Dokument jest dodatkiem do prezentacji

„Security, jak łatwo okraść Cię w sieci."

Przedstawiono tu zasady bezpieczeństwa, jak wprowadzić uwierzytelnianie dwuskładnikowe na przykładowym serwisie, jak weryfikować adresy, linki oraz załączniki w wiadomościach oraz wypisano wszystkie strony/linki omawiane w prezentacji i te, które zdaniem prowadzącego przydadzą się Państwu.

OGÓLNE ZASADY, JAK SIĘ CHRONIĆ?

1. Włącz uwierzytelnianie dwuskładnikowe (opisano na przykładowym serwisie w rozdziale „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 Amazonu, logujesz się do Amazonu a nie hackerTest.com?
4. Sprawdzaj adres nadawcy, linki oraz załączniki (opisano w rozdziale „Weryfikacja adresu email, linków oraz załączników).

   NIE KLIKAJ W LINKI I NIE ŚCIAGAJ ZAŁĄCZNIKÓW!!!

   Przykład z prezentacji został przedstawiony celowo, by pokazać, że mimo iż klikamy w link o nazwie „bank", mimo iż na stronie wyświetla nam się logo banku, to nie jest to strona bankowa, a strona postawiona przez przestępców.
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, nie ważne jakie jest przeznaczenie sklepu.
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 pamiętajmy, że komputery i telefony są nośnikami np. zdjęć, filmów. Nie stracimy może dokumentu „podsumowanie 3 kwartału 2022" ale możemy stracić zdjęcia/filmy np. „roczek dzieci".
11. Podchodź do sprawy „na chłodno", nawet jeżeli otrzymana przez Ciebie wiadomość narzuca formę „natychmiastowej płatności", „TERAZ, ZARAZ!" – zachowaj spokój.

UWIERZYTELNIANIE DWUSKŁADNIKOWE

Jak włączyć 2FA (weryfikacja dwuetapowa)?

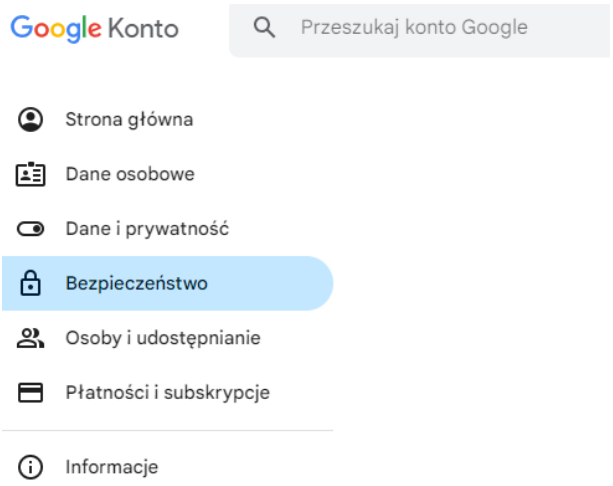
W każdym przypadku czy to jest Facebook, Instagram, inne social media, giełdy, banki – wpisz w przeglądarce (może być w Google) nazwę usługi oraz „uwierzytelnianie dwuskładnikowe instrukcja", np.:

- mbank uwierzytelnianie dwuskładnikowe instrukcja,
- allegro uwierzytelnianie dwuskładnikowe instrukcja.

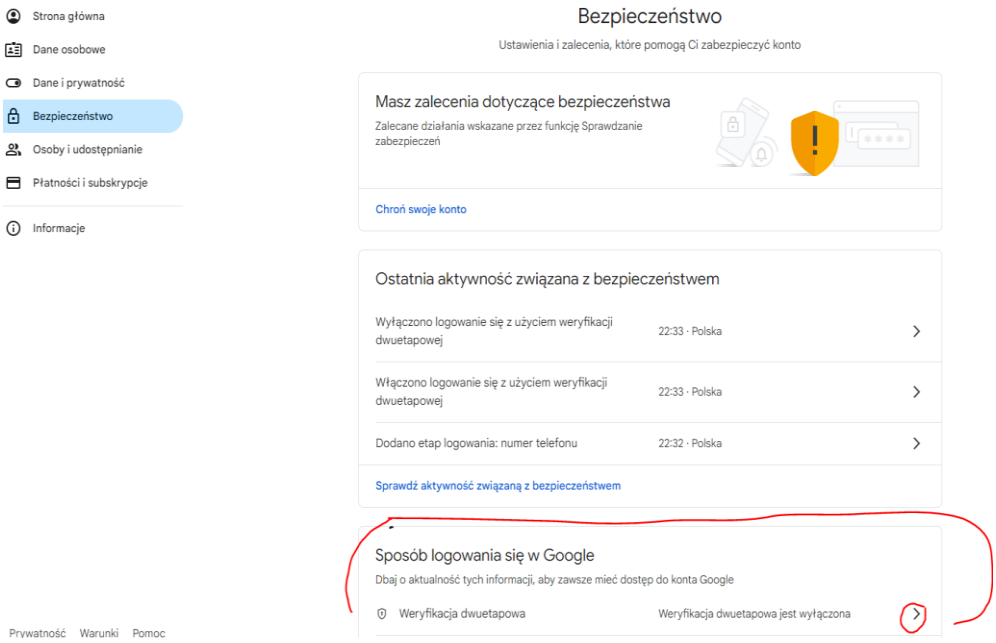
Przykład włączenia uwierzytelniania w Google.

1. wejdź na swojego Gmaila,
2. w prawym górnym roku kliknij ikonke swojego profilu,

3. przejdź do „Zarządzaj swoim kontem"
4. w menu po lewej stronie kliknij „Bezpieczeństwo"



5. Włącz uwierzytelnianie dwuskładnikowe.

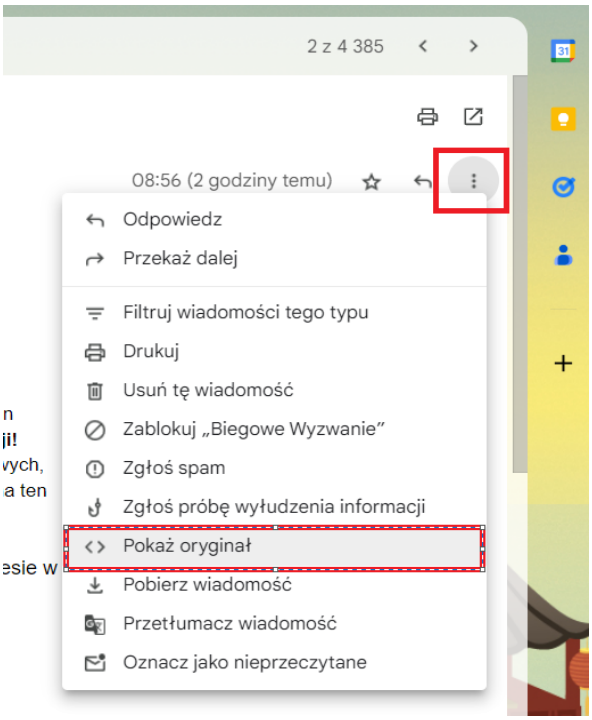


6. Dalej postępuj zgodnie z instrukcjami na ekranie. Google przejdzie z Tobą przez wszystkie kroki.

WERYFIKACJA ADRESU EMAIL, LINKÓW ORAZ ZAŁĄCZNIKÓW:

1. Weryfikacja nadawcy

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.



- Sprawdź "Od":

Znajdź linijkę, która zaczyna się od "From" lub "Od". To 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?

- Patrz na "Received":

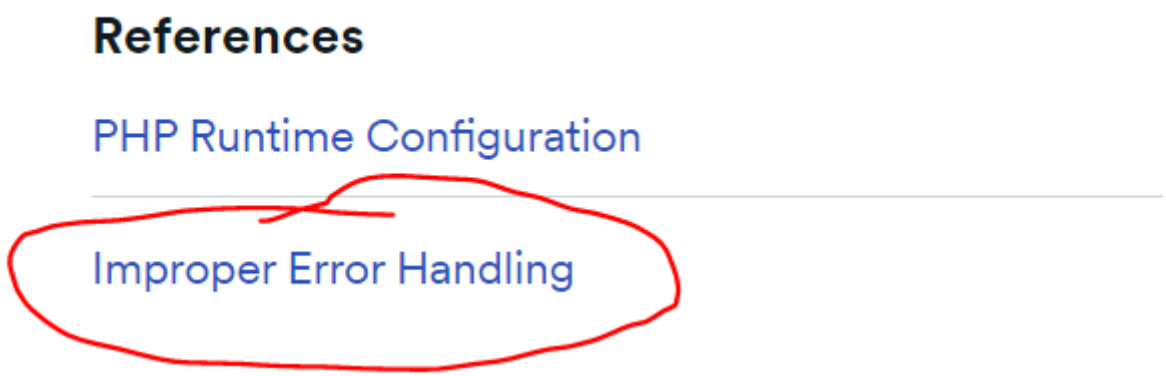
Znajdź sekcję "Received". To pokazuje, przez jakie serwery przesz. Patrz, czy są to serwery związane z oficjalnymi dostawcami e-maila lub firma

2. 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.

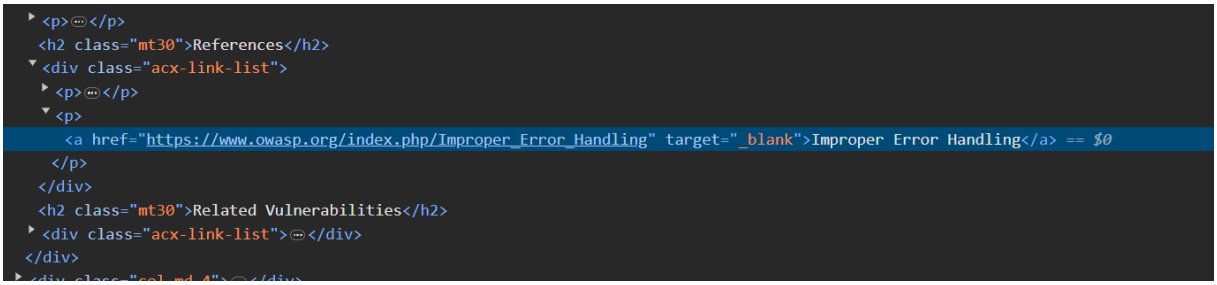
Jak najbardziej można też zweryfikować go w źrodle strony. Załóżmy że mamy taki link:



- 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.



- 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

3. 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.

Materiał został przygotowany przez Katarzynę Trojanowską.

Dziękujemy!