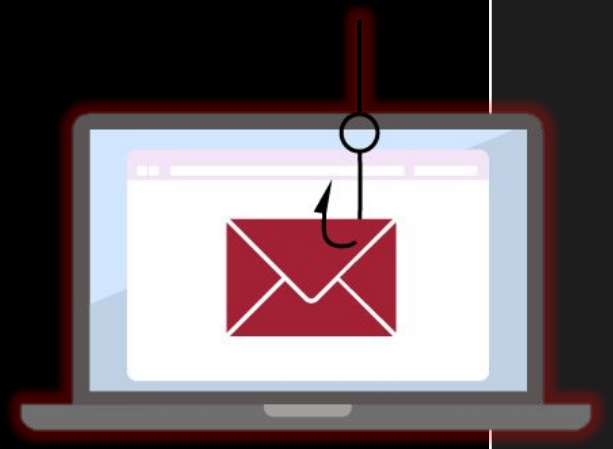
Chodzi o to, żebyś... kliknął!

Fake Shop

Chodzi o to żebyś… kupił!

Scam

Chodzi o to, żebyś… wysłał!



Amateurs hack systems,
proffesionals hack people.

Amatorzy hakują systemy,
profesjonaliści hakują ludzi.

~Bruce Schneier

Najsłabszym ogniwem w łańcuchu bezpieczeństwa jest czynnik ludzki.

Kevin

Co jeżeli damy się złapać?

01

Jeżeli masz dostęp do serwisu – zmień hasło, włącz uwierzytelnianie dwuskładnikowe.

Co jeżeli damy się złapać?

01

Jeżeli masz dostęp do serwisu – zmień hasło, włącz uwierzytelnianie dwuskładnikowe.

02

Wyloguj się ze wszystkich aktywnych sesji podpiętych pod konto

Co jeżeli damy się złapać?

01

Jeżeli masz dostęp do serwisu – zmień hasło, włączenie uwierzytelniani e dwuskładnikowe.

02

Wyloguj się ze wszystkich aktywnych sesji podpiętych pod konto

03

Sprawdź, czy nie zostały podpięte do konta żadne nieznane aplikacje.

Co jeżeli damy się złapać?

01

Jeżeli masz dostęp do serwisu – zmień hasło, włączenie uwierzytelniani e dwuskładnikowe.

02

Wyloguj się ze wszystkich aktywnych sesji podpiętych pod konto.

03

Sprawdź, czy nie zostały podpięte do konta żadne nieznane aplikacje.

04

Jeżeli chodzi o utratę danych karty bankowej/ dowodu osobistego – zastrzeż je i poinformuj służby

CERT Polska

Cert Polska Zgłoś Incydent

Ostrzeżenia

Raport roczny 2023

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:
Zgłaszanie osoby kontaktowej do CSIRT NASK.

Jeżeli chcą Państwo zgłosić złośliwą domenę, proszę użyć poniższego odnośnika:
Zgłaszanie domeny internetowej służącej do wyłudzeń danych i środków finansowych.

Zgłaszanie podejrzanych wiadomości SMS

Wszystkie podejrzane wiadomości SMS z linkami można zgłosić używając funkcji "Przekaż", bezpośrednio na numer:

8080

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

- Osoba fizyczna / inne podmioty
- Operator usług kluczowych
- Dostawca usługi cyfrowej
- Podmiot publiczny

Jak się zabezpieczyć?

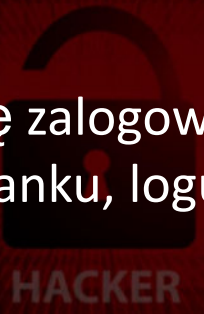
OGÓLNE ZASADY, JAK SIĘ CHRONIĆ?

1. Włącz uwierzytelnianie dwuskładnikowe.

2. Zachowaj ostrożność w sytuacji, gdy jedyną formą płatności w sklepie internetowym jest płatności kartą.

3. Jeżeli nastąpi przekierowanie na serwis do którego musisz się zalogować – zweryfikuj adres strony. Czy na pewno logując się do swojego banku, logujesz się do banku, a nie hackerTest.com?

4. Sprawdzaj adres nadawcy, linki oraz załączniki
   NIE KLIKAJ W LINKI I NIE ŚCIĄGAJ ZAŁĄCZNIKÓW!!!



OGÓLNE ZASADY, JAK SIĘ CHRONIĆ?

5. Sprawdzaj co jakiś czas czy twoje hasło znalazło się w wycieku danych:

haveibeenpwned.com

6. Zwracaj uwagę na formę zdań, błędy ortograficzne, literówki (nieważne czy w mailu/sms, czy na stronach internetowych).

7. Używaj silnych haseł – stosuj zasady sugerowane przez CERT Polska
https://cert.pl/bezpieczne-hasla/

8. Pamiętaj, że googlowska reklama sklepu wcale nie znaczy, że jest on godny zaufania. Takie reklamy można wykupić samemu, nieważne jakie jest przeznaczenie sklepu.

OGÓLNE ZASADY, JAK SIĘ CHRONIĆ?

9. Jeżeli twój bliski znajomy/rodzina poprosi Cię na social mediach o przesłanie pieniędzy – zadzwoń do niego. Zweryfikuj tę wiadomość.

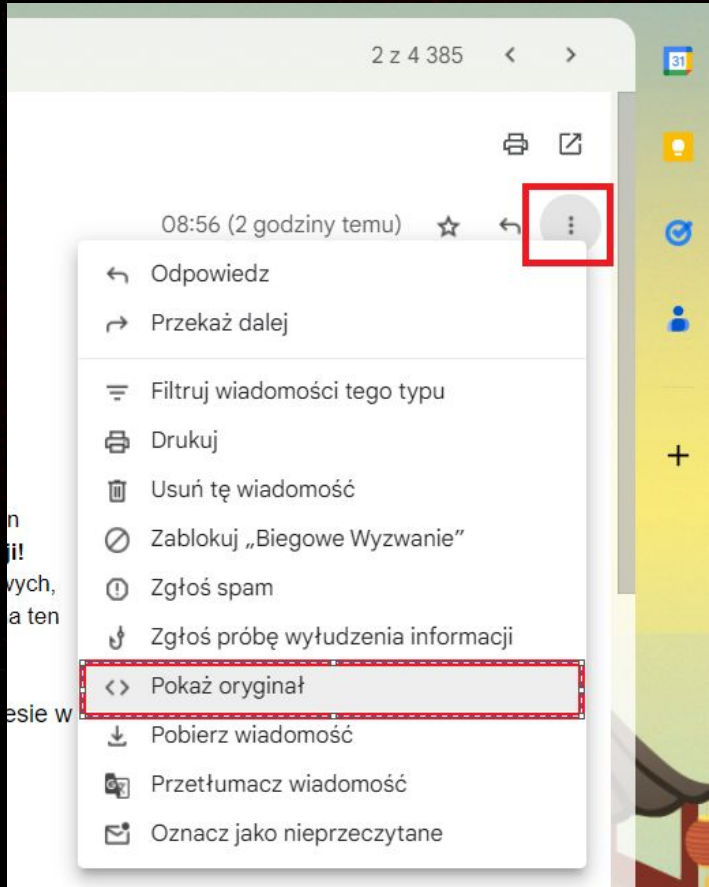
10. Rób co jakiś czas kopię zapasową swoich danych. Nawet jeżeli utrata danych nie zabolałaby nas tak bardzo jak duże przedsiębiorstwo, to jednak zamiętajmy, że komputery i telefony są nośnikami np. zdjęć, filmów. Nie stracimy może dokumentu „podsumowanie 3 kwartału 2022”, ale możemy stracić zdjęcia/filmy np. „ostatnie wakacje”.

11. Podchodź do sprawy „na chłodno”, nawet jeżeli otrzymana przez Ciebie wiadomość narzuca formę „natychmiastowej płatności”, „TERAZ, ZARAZ!” – zachowaj spokój.

WERYFIKACJA ADRESU EMAIL, LINKÓW ORAZ ZAŁĄCZNIKÓW w poczcie

Otwórz e-mail i znajdź opcję wyświetlania pełnych nagłówków.

W większości programów pocztowych możesz to zrobić, otwierając e-mail, a następnie szukając opcji "Pokaż źródło", "Pokaż nagłówki" lub podobnej.



WERYFIKACJA ADRESU EMAIL, LINKÓW ORAZ ZAŁĄCZNIKÓW w poczcie

- Sprawdź "Od":

Znajdź linijkę, która zaczyna się od "From" lub "Od".
Tu powinno zawierać rzeczywisty adres e-mail nadawcy. Zwróć uwagę na cały adres, nie tylko na nazwę nadawcy.

- Zweryfikuj domenę:

Sprawdź, czy domena (część adresu e-mail po znaku "@") wydaje się autentyczna. Czy to jest np. "nazwafirmy.com" dla oficjalnej firmy, czy coś podejrzanego i dziwnego?

WERYFIKACJA ADRESU EMAIL, LINKÓW ORAZ ZAŁĄCZNIKÓW w poczcie

- Patrz na "Received" (Otrzymane):

Znajdź sekcję "Received". To pokazuje, przez jakie serwery przeszła wiadomość. Sprawdź, czy są to serwery związane z oficjalnymi dostawcami .

- Weryfikacja linków:

Najedź kursorem myszy na link, ale go nie klikaj. Przytrzymaj kursor przez kilka sekund, po chwili powinno wyświetlić się miejsce docelowe linku.

Link, który wydaje się prowadzić do jednej lokalizacji, ale w rzeczywistości prowadzi do innej, powinien dać nam do myślenia.

WERYFIKACJA LINKÓW

Jak najbardziej można też zweryfikować go w źródle strony:

- najedź myszką na link,
- kliknij prawy przyciskiem myszy i zaznacz „Zbadaj”.
- Na waszym ekranie pojawi się kod z zaznaczoną linijką tekstu. Ta linijka odpowiada właśnie za link w wiadomości.

```
<div class="acx-link-list">
  <p>…</p>
  <p>
    <a href="https://www.owasp.org/index.php/Improper_Error_Handling" target="_blank">Improper Error Handling</a> == $0
  </p>
</div>
<h2 class="mt30">Related Vulnerabilities</h2>
```

- w znaczniku href po znaku równa się zapisany jest prawdziwy link pod jaki przejdziemy po kliknięciu w hiperłącze. W tym przypadku jest to: https://www.owasp.org/index.php/Improper_Error_Handling

WERYFIKACJA ZAŁĄCZNIKÓW

Jeżeli masz, chociaż najmniejsze podejrzenia co do zaufania załączniku, zweryfikuj go przez usługę VirusTotal.

Jest to bezpłatna usługa online umożliwiająca skanowanie plików pod kątem obecności złośliwego oprogramowania.

Usługa ta umożliwia również weryfikację hiperłącza.

https://www.virustotal.com/gui/home/upload

PRZYDATNE STRONY

https://cert.pl – Strona CERT Polska

https://incydent.cert.pl/ - CERT Polska Zgłoś Incydent

https://cert.pl/bezpieczne-hasla/ - CERT Polska zasady silnych haseł

https://haveibeenpwned.com/ - Sprawdź, czy twoje hasło było w jednym z wycieków danych

https://www.virustotal.com/gui/home/upload - Weryfikacja załączników/linków.

Dziękuję za uwagę.

Prezentacja z materiałów OSE Hero

opracowanie do formatu Prezentacji Google
Andrzej Gągało