cyber SIGHT

BEZPIECZEŃSTWO W SIECI DLA ROLNIKÓW I AGROPRZEDSIĘBIORCÓW

LEONARD WYCHOWANIEC - CZŁONEK ZESPOŁU CYBER SIGHT,
PROJEKTU W RAMACH OLIMIADY ZWOLNIENI Z TEORII

BEZPIECZEŃSTWO W SIECI DLA STUDENTÓW UNIWERSYTETU ROLINICZEGO

Czyli jak chronić swoje dane, biznes i finanse przed zagrożeniami w Internecie?

Autor tekstu: Leonard Wychowaniec - członek projektu Cyber SIGHT, wraz ze Stowarzyszeniem Liderki Innowacji
Rdakcja i korekta: Amelia Sujak, Michalina Kapała, Igor Cała
Oprawa graficzna: Michalina Kapała
Wydanie: 2025

Spis treści:

I

Wprowadzenie do tematu cyberbezpieczeństwa

Wraz z intensywnym wzrostem popularności komputerów i Internetu przez ostatnie dwadzieścia lat, utrzymywanie bezpieczeństwa swoich urządzeń oraz danych stało się niezwykle ważnym tematem. W codzie - nnym życiu coraz częściej korzystamy z Internetu w celu wyszukiwania informacji, czy promowania swoich produktów w social mediach. Poprzez sieć możemy także sprawnie aplikować i korzystać z różnych programów rządowych i unijnych. Jednak przy korzystaniu z Internetu należy uważać - znajduje się w nim wiele osób, w których interesie leży nasza krzywda.

Ogół sposobów, dzięki którym chronimy się przed atakami hakerskimi, wyciekami danych osobowych, czy wyłudzeniami, nazywamy cyberbezpieczeństwem. Jedną z metod ochrony jest ograniczanie ryzyka poprzez unikanie najczęstszych zagrożeń. Większość wyłudzeń i oszustw opiera się na nieuwadze ofiary. Przykładowo na stronach do pobierania programów należy uważać na to, który przycisk służy do faktycznego ściągania programu, gdyż często reklamy na tych stronach przypominają takowe przyciski. Tego rodzaju reklamy można ukrywać dzięki programom takim jak *Ublock origin* w przeglądarce *Firefox* lub domyślnie w przeglądarce *Brave*. Popularne także są oszustwa zwane *phishingiem*, polegające na kradzieży danych lub pieniędzy poprzez podszywanie się pod znane firmy lub witryny internetowe.

II

Silne hasła - tworzenie i ochrona

Tworzenie mocnych haseł, choć na pierwszy rzut oka wydaje się być proste, może okazać się zwodniczo trudne. Nie zagłębiając się w kryptografię: im dłuższe hasło, tym więcej czasu i prób zajmuje poprawne odgadnięcie go. Dodatkowo, korzystając z cyfr i znaków specjalnych, zwiększa się pula opcji, które muszą być poprawnie zapisane, by otrzymać hasło. Przykładowo dla 8-mio literowego hasła, korzystającego tylko z cyfr (np. 08051946) liczba kombinacji jest równa 24 310, dla hasła z literami (nie wliczając dużych cyfr) i cyframi o takiej samej długości (np. ACTH5889) jest to już 145 008 513, a dla 8-mio literowego hasła korzystającego z liter, liczb oraz znaków specjalnych (np. TMIB22!!) liczba kombinacji jest równa 1 652 411 475. Hasło o 16 znakach ze znakami specjalnymi literami i cyframi ma ich już $6{,}48 \times 1014$. Rozróżniając małe i duże litery w kombinacjach powyższe liczby rosną wielokrotnie.

Pytanie, jakie może w tej chwili nasuwać na myśl, może brzmieć: „Jak to możliwe, że silne hasła mogą być odgadnięte przez hakerów i użyte, by dostać się do moich kont?”. Otóż jest to spowodowane naszą ludzką naturą. Bardzo często po wymyśleniu jednego, silnego hasła używamy je wszędzie, gdzie jesteśmy proszeni o założenie konta. W rzadszych przypadkach tworzymy różne (teoretycznie silne) hasła na podstawie jednego schematu, by uprościć nam ich zapamiętanie, np. “imię+rok urodzenia + !” = Janina1999!.

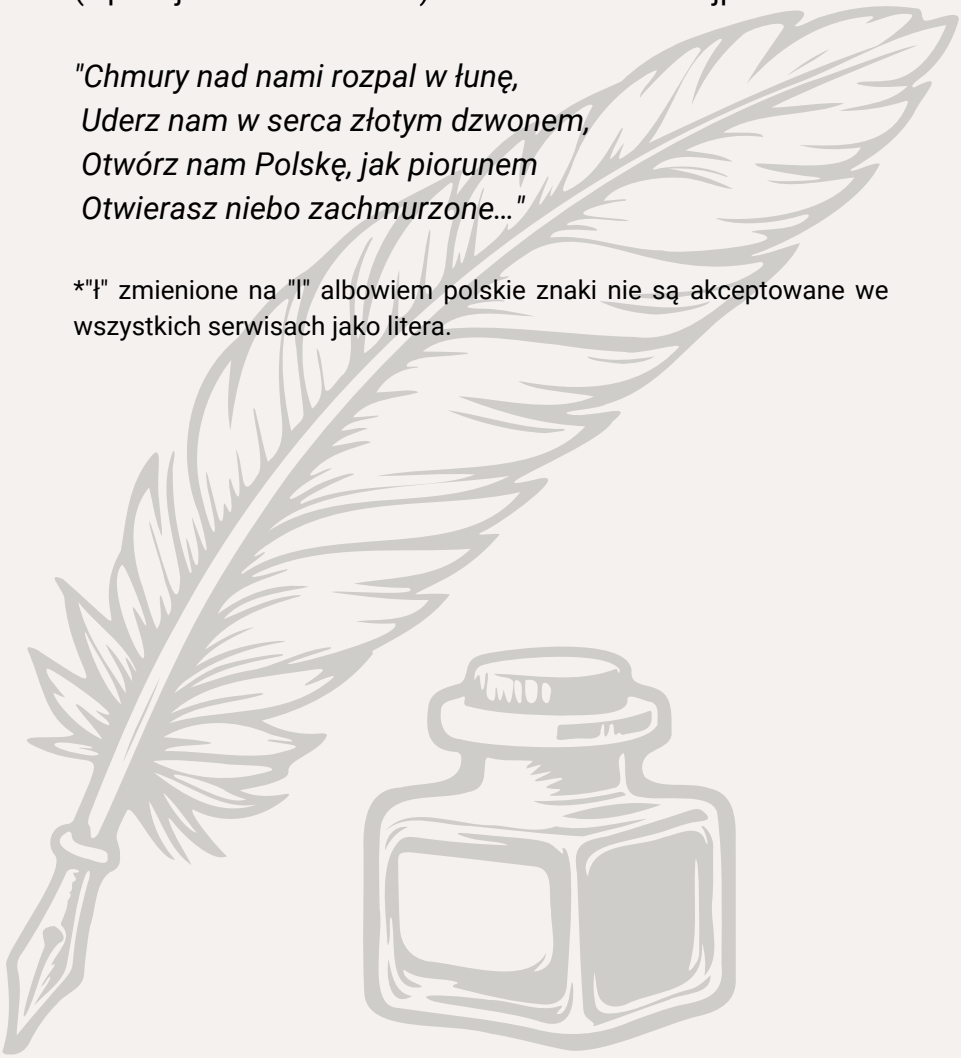
Postępowanie według powyższego schematu znacząco upraszcza hakerom zgadnięcie haseł. Działają oni na podstawie naszych danych demograficznych dostępnych na wyciągnięcie ręki w sieci lub zamieszczonych przez nas samych w social mediach. Należy także pamiętać o tym, iż używanie tych samych haseł na różnych serwisach, zwiększa ich szansę na wycieknięcie w razie złamania zabezpieczeń danego serwisu. Stanowi to następnie niebezpieczeństwo dla naszych pozostałych kont, na które mogą się zalogować osoby trzecie, korzystające z odpowiednich stron na *darknecie*. Dodatkowo trzeba być ostrożnym i patrzeć na link url strony, na której się logujemy. Często strona może wyglądać w identyczny sposób do prawdziwej, ale link może różnić się jedną literą. Na takich stronach skamerzy (oszuści; zwykle zachęcający do zakupu wątpliwej jakości produktów) lub hakerzy przechwytują dane, które my wpisujemy i używają ich do zalogowania się na nasze konto. Zmieniają maila odzyskiwania i hasła, tym samym przejmując pełny dostęp w przypadku, gdy na danym serwisie nie mamy włączonego dwuskładnikowego uwie-

rzytelniania (np. otrzymywania SMS z kodem potwierdzającym na nasz numer telefonu przy każdym logowaniu).

Częstym sposobem skutecznego tworzenia silnych haseł jest użycie jakiegoś cytatu lub wiersza poprzez zapożyczenie pierwszych liter każdego słowa, a następnie dodanie cyfr i znaków specjalnych na koniec. Przykładowo (z poezji Juliana Tuwima): CnnrwlUnwszdOnPjpOnz46!

"Chmury nad nami rozpal w łunę,
Uderz nam w serca złotym dzwonem,
Otwórz nam Polskę, jak piorunem
Otwierasz niebo zachmurzone..."

*"ł" zmienione na "l" albowiem polskie znaki nie są akceptowane we wszystkich serwisach jako litera.



Manager haseł to program/aplikacja, która może zapisywać i magazynować nasze hasła. Dzielą się na dwa typy: online i offline. Oba korzystają z tzw. *master passwords* - haseł dających dostęp do pozostałych (pamiętając, że jedno hasło odblokowuje dostęp do magazynu z naszymi pozostałymi hasłami). Bez nich traci się wszelki dostęp do pozostałych haseł, przez co zaleca się zapisanie ich w formie analogowej.

Menedżery online są prostsze w użytkowaniu i wypełnianiu, gdyż hasła są trzymane na chmurze, na serwerach firmy, z której usług się korzysta (w większości odpłatnych). Hasła w nich są synchronizowane pomiędzy wszystkimi urządzeniami z menadżerem. Pomimo posiadania dużych zabezpieczeń przez te firmy, mają one o wiele więcej osób próbujących włamać się na ich serwery. Jednymi z najlepszych jeśli chodzi o politykę prywatności i bezpieczeństwo swoich serwerów jest *Dashlane* i *Proton Pass*.

Menedżery offline są zazwyczaj bezpłatne, trzymają lokalnie hasła, ale są trudniejsze w użytkowaniu. Trzeba pobierać je z wiarygodnych stron wydawców tego oprogramowania (np. *https://keepassxc.org*) i manualnie instalować aktualizacje. Są one dostępne tylko na jednym urządzeniu, a możliwości automatycznego wypełniania też są mniejsze. Menedżery haseł są dość przydatnym narzędziem, by nie zapominać mocnych haseł, jednocześnie utrzymując ich prywatność.

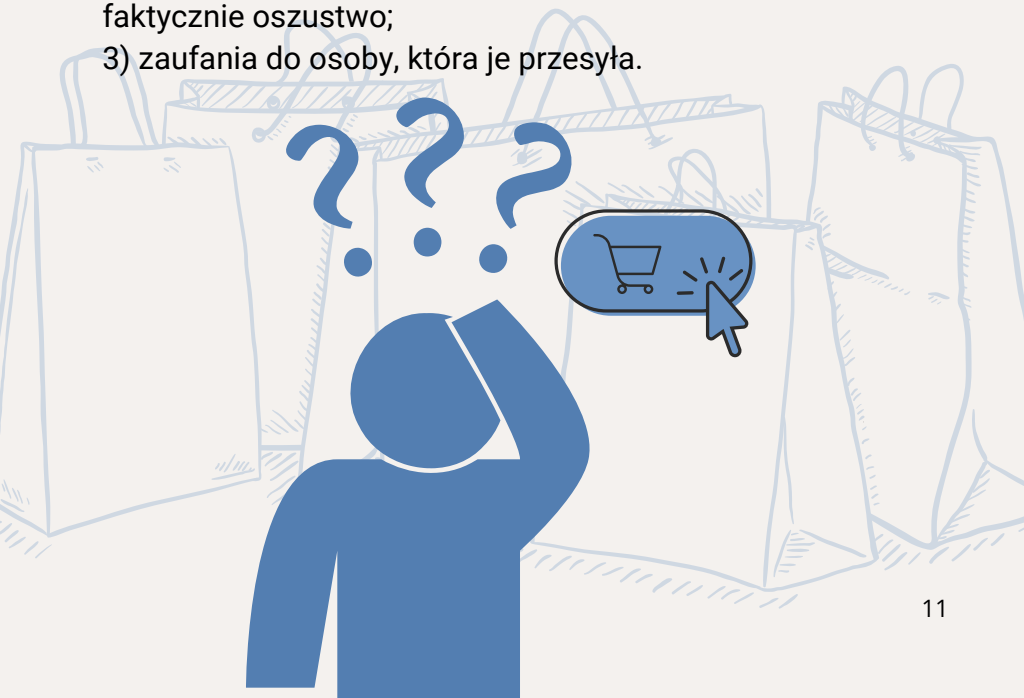
III

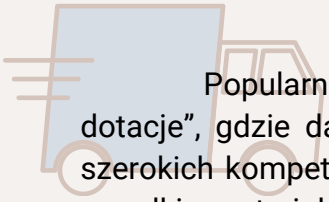
Oszustwo „na ZUS” i nie tylko, czyli jak rozpoznawać i bronić się przed mistyfikatorami

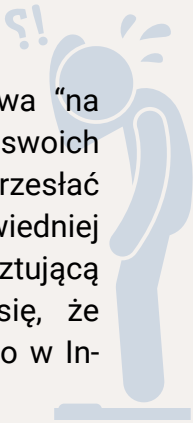
Oszustwa w Internecie można znaleźć w jego każdym, nawet najbardziej niszowym zakątku. Na platformie komunikacyjnej między graczami o nazwie *Discord* częste są oszustwa dotyczące nieprawidłowego zgłoszenia czyjegoś konta i potrzeby kontaktu z „działem obsługi klienta” na mail, który jest faktycznie używany przez oszusta lub przez link do zalogowania się na swoje konto, który kradnie dane. Tego rodzaju przekręty poprzez tekst nie dotyczą tylko graczy, lecz każdego z nas. Czasami przez złe zabezpieczenia, przez takiego rodzaju oszustwo może zostać przejęte konto społecznościowe danej osoby. Następnie wysyła ona do wszystkich osób na swojej liście znajomych, np. prośbę o przelanie pieniędzy/ wsparcie zrzutki lub kod do odblokowania, np. jego facebooka, który faktycznie jest kodempozwalającym oszuście na przejęcie konta ofiary z listy przyjaciół. Często te wiadomości mają dziwną gramatykę lub formatowanie i mają wywoływać efekt “teraz albo nigdy”. Trzeba także pamiętać, by w wypadku kliknięcia na niebezpieczny link nie podawać żadnych informacji, odłączyć się od Internetu (poprzez włączenie trybu samolotowego lub odłączenie kabla od Internetu) i sprawdzić swoje urządzenie za pomocą programu antywirusowego.

Przy zachowaniu ostrożności na oszustwa trzeba też pamiętać o przyjmowaniu zasady, iż jeśli coś jest zbyt dobre, by być prawdziwe, to takie nie jest. Często na F*acebook Marketplace*, czy *OLX* pojawiają się oferty, które nie są realne. Sprzedawca daje przedmiot o znacznie niższej cenie, np. sprzedaje używanego iphone'a, który wygląda na ofercie jak typowy, prawidłowy iphone, ale po otwarciu i włączeniu okazuje się być telefonem z systemem android, wartym niecałe kilkaset złotych w momencie, gdy zapłacono o wiele więcej. Wszelkie linki wysłane przez wiadomości powinny być uważnie sprawdzone przed kliknięciem pod względem:

1) dokładnego *kodu url* (czasem może być dodany niewidzialny znak, który się nam nie wyświetla i url wygląda tak samo, ale jest różny dla komputera);
2) sprawdzenia w internecie, czy taka sytuacja nie zdarzyła się komuś innemu, wyszukując, np. "facebook marketplace airpods scam", co pomaga w upewnieniu się, czy jest to faktycznie oszustwo;
3) zaufania do osoby, która je przesyła.







Popularne w kręgu rolniczym są oszustwa “na dotacje”, gdzie dana firma doradcza zapewnia o swoich szerokich kompetencjach i zaświadcza, że może przesłać wszelkie materiały potrzebne do znalezienia odpowiedniej dotacji dla firmy poprzez paczkę kurierską kosztującą kilkaset złotych. Po dotarciu paczki okazuje się, że dokumenty są stare, ogólne lub dostępne za darmo w Internecie, a firma doradcza nagle znika.

Aby uniknąć tego rodzaju oszustw należy ostrożnie sprawdzać kompetencje firmy doradczej, referencje innych rolników i ocenić szczególnie ich wszelkie dane firmowe (gdzie są zarejestrowani, siedzibę firmy, stronę internetową). Dodatkowo w momencie, gdy dana firma zapewnia, że na pewno uda się zdobyć dofinansowanie, które jest w formie konkursu. powinna zapalić się przysłowiowa czerwona lampka.

Oto przydatne strony w zakresie rozpoznawania tego rodzaju przekrętów i faktycznego naboru do dotacji:

1. Oficjalny Portal Funduszy Europejskich, gdzie można bezpłatnie znaleźć informacje o naborach:
https://www.funduszeeuropejskie.gov.pl/strony/skorzystaj/

2. Krajowy Rejestr Sądowy – KRS:
https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/index.html

3. Centralna Ewidencja i Informacja o Działalności Gospodarczej – CEIDG:
https://aplikacja.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Search.aspx

4. Kto do mnie dzwonił?
https://www.nieznany-numer.pl/

I wreszcie jako ostatnie bierzemy na warsztat tytułowe oszustwo “na ZUS” polegające na otrzymaniu wiadomości od oszusta podającego się za ZUS, gdzie przesyła link, aby uregulować wezwanie do zapłaty lub otrzymać świadczenie ZUS. Po kliknięciu na link pokazuje się strona podobna do ZUS-owskiej, ale z innym url-em, gdzie proszą o podanie danych osobowych i informacji z karty kredytowej/debetowej. W przypadku wprowadzenia tych informacji kradziona jest nasza tożsamość i pieniądze z karty.

ZUS wielokrotnie na swojej stronie ostrzega, iż nie wysyła linków w wiadomościach i nie posługuje się tym rodzajem korespondencji (mailowa / sms), o ile nie została ta metoda wybrana na portalu *PUE*. Należy unikać wchodzenia na wszelkie linki i załączniki w wiadomościach, które wyglądają na wysłane przez ZUS. W razie wątpliwości co do opłacenia składek powinno się bezpośrednio komunikować z oddziałem ZUS przez oficjalne kanały podawane na ich stronie pod linkiem: *https://www.zus.pl/o-zus/kontakt*.

IV

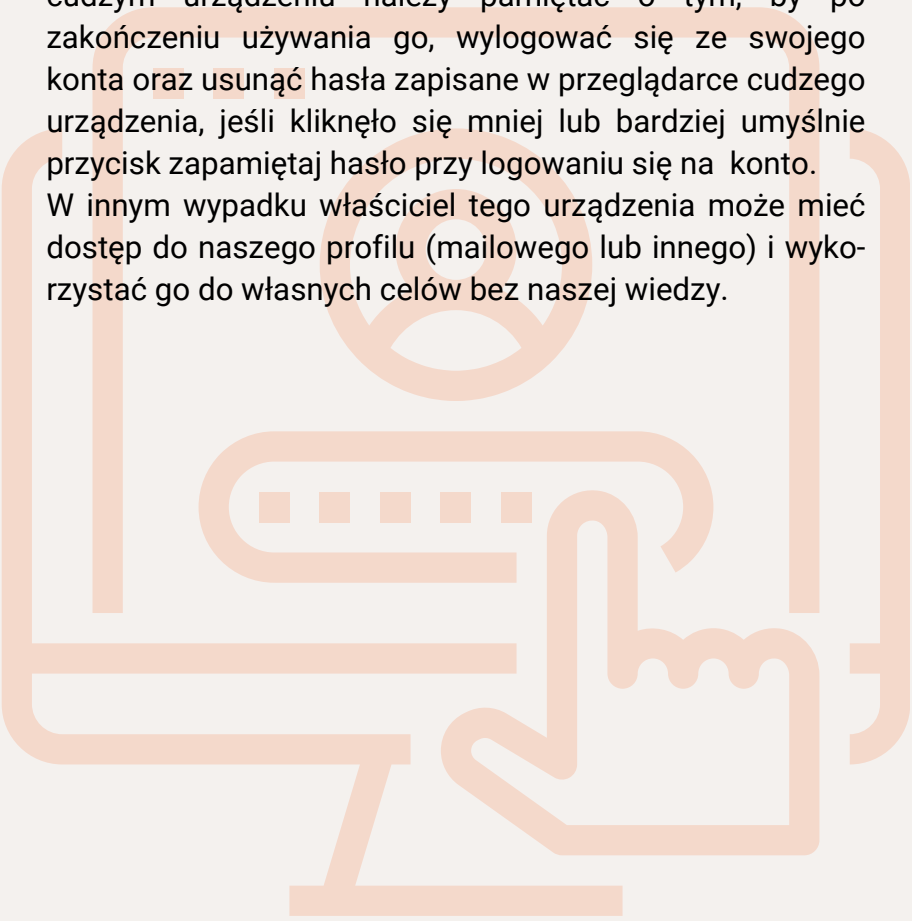
Bezpieczeństwo w mediach społecznościowych

Temat utrzymywania bezpieczeństwa w mediach społecznościowych można rozpatrzyć od dwóch stron: osobistej danego prywatnego użytkownika oraz z punktu widzenia prowadzenia działalności internetowej, gdzie promuje się na niej swoje produkty. Obie strony skupiają się na uważnym dzieleniu się danymi osobowymi, które dajemy na social media.

W przypadku osób fizycznych należy uważać na informacje dotyczące m.in. dłuższych pobytów poza domem (w wyniku których osoby trzecie mogą wiedzieć, kiedy móc się włamać), miejsca zamieszkania, historii rodzinnej, czy zdjęć członków swojej rodziny. Jednakowoż większość z tych problemów można rozwiązać ograniczając dostęp do swojego konta poprzez używanie tak zwanych *kont prywatnych*. Stąd dobrym sposobem może być utrzymywanie dwóch kont na mediach społecznościowych, w których jedno jest z bardziej wrażliwymi danymi, dostępne jedynie dla bliskich przyjaciół i rodziny, a drugie ma mniej informacji i jest dla ogólnych celów komunikowania się z nowymi ludźmi.

Od strony firm należy uważać na dane powiązane z działalnością (typu konkretne projekty, przetargi, zdjęcia osób pracujących nad projektem). Przez przypadek mogą one wyciec, upraszczając innym podszycie się pod twoją firmę i stworzenia dla niej złej reputacji poprzez różnego rodzaju oszustwa. Większość tego rodzaju poufnych informacji powinna być przekazywana jedynie wewnętrznie lub potencjalnie z osobami inwestującymi w firmę w sposób kontrolowany. W wewnętrznych komunikacjach przedsiębiorstwa raczej zalecamy używanie firmowych maili oraz aplikacji *Signal*, która jest prywatna w sposób *end-end* (jedynie nadawca i odbiorca mają klucze pozwalające na odszyfrowanie wiadomości przez ich urządzenie) i nie zapisuje na serwerach firmy danych użytkownika. W wyniku włamań lub wymagań rządu do oddania danych użytkownika nie ma ryzyka wpadnięcia tych danych w niepowołane ręce.

Jak wspomniano w poprzednich rozdziałach, jednym z najlepszych sposobów, aby uniknąć utraty kontroli nad kontem (w tym na mediach społecznościowych) jest używanie *2FA* (uwierzytelniania dwuskładnikowego). Przy włączonym 2FA, jedynie przy potwierdzeniu z telefonu lub maila (w zależności od wybranej metody autoryzacji) można zalogować się na konto. W wyniku wycieku hasła i maila konta sprawia to, że można zablokować dalsze próby logowania, zmienić hasło i uchronić się przed utratą konta. Dodatkowo w wypadku potrzeby zalogowania się na cudzym urządzeniu należy pamiętać o tym, by po zakończeniu używania go, wylogować się ze swojego konta oraz usunąć hasła zapisane w przeglądarce cudzego urządzenia, jeśli kliknęło się mniej lub bardziej umyślnie przycisk zapamiętaj hasło przy logowaniu się na konto.
W innym wypadku właściciel tego urządzenia może mieć dostęp do naszego profilu (mailowego lub innego) i wykorzystać go do własnych celów bez naszej wiedzy.



V

Transakcje i płatności - jak nie dać się oszukać?

Kupowanie rzeczy w sieci jest jednym z wygodniejszych sposobów, który pozwala na znalezienie wśród szerokiego asortymentu poszukiwanych rzeczy tej najlepszej. Trzeba jednak uważać przy wyborze strony, z której się kupuje lub przez którą się płaci. Należy dokładnie patrzeć na całość paska url, a nie tylko kłódkę i to, czy znajduje się z przodu napis https://, gdyż niektóre strony online podszywają się pod normalne, bezpieczne strony i mają minimalnie zmieniony link url. Na przykład zamiast *paypal.com* będzie *pay-pail.com*. W ten sposób oszuści mogą wyłudzić od nas informacje z karty kredytowej bez naszego zrozumienia sytuacji i wypłacić z niej pieniądze przed możliwością zastrzeżenia jej.

Profilaktycznie przed taką sytuacją powinno się chronić ustawiając:

1) autoryzację transakcji kartą poprzez sms;
2) niższy limit na karcie, a za większe zamówienia płacić przykładowo przelewem lub blikiem.

Trzeba też pamiętać o tym, że *kod cvv* karty powinno się traktować jak swój PESEL i nie podawać go w nieistotnych wiadomościach lub mailach. Przy mało znanych stronach, których pochodzenia i prawdziwości nie jesteśmy pewni, można najpierw (tak jak i z innymi linkami) sprawdzić na stronie *https://www.urlvoid.com/*, a także jak wcześniej wspomniano przy sekcji dotyczącej unikania znanych oszustw: należy kierować się zasadą, że jeśli coś jest zbyt dobre by być prawdziwe, to takie nie jest.

Większość sprzedawców można zweryfikować poprzez sprawdzenie na różnych forach internetowych, czy faktycznie sprzedają produkty, które wystawiają.

Najczęściej anglojęzycznych/zagranicznych sprzedawców można sprawdzić na stronach takich jak *Reddit,* czy są warci zaufania, szybko ich wyszukując.

VI

Praktyczne narzędzia do ochrony w Internecie

Jednym z najlepszych i bezpłatnych narzędzi pozwalających na ochronę antywirusową jest *Windows Defender,* dołączony do każdego systemu Windows. Z płatnych programów antywirusowych jednym z lepszych jest *McAfee*. Oba programy są niezawodne w ogólnym rozrachunku, jeśli chodzi o ochronę antywirusową.

Dodatkowo można uprościć ochronę przed bardziej znanymi oszustwami, spamem itp. na stronach internetowych. Warto też szybko skanować w poszukiwaniu wirusów dzięki rozszerzeniu *malware bytes browser guard*, które w połączeniu z następnymi narzędziami przyniosą nam wiele pożytku.

Blokowanie niechcianych reklam (typu sidebar i pop-up) można osiągnąć dzięki rozszerzeniu *uBlock origin* na przeglądarkach *Firefox* oraz jego modyfikacjach (Mullavad i Librewolf), a także wbudowanych blokerów reklam w przeglądarce *Brave*.

Uważamy, że pomimo tego, iż mało można zrobić z danymi, które wyciekły na *Darknet*, to jednym z najlepszych narzędzi jest strona internetowa *https://haveibeenpwned.com/*. Pozwala ona na zobaczenie, czy wybrane przez nas dane wyciekły. Prowadzona jest przez eksperta cyberbezpieczeństwa z Australii - Troy'a Hunt.

W przypadku anonimowego łączenia się z siecią, największe możliwości dla zaawansowanych użytkowników daje przeglądarka *TOR* (the onion router), pozwalająca także na korzystanie z różnych silników wyszukiwania i przeglądania stron. TOR, dzięki swojemu systemowi szyfrowania *P2P* (Peer to Peer) lub poprzez wbudowany płatny system tzw *vpn mullvad* pozwala na maskowanie adresu IP użytkownika. Adres IP pozwala na ustalenie przybliżonej lokalizacji danego urządzenia (np. naszego komputera, telefonu) na świecie mniej więcej znajduje się dany człowiek. Lepiej nie łączyć jednego narzędzia z drugim. Dzięki temu pozwalają także na oglądanie niedostępnych z powodu tak zwanych geo-restrykcji (blokady na oglądanie danych filmów w jakimś regionie świata, które są dostępne na tej samej platformie w innym miejscu) treści.

VII

PODSUMOWANIE

Cyberbezpieczeństwo jest kluczowe w dzisiejszym cyfrowym świecie, zwłaszcza przy tak intensywnym korzystaniu z internetu. Ochrona danych osobowych, unikanie oszustw, a także odpowiednie zabezpieczanie kont i transakcji są niezwykle istotne, by minimalizować ryzyko utraty danych lub pieniędzy. W e-booku omówiono różne aspekty ochrony prywatności w sieci, takie jak stosowanie silnych haseł, unikanie oszustw (np. phishingu, oszustw na ZUS), zapewnienie bezpieczeństwa w mediach społecznościowych, utrzymywanie bezpieczeństwa transakcji online oraz wykorzystywanie odpowiednich narzędzi do ochrony przed tak zwanym malware i drapieżnymi reklamami takich jak programy antywirusowe i alternatywne przeglądarki.

Lista kontrolna bezpieczeństwa w sieci

1. *Twórz silne hasła*

- Używaj haseł o długości co najmniej 8 znaków - im więcej, tym lepiej;
- Zastosuj kombinację liter, cyfr i znaków specjalnych;
- Unikaj używania tych samych haseł na różnych stronach;
- Skorzystaj z menedżerów haseł do przechowywania
- i zarządzania hasłami.

2. *Używaj uwierzytelniania dwuskładnikowego (2FA)*

- Włącz 2FA na wszystkich ważnych kontach.
- Używaj aplikacji do 2FA lub autoryzacji przez SMS.

3. *Bądź ostrożny przy klikaniu linków*

- Sprawdzaj dokładnie URL strony, zwracając uwagę na małe różnice w pisowni.
- Unikaj kliknięcia w podejrzane linki w wiadomościach e-mail i SMS.

4. *Unikaj oszustw online*

- W przypadku nieoczekiwanych wiadomości o pilnych płatnościach lub ofertach sprawdzaj wiarygodność nadawcy.
- Jeśli oferta jest zbyt dobra, by była prawdziwa, prawdopodobnie jest oszustwem.

5. *Chroń swoje dane w mediach społecznościowych*

- Ustaw konta jako prywatne, aby ograniczyć dostęp do informacji.
- Unikaj udostępniania informacji o swoim miejscu zamieszkania, planowanych podróżach i zbyt dużo szczegółów z historii życia.

6. *Zabezpiecz transakcje online*

- Używaj metod płatności, które oferują dodatkowe możliwości autoryzacji, takich jak przelewy bankowe lub Blik.
- Ustaw autoryzację transakcji kartą kredytową/ debetową przez SMS.
- Sprawdzaj strony pod kątem bezpieczeństwa przed wprowadzeniem danych karty.

7. *Używaj narzędzi do ochrony przed złośliwym oprogramowaniem*

- Zainstaluj i regularnie aktualizuj programy antywirusowe (np. Windows Defender, McAfee).
- Używaj rozszerzeń takich jak Malwarebytes Browser Guard i uBlock Origin, by blokować złośliwe oprogramowanie i reklamy.

8. *Sprawdzaj, czy twoje dane wyciekły*

- Skorzystaj z narzędzi takich jak Have I Been Pwned do sprawdzenia, czy twoje dane zostały ujawnione
- w wyniku wycieku.

9. *Zadbaj o bezpieczeństwo podczas korzystania z publicznych sieci*

- Używaj VPN, aby chronić informacje skąd łączysz się ze stroną.
- W przypadku wymagania większej anonimowości przy korzystaniu z internetu korzystaj z przeglądarki TOR.

10. *Zabezpiecz konto na każdym urządzeniu*

- Zawsze wylogowuj się z konta jeśli nie masz pewności, że ktoś może mieć dostęp do twojego odblokowanego komputera, a szczególnie na cudzych urządzeniach.
- Usuń zapisane hasła z przeglądarek po zakończeniu sesji na obcych urządzeniach.

Te zasady stanowią podstawę bezpieczeństwa w Internecie i powinny być stosowane regularnie, aby zmniejszyć ryzyko ataków hakerskich, oszustw oraz utraty danych.

Gdzie szukać pomocy, jeśli padłaś ofiarą cyberprzestępczości?

Jeśli padłaś/eś ofiarą cyberprzestępczości, ważne jest, aby jak najszybciej podjąć odpowiednie kroki, aby zminimalizować szkody i zgłosić incydent odpowiednim służbom.

Oto kilka kroków, które możesz podjąć:

1. *Zgłoś incydent odpowiednim służbom*

- Polska Policja: Zgłoś cyberprzestępstwo na najbliższym komisariacie policji lub poprzez stronę internetową Krajowej Policji lub *ePUAP*.

- CERT Polska: Zgłoś incydent do *CERT Polska*, który zajmuje się przeciwdziałaniem zagrożeniom
- w cyberprzestrzeni. Można to zrobić przez formularz na stronie.

- Urząd Ochrony Danych Osobowych (UODO): Jeśli zostały wykradzione Twoje dane osobowe, zgłoś incydent do *UODO*, który zajmuje się ochroną prywatności.

- Prokuratura: W przypadku poważnych przestępstw cybernetycznych, takich jak oszustwa finansowe, możesz zgłosić sprawę bezpośrednio do prokuratury.

2. *Zabezpiecz swoje dane*

- Zmieniaj hasła: zmień wszystkie hasła do kont, które zostały zhakowane i nie akceptuj prób zalogowania za pomocą 2FA na kontach z nim ustawionym.
- Na kontach bez niego spróbuj poprosić o zablokowanie konta przez serwis. Skontaktuj się z bankiem: jeśli oszustwo dotyczy Twoich danych bankowych, natychmiast skontaktuj się ze swoim bankiem, aby zablokować karty i zabezpieczyć konto oraz w niektórych przypadkach utraty mniejszych kwot pieniężnych odzyskać pieniądze.

3. *Zgłoś oszustwa w Internecie*

- Ostrzeż innych: jeśli spotkałeś/aś się z oszustwem w sieci, np. jakimś rodzajem phishingu lub ze stroną podszywającą się pod reputowaną, ostrzeż innych, np. poprzez media społecznościowe lub fora, aby pomóc im uniknąć tych stron i podobnych pułapek.

- Skontaktuj się z administratorem serwisu: jeśli twoje konto zostało przejęte przez cyberprzestępców, skontaktuj się z administratorem strony lub platformy, aby odzyskać dostęp lub zablokować konto, aby zmniejszyć potencjalnie wyrządzone szkody.

4. *Zgłoszenie do instytucji branżowych*

- Organizacje zajmujące się ochroną konsumentów: możesz również zgłosić dane oszustwo polegające na sprzedaniu innego produktu niż reklamowany do instytucji, które zajmują się ochroną praw konsumentów, np. do *Federacji Konsumentów* i z ich pomocą szukać rozwiązania sprawy dzięki ich ekspertom. Trzeba jednak pamiętać, że prawa konsumenckie tyczą się jedynie tego, kiedy kupujemy na nasze własne potrzebny, a nie firmowe od jakiegoś przedsiębiorcy ani od osoby prywatnej (takich jak większość sprzedawców na allegro, vinted i olx).

W przypadku zakupu od osoby fizycznej należy skontaktować się z serwisem przez który zakupiliśmy dany przedmiot.

- Instytucje zajmujące się ochroną danych: jeśli przestępstwo dotyczy Twoich danych osobowych, możesz skontaktować się z Generalnym Inspektorem Ochrony Danych Osobowych.

Warto pamiętać, że im szybciej zgłosisz przestępstwo i podejmiesz działania, tym większa szansa na odzyskanie kontroli nad swoimi danymi lub kontem, a także na zminimalizowanie potencjalnych strat.

DODATKI

📌Checklista do wydrukowania

„Jak zabezpieczyć swoje konto w 5 minut?”

- ☐ *Zmieniaj hasła do kont – używaj silnych, unikalnych haseł.*
- ☐ *Włącz uwierzytelnianie dwuskładnikowe (2FA) – dodaj dodatkową warstwę ochrony na każdym koncie.*
- ☐ *Aktualizuj oprogramowanie – upewnij się, że system i aplikacje są na bieżąco aktualizowane.*
- ☐ *Zainstaluj oprogramowanie antywirusowe – zabezpiecz swoje urządzenia przed złośliwym oprogramowaniem.*
- ☐ *Ogranicz dostęp do danych osobowych – sprawdź ustawienia prywatności w aplikacjach i na stronach internetowych.*

📌Mini słownik pojęć internetowych

Phishing – oszustwo internetowe polegające na wyłudzeniu poufnych danych, takich jak hasła i numery kart kredytowych, poprzez podszywanie się pod zaufane instytucje, strony internetowe lub przyjaciół.

Malware – Złośliwe oprogramowanie, które może uszkodzić komputer, wykraść dane lub przejąć kontrolę nad systemem. Dzieli się na różne podtypy takie jak ransomware, czy spyware, które potajemnie zbiera informacje o nas działając w tle naszego systemu

VPN (Virtual Private Network) – usługa umożliwiająca połączenie z internetem maskujące adres IP użytkownika jednym z adresów serwerów danej firmy. Kryje dzięki temu faktyczną lokalizację geograficzną użytkownika.

Ransomware – oprogramowanie, które blokuje dostęp do danych użytkownika i żąda okupu za ich odblokowanie.

Firewall (Zapora sieciowa) – system zabezpieczający komputer lub sieć przed nieautoryzowanym dostępem i zagrożeniami z sieci.

2FA (Uwierzytelnianie dwuskładnikowe) – metoda zabezpieczania konta polegająca na wymaganiu dwóch różnych form weryfikacji tożsamości użytkownika. Najpierw podania hasła, a potem weryfikacji przez kod podany w mailu, sms-ie lub aplikacji firmy.

P2P Network - sieć składająca się węzłów utrzymywanych przez użytkowników danego serwisu/przeglądarki (np. Pirate Bay lub TOR), które pozwalają na anonimizację połączenia użytkownika poprzez połączenie się przez szereg węzłów, co kryje skąd pochodzi oryginalne wyszukiwanie.

📌Lista przydatnych stron i kontaktów

CERT Polska – *https://www.cert.pl*
Pomoc w zakresie zabezpieczeń i przeciwdziałania cyberzagrożeniom.

Infolinia RODO (Generalny Inspektorat Ochrony Danych Osobowych) *– 606 050 000*
Pomoc w sprawach związanych z ochroną danych osobowych.

Polska Policja – *https://www.policja.pl*
Zgłoszenia dotyczące cyberprzestępczości i innych przestępstw.

UODO (Urząd Ochrony Danych Osobowych) – *https://uodo.gov.pl*
Pomoc w zakresie ochrony prywatności i danych osobowych.

Have I Been Pwned – *https://haveibeenpwned.com*
Narzędzie do sprawdzania, czy Twoje dane znalazły się w wyciekach.

https://support.torproject.org/faq/ - w tym miejscu można znaleźć odpowiedzi na częste pytania powiązane z przeglądarką TOR

https://www.reddit.com/ - serwis zawiera głównie anglojęzyczne fora (tak zwane subreddity) o różnorodnej tematyce, gdzie można znaleźć odpowiedź na większość prostych i też bardziej ezoterycznych pytań dotyczących cyberbezpieczeństwa na np. r/cybersecurity

https://www.gov.pl/web/arimr - rządowa strona pozwalająca na składanie wniosków o dofinansowanie i zawierająca informacje przydatne dla rolników i agroprzedsiębiorców.

Te dodatki mogą pomóc w szybkim zabezpieczeniu Twoich danych oraz w znalezieniu wsparcia w przypadku cyberzagrożeń.