

WYDZIAŁ
**ELEKTROTECHNIKI
I INFORMATYKI**
POLITECHNIKI RZESZOWSKIEJ

Katarzyna Szostak

Phishing – przykłady, prezentacja,
oprogramowanie.

Inżynieria i Analiza Danych
L5

1. Wstęp

Phishing to jeden z najpopularniejszych rodzajów ataku internetowego, który bazuje na przekazywaniu fałszywych informacji za pomocą e-maili lub SMS-ów. Wykorzystuje technikę inżynierii społecznej, która polega na manipulacjach mających na celu oszukanie odbiorcy i nakłonienie go do podejmowania działań zgodnych z intencjami przestępców internetowych. Atakujący, podszywając się np. pod firmy kurierskie, urzędy administracyjne, operatorów telekomunikacyjnych, banki czy nawet znajome osoby, próbują wyłudzić poufne dane, takie jak dane do logowania do kont bankowych czy użytkowanych przez nas platform społecznościowych bądź systemów biznesowych. [1]¹

Termin „phishing” nawiązuje do łowienia ryb, co odnosi się do strategii stosowanej przez cyberprzestępców, podobnej do tej wykorzystywanej przez wędkarzy. Oszuści starają się stworzyć odpowiednio spreparowaną "przynętę", często w postaci sfalszowanych e-maili i SMS-ów. Współcześnie coraz częściej atakują również poprzez komunikatory i portale społecznościowe, np. korzystając z "metody na BLIKa".



Wiadomości phishingowe są tak opracowywane przez przestępców, aby wydawały się autentyczne, chociaż w rzeczywistości są fałszywe. Celem może być nakłonienie do ujawnienia poufnych informacji, zawarcie szkodliwego oprogramowania poprzez link do fałszywej strony internetowej (często o nazwie podobnej do autentycznej) lub dołączenie zainfekowanego załącznika.

2. Rodzaje phishingu

Obecnie wyróżnia się kilka różnych rodzajów phishingu, z których każdy ma swoje charakterystyczne cechy. W kolejnych podpunktach postaramy się je scharakteryzować i opisać, jak rozpoznawać zjawisko phishingu w zależności od jego rodzaju. Poniższe zrzuty ekranu pochodzą z https://twitter.com/CERT_Polska.

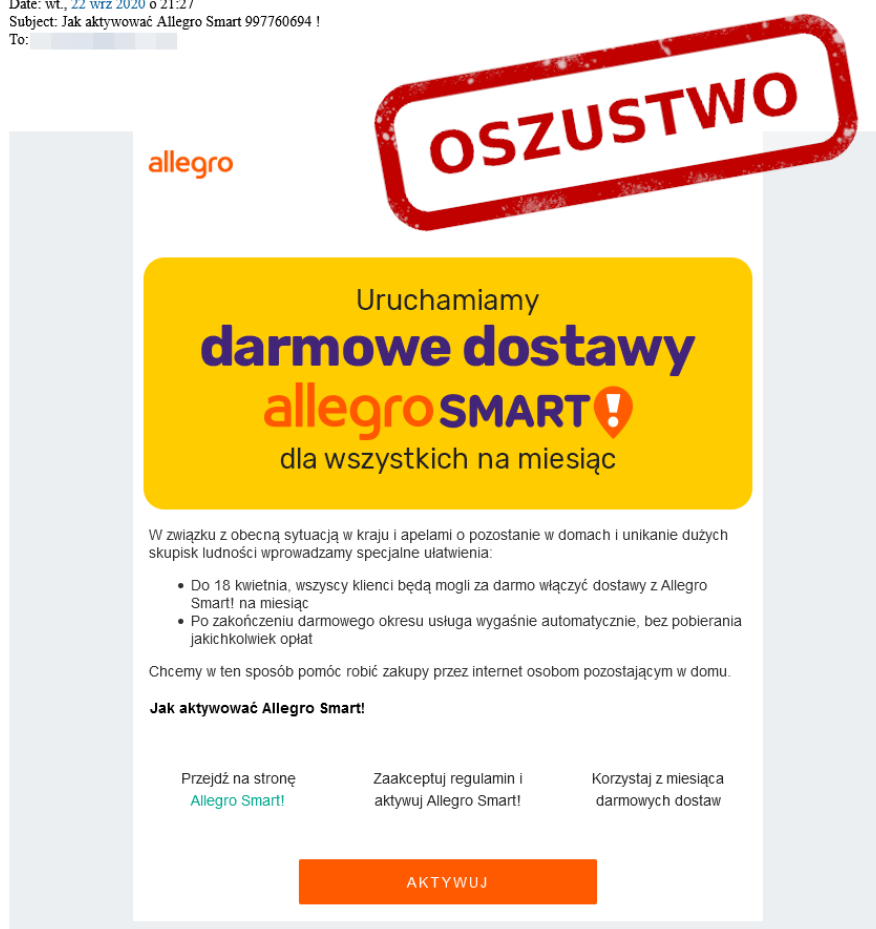
¹ <https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzanе-widomosci-e-mail-oraz-sms-y>

2.1. Phishing e-mailowy

Phishing e-mailowy to najczęstsza forma phishingu. Oszuści wysyłają fałszywe e-maile, udając inne firmy, instytucje lub osoby, aby przekonać odbiorcę do ujawnienia poufnych informacji lub kliknięcia w złośliwe linki.

Poniżej e-mail podszywający się pod Allegro – popularny portal umożliwiający handel online. Pierwsze, co powinno zaniepokoić osobę, która dostanie takiego maila to przede wszystkim fakt, że nadawcą wiadomości nie jest allegro.pl oraz podejrzana treść wiadomości. Nadawcą wiadomości w tym przypadku jest nietypowy adres onlines@frankkoch.club, który jak można się domyśleć, nie ma nic wspólnego z oficjalnym portalem allegro.

Od: Allegro <onlines@frankkoch.club>
Date: wt., 22 wrz 2020 o 21:27
Subject: Jak aktywować Allegro Smart 997760694 !
To: [redacted]



Poza tym powinniśmy uważać na wszystkie oferty, które:

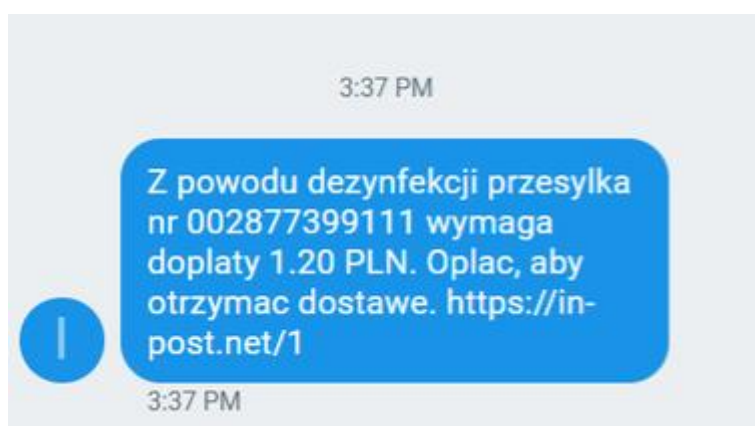
- Wydają się być “zbyt atrakcyjne”, oferujące nagrody, rozdające coś darmowego lub oferujące dostęp do czegoś tajemniczego,
- Nie są adresowane do odbiorcy z imienia i nazwiska, a zamiast tego używane są zwroty “ceniony klient” czy “przyjaciel”.
- Są napisane niepoprawnie gramatycznie lub niepoprawnie logicznie.
- Zawierają sugestie natychmiastowego działania lub inne ukryte zagrożenia.
- Zawierają podejrzane linki.

- Proszą o podanie danych osobowych.

2.2. Phishing SMS-owy

Phishing SMS-owy (SMiShing) to rodzaj ataku, gdzie podobnie jak w przypadku phishingu e-mailowego, oszuści wysyłają fałszywe wiadomości tekstowe, często informując ofiarę o rzekomych problemach z jej kontem lub prosząc o natychmiastowe działanie.

Poniżej przykład Phishingu SMS-owego:



Atakujący próbował złowić ofiary na dopłatę z powodu dezynfekcji. Finalnie jest się odsyłanym do fałszywego panelu płatności. Zaniepokoić powinny następujące spostrzeżenia: Wiadomość napisana jest bez polskich znaków, żądana jest natychmiastowa dopłata oraz podany jest podejrzany link. Oficjalny link do strony Inpostu to <https://inpost.pl/>.

2.3. Phishing telefoniczny (Vishing)

Phishing telefoniczny (Vishing) to rodzaj ataku, gdzie atakujący kontaktują się z ofiarą telefonicznie, podszywając się pod instytucje finansowe, firmy czy inne organizacje. Celem jest zdobycie informacji, takich jak numery kart kredytowych lub dane do logowania. Charakterystyczną cechą vishingu jest używanie manipulacji werbalnej, gróźb lub podstępnych technik, aby uzyskać pożądane informacje.

Aby zabezpieczyć się przed vishingiem, zawsze warto potwierdzać tożsamość osoby dzwoniącej, zwłaszcza jeśli dotyczy to kwestii finansowych. Ważne jest, aby nigdy nie udostępniać poufnych informacji w odpowiedzi na nieoczekiwane połączenia telefoniczne i być czujnym na wszelkie próby manipulacji werbalnej czy naglącego działania. Ponadto, warto korzystać z autentycznych numerów telefonów znanych instytucji, zamiast oddzwaniać na numery podane w niepewnych sytuacjach.

Szczególnie niebezpieczna jest ta metoda współcześnie, ponieważ przestępcy coraz częściej wykorzystują zaawansowane algorytmy AI do personalizacji ataków vishingowych.

Sztuczna inteligencja pozwala na dostosowanie treści wiadomości czy strony internetowej do konkretnej ofiary, co sprawia, że ataki stają się bardziej skuteczne i trudniejsze do rozpoznania. Przestępcy mogą podszywać się nawet pod przyjaciół czy członków rodziny w celu wyłudzenia informacji lub pieniędzy. Za pomocą techniki deep fake mogą oni generować także fałszywe nagrania z wykorzystaniem wizerunku podszywanych osób. Dlatego szczególnie ważne jest, aby dokładnie weryfikować tożsamość osoby dzwoniącej i zanim zdecydujemy się wykonać przelew, upewnijmy się, czy osoba, z którą rozmawiamy jest tą za którą się podaje.

2.4. Pharming

Pharming to zaawansowana forma phishingu, w której oszuści przechwytują ruch internetowy i kierują ofiary na fałszywe strony internetowe, nawet jeśli wpiszą poprawny adres URL. Głównym celem pharmingu jest uzyskanie poufnych informacji, takich jak dane logowania do kont bankowych, kont społecznościowych czy informacje kredytowe.

Charakterystyczną cechą pharmingu jest manipulacja danymi w systemie DNS (Domain Name System), który jest odpowiedzialny za przekształcanie zrozumiałych dla ludzi adresów internetowych na numery IP, używane przez komputery w celu identyfikacji serwerów sieciowych. W atakach pharmingowych, cyberprzestępcy zmieniają wpisy DNS, aby przekierować ruch użytkowników na fałszywe strony internetowe, które są kontrolowane przez atakujących.

Pharming może przybierać różne formy, a jedną z najczęstszych jest DNS spoofing, w którym atakujący fałszuje odpowiedzi DNS, przypisując fałszywe adresy IP do prawidłowych domen internetowych. Innym podejściem jest atak typu "host file poisoning," gdzie zmienia się pliki hostów na komputerze ofiary, co prowadzi do błędnej interpretacji adresów internetowych.

Ataki pharmingowe są szczególnie niebezpieczne, ponieważ ofiara często nieświadomie odwiedza fałszywe strony, które wyglądają identycznie lub bardzo podobnie do oryginalnych. W efekcie atakujący mogą przechwycić poufne dane, takie jak hasła bcy numery kart kredytowych. Aby się zabezpieczyć przed pharmingiem, zaleca się korzystanie z zabezpieczeń, takich jak firewall, oprogramowanie antywirusowe, a także regularne sprawdzanie autentyczności stron internetowych poprzez sprawdzenie certyfikatu SSL czy uważne monitorowanie adresów URL.

2.5. Spear-phishing

Spear-phishing to rodzaj phishingu jest ukierunkowany na konkretną osobę lub organizację. Atakujący dokładnie zbierają informacje o swoich ofiarach, co pozwala im dostosować wiadomości i sprawić, że wydają się bardziej autentyczne. Atakujący wykorzystują różne techniki, takie jak e-maile, SMS-y czy komunikatory, starając się podszyć pod znane osoby lub firmy, co utrudnia rozpoznanie fałszywych komunikatów.

Ze względu na wysoki poziom personalizacji i dokładnego przygotowania, spear-phishing może być trudniejszy do wykrycia niż standardowe ataki phishingowe, dlatego też wymaga podwójnej uwagi i świadomości ze strony potencjalnych ofiar. W odróżnieniu od klasycznego phishingu, spear-phishing jest znacznie bardziej efektywny. Choć wymaga większego zaangażowania ze strony oszustów, oraz niemal bezpośredniego kontaktu z ofiarą, dobrze przemyślany atak może wprowadzić w błąd nawet najbardziej świadomego użytkownika internetowego.

2.6. Clone phishing

Clone phishing: Oszuści tworzą kopie autentycznych e-maili, zmieniając jedynie pewne elementy, na przykład linki lub załączniki, aby wprowadzić ofiarę w błąd.

Aby skutecznie się bronić przed clone phishingiem, zaleca się szczegółową weryfikację adresów e-mail nadawców, unikanie klikania w podejrzane linki czy otwierania załączników, zwłaszcza gdy wiadomość wydaje się nietypowa. Warto również być świadomym ewentualnych subtelnych zmian w treści wiadomości, które mogą wskazywać na próbę oszustwa. W przypadku prośby o przekazanie poufnych informacji, zawsze warto zweryfikować ją bezpośrednio poprzez inne kanały komunikacji

2.7. Whaling

Whaling: Ten rodzaj ataku phishingowego skupia się na wysokich rangą osobach w organizacjach, takich jak dyrektorzy generalni. Oszuści starają się wyłudzić od nich kluczowe informacje czy dostęp do poufnych danych. Atak ten jest precyzyjny i wymaga dokładnego zbadania ofiary w celu stworzenia autentycznie wyglądającego przekazu, zazwyczaj poprzez podszywanie się pod osoby z najwyższego szczebla zarządzania.

Aby się chronić, należy zawsze sprawdzać tożsamość osób, zwłaszcza w przypadku nieoczekiwanych żądań informacji, nawet od wysoko postawionych pracowników. Warto także Wykorzystywać zaawansowane ustawienia bezpieczeństwa e-maili, zdolne do wykrywania i blokowania podejrzanych wiadomości związanych z whalingiem. Ważne jest również, aby Regularnie monitorować ruch sieciowy w celu wczesnego wykrywania potencjalnych zagrożeń i podejrzanych aktywności online.

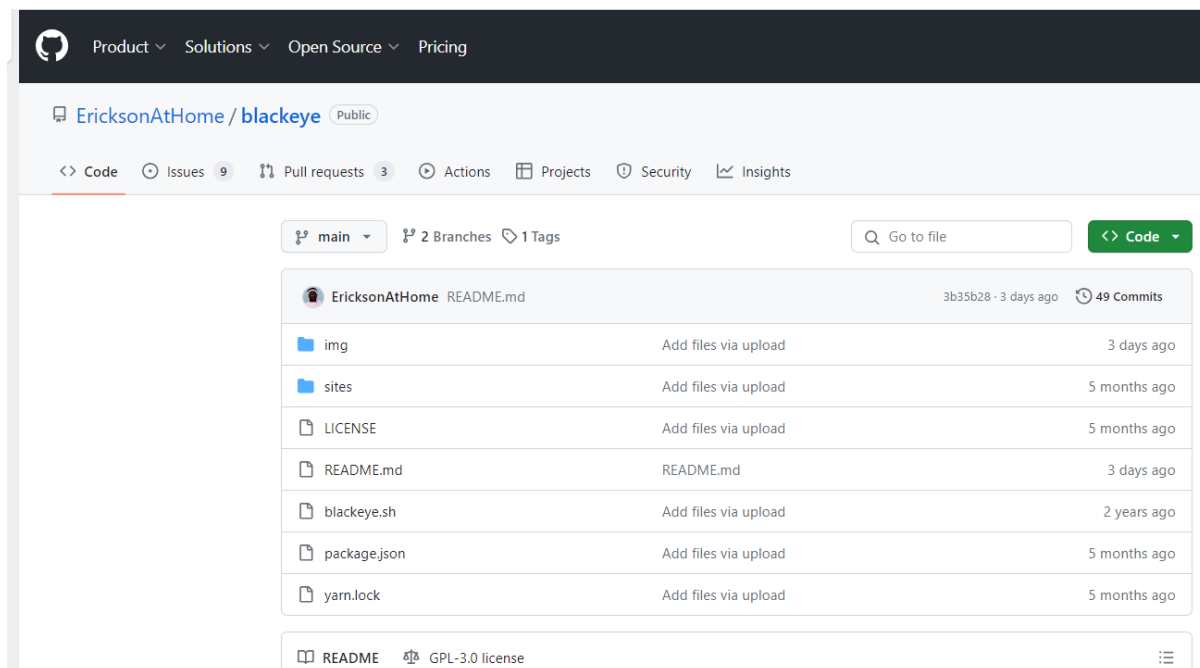
2.8. Angler phishing

Angler phishing to rodzaj ataku phishingowego, który wykorzystuje fałszywe informacje o zdarzeniach bieżących, takie jak ważne wydarzenia społeczne, katastrofy naturalne czy incydenty cybernetyczne. Oszuści wykorzystują aktualne tematy, aby skłonić ofiary do kliknięcia w złośliwe linki lub otwarcia zainfekowanych załączników.

Aby się przed nim obronić, zawsze należy weryfikować źródło informacji i sprawdzać informacje o bieżących zdarzeniach na oficjalnych stronach informacyjnych, potwierdzać wiadomości.

3.Oprogramowanie

Stworzenie strony phishingowe niestety jest znacznie szybsze i prostsze niż może nam się wydawać. Aby się o tym przekonać wejdziemy na stronę <https://github.com/EricksonAtHome/blackeye>, gdzie w celach edukacyjnych udostępniono materiały pozwalające przeprowadzić eksperyment ataku phishingowego. Wyraźnie wspomniano również, aby nie używać tych narzędzi w celu prawdziwych ataków mogących wyrządzić komuś krzywdę.



Kierując się zgodnie z instrukcją, uruchamiamy terminal i wpisując odpowiednie polecenia dochodzimy do następującego momentu, kiedy po wpisaniu komendy `bash blackeye.sh` wyskakują nam strony, które chcemy sklonować do eksperymentu. Naszym celem stanie Amazon.

```

kasia@linux:~/blackeye$ bash blackeye.sh
:: Disclaimer: Developers assume no liability and are not ::
:: responsible for any misuse or damage caused by BlackEye. ::
:: Only use for educational purposes!! ::

:: BLACKEYE By @EricksonAtHome ::

[01] Instagram      [17] DropBox          [33] eBay
[02] Facebook       [18] Line              [34] Amazon
[03] Snapchat       [19] Shopify           [35] iCloud
[04] Twitter        [20] Messenger         [36] Spotify
[05] Github         [21] GitLab            [37] Netflix
[06] Google         [22] Twitch            [38] Reddit
[07] Origin         [23] MySpace           [39] StackOverflow
[08] Yahoo          [24] Badoo             [40] Custom
[09] LinkedIn       [25] VK
[10] Protonmail     [26] Yandex
[11] Wordpress      [27] devianART
[12] Microsoft     [28] Wi-Fi
[13] IGFollowers    [29] PayPal
[14] Pinterest      [30] Steam
[15] Apple ID       [31] Tiktok

```

Zanim jednak wybierzemy numer celu ataku, rejestrujemy się na stronie ngrok, postępujemy zgodnie z instrukcją, instalujemy potrzebne pliki oraz uruchamiamy poleceniem `php -S localhost:8080` serwer.

```

kasia@linux:~/local/share/trash/files/blackeye$ php -S localhost:8080
[Wed Jan 17 15:02:50 2024] PHP 8.1.2-1ubuntu2.14 Development Server (http://localhost:8080) started
[Wed Jan 17 15:02:55 2024] 127.0.0.1:56676 Accepted
[Wed Jan 17 15:02:55 2024] 127.0.0.1:56676 [404]: GET / - No such file or directory
[Wed Jan 17 15:02:55 2024] 127.0.0.1:56676 Closing
[Wed Jan 17 15:02:55 2024] 127.0.0.1:56684 Accepted
[Wed Jan 17 15:02:55 2024] 127.0.0.1:56684 [404]: GET /favicon.ico - No such file or directory
[Wed Jan 17 15:02:55 2024] 127.0.0.1:56684 Closing

```

Wracamy do okienka z wyborem celu. Wpisujemy 34, gdyż jest to numer Amazona.


```

[ Choose an option:]-[~]
└─ ~ 34

1.Ngrok
2.Localtunnel

[ Choose the tunneling method:]-[~]
└─ ~ 1

[*] Starting php server...
[*] Starting ngrok server...
blackeye.sh: line 408: curl: command not found
[*] Send this link to the Victim:
blackeye.sh: line 412: curl: command not found
blackeye.sh: line 412: jq: command not found
blackeye.sh: line 412: xsel: command not found
blackeye.sh: line 412: xsel: command not found
[*] Use shortened link instead:

[*] Waiting victim open the link ...

[*] IP Found!
blackeye.sh: line 308: curl: command not found
blackeye.sh: line 308: jq: command not found
blackeye.sh: line 309: curl: command not found
blackeye.sh: line 309: jq: command not found
blackeye.sh: line 310: curl: command not found

```

Stworzone linki do kliknięcia:

```

[*] Send this link to the Victim: https://www-amazon-com.loca.lt
[*] Use shortened link instead: http://tinyurl.com/ya8xs7v

```

Wchodzimy w link naszego localhosta i pojawia się stworzona przez nas strona phishingowa:

```

[*] IPv6: 127.0.0.1
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0
[*] Country:
[*] Region:
[*] City:
[*] Postal:
[*] Location:
[*] Maps: https://www.google.com/maps/search/?api=1&query=,
[*] ISP:
[*] Timezone:
[*] Saved: amazon/saved.ip.txt

[*] Waiting credentials ...

```



amazon seller central

Sign in

Email (phone for mobile accounts)

Password

[Forgot your password?](#)

Sign in

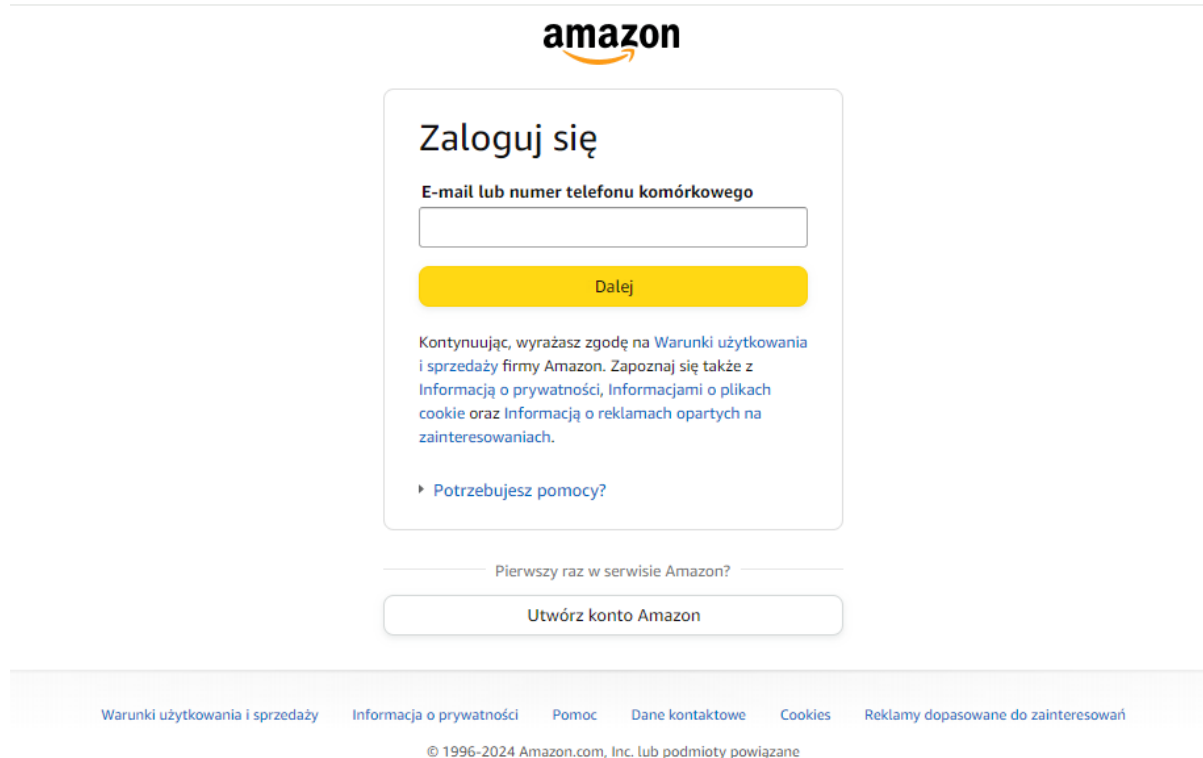
☐ Keep me signed in. [Details](#) ▼

Register now

[Help](#)

© 1996-2018, Amazon.com, Inc. or its affiliates

Dla porównania, prawdziwa strona do logowania do Amazon wygląda tak:



amazon

Zaloguj się

E-mail lub numer telefonu komórkowego

Dalej

Kontynuując, wyrażasz zgodę na [Warunki użytkowania i sprzedaży](#) firmy Amazon. Zapoznaj się także z [Informacją o prywatności](#), [Informacjami o plikach cookie](#) oraz [Informacją o reklamach opartych na zainteresowaniach](#).

► [Potrzebujesz pomocy?](#)

Pierwszy raz w serwisie Amazon?

Utwórz konto Amazon

[Warunki użytkowania i sprzedaży](#) [Informacja o prywatności](#) [Pomoc](#) [Dane kontaktowe](#) [Cookies](#) [Reklamy dopasowane do zainteresowań](#)

© 1996-2024 Amazon.com, Inc. lub podmioty powiązane

Cieężko jest zatem odróżnić patrząc po samym wyglądzie strony. Jednak jest coś czym strony znacznie się różnią, a tą rzeczą jest link. Oto link do prawdziwej strony logowania amazona:

  https://www.amazon.pl/ap/signin?openid.pape.max_auth_age=900&openid.return_to=http 

A to link strony phishingowej:

  <https://wmw-amazon-com.locat.lt>

Dlatego tak bardzo ważnym jest, by patrzeć, w jakie linki wchodzimy, czy nie wydają się nam podejrzane.

Kontynuując, wprowadzamy fikcyjne dane do logowania do naszej strony phishingowej:

localhost:8080/login.html

amazon seller central

Sign in

Email (phone for mobile accounts)

Password [Forgot your password?](#)

☐ Keep me signed in. [Details](#)

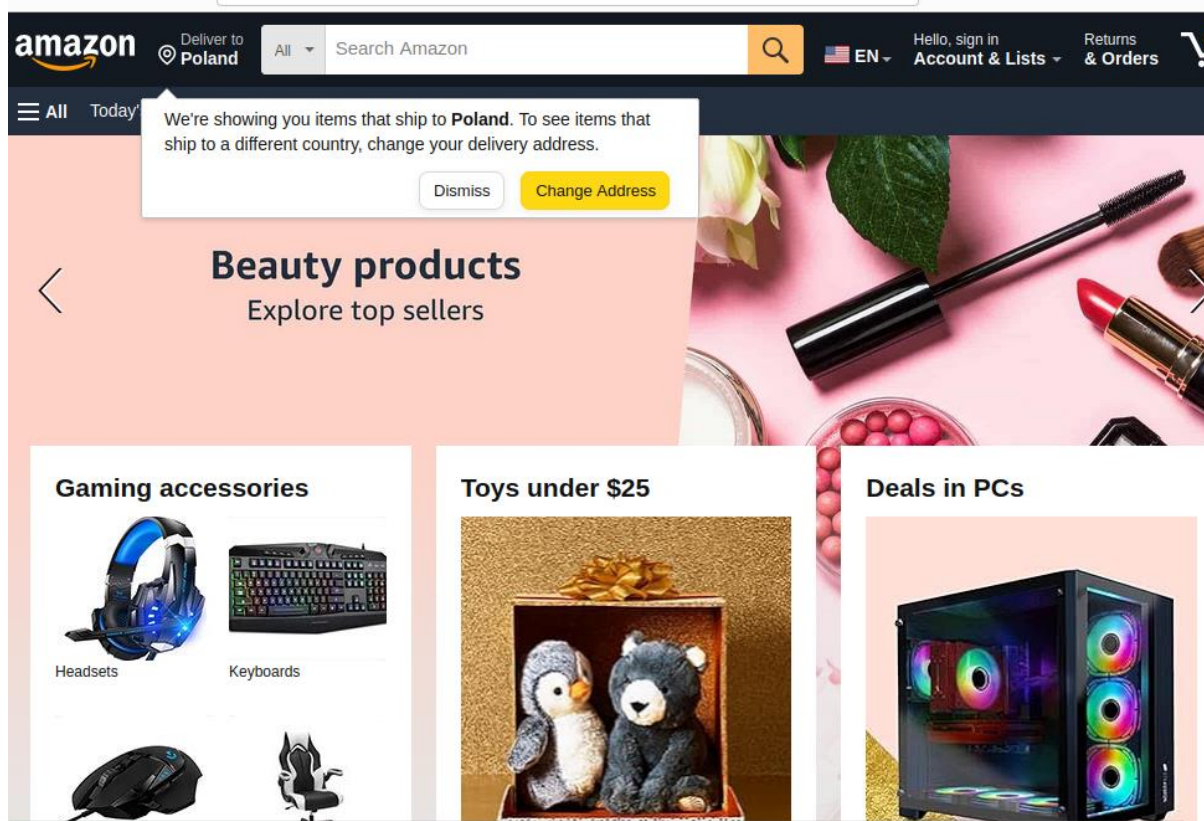
[Help](#)

© 1996-2018, Amazon.com, Inc. or its affiliates

W terminalu widzimy wpisane przez użytkownika dane oraz hasło, które mogło mu się wydawać, że wpisuje zahashowane. W taki sam sposób hakerzy zdobywają dane od użytkowników rozsyłając wirusowe linki i pobierając wpisywane przez nich loginy i hasła.

```
[*] Credentials Found!  
[*] Account: test-email@gmail.com  
[*] Password: test-haslo  
[*] Saved: sites/amazon/saved.usernames.txt  
kasia@linux:~/blackeye$
```

Użytkownik może nawet nie zauważyć że właśnie doświadczył oszustwa, gdyż po zalogowaniu się ukazuje mu się oficjalna strona Amazon. Jednak zaniepokoić powinien fakt, że pomimo logowania się, nie jest on zalogowany na stronie:



4.Podsumowanie

W świecie, w którym jesteśmy przepelnieni bodźcami i przetwarzanymi przez nas informacjami, niezwykle ważne jest, aby uważać, w jakie linki wchodzimy oraz gdzie się logujemy. Zawsze powinniśmy zachowywać czujność i weryfikować nadawców.

Niebezpieczeństwo to staje się coraz większe ze względu na przełom jaki dokonuje się przez technologię AI oraz sytuacje, kiedy nie jesteśmy w stanie odróżnić choćby głosu oszusta od głosu członka rodziny.

W przeprowadzonym w tym projekcie eksperymencie widać, że choć stworzenie fishingowej strony wymaga pewnych umiejętności obycia się w środowisku programistycznym, nie jest jednak czymś ciężko dostępnym oraz wymagającym czasowo. Po zastosowaniu odpowiednich narzędzi w kilka sekund generowane są linki do fałszywych stron wyłudzające dane.