CYBER
RESCUE

CyberBezpieczny Senior

CYBER RESCUE

SPIS TREŚCI

NOTKA OD NAS 1

Drogi Czytelniku!

Tym razem proponujemy Ci Poradnik, który tworzyliśmy przede wszystkim z myślą o nieustraszonych, odrobinkę starszych użytkownikach sieci.

W środku znajdziesz solidną dawkę wiedzy o popularnych oszustwach, sposobach na ich rozpoznanie i dodatkową garść naszych porad, jak nie dać się Cyberłobuzom w przepastnych odmętach Internetu.

To lektura obowiązkowa nie tylko dla CyberBezpiecznego Seniora, ale także dla każdego, kto chciałby lepiej zrozumieć mechanizmy przekrętów online! W kolejnych Rozdziałach w prosty sposób tłumaczymy dla Ciebie najważniejsze kwestie cyberbezpiecznych praktyk.

Niezależnie od wieku, śmiało zabieraj się za czytanie, żeby zwiększyć swoją świadomość lub ugruntować posiadaną już wiedzę!

Do Dzieła!

CYBER RESCUE

WSTĘP 2

Śmiali Seniorzy z roku na rok spędzają w sieci coraz więcej czasu. Według danych z ZUS z tego roku, ponad 80% Emerytów otrzymuje comiesięczne świadczenia na konto, a nawet 65% ma dostęp do bankowości online! Osoby z grupy 60+ lubią też sprawdzać w Internecie najnowsze informacje (63%), komunikować się z bliskimi przy wykorzystaniu mediów społecznościowych lub maila (nawet 62%), a przeszło połowa* jest Klientami sklepów online.

Statystyki robią ogromne wrażenie, jednak nie można zapominać, że - mimo wielu walorów - Internet jest też wyjątkowo intratną przestrzenią działania dla przestępców!

Jesteś aktywnym użytkownikiem sieci? Pewnie zastanawiasz się co zatem robić, żeby nie paść ofiarą wszędobylskich oszustów. Spokojna głowa! Mamy dla Ciebie sporo użytecznych sztuczek i tricków jak nie dać się nabrać, ale przede wszystkim chcemy Ci podpowiedzieć jak możesz się realnie zabezpieczyć podczas swoich wojaży online!

*Za: kobietybiznesu.pl; Raport Seniorzy w świecie cyfrowym 2023

CYBER RESCUE

BEZPIECZNE HASŁA 3

... I WSZYSTKO CO MUSISZ O NICH WIEDZIEĆ!

Mocne hasło to podstawa odpowiedniego zabezpieczenia kont i aplikacji, z których korzystasz. Bankowość internetowa, poczta, sklepy online czy Twój profil w mediach społecznościowych – wszędzie musisz zadbać o to, by używać unikatowych i silnych haseł. Już tłumaczymy co to właściwie znaczy.

Jak stworzyć bezpieczne hasło?

Naprawdę dobre i mocne hasło jest przede wszystkim zupełnie... niepowtarzalne! Warto, żeby technicznie w treści hasła pojawiały się: duże i małe litery, cyfry i znaki specjalne - łącznie minimum 12 znaków!

TRIK WART UWAGI

- Hasło nie musi być ciągiem nic nie znaczących znaków lub jednym wyrazem! Fajnym sposobem na jego stworzenie jest użycie ulubionego cytatu albo fragmentu piosenki.
- Pamiętaj, że tekst musi być pisany bez przerw - zamiast nich możesz użyć np. znaków interpunkcyjnych.
- Niektóre znaki specjalne mogą zastąpić litery, np. zamiast a użyj @ lub wymień s na $
- Na przykład: Jeste$mynawcz@sach,wtychgoralskichlasach!1972

CYBER RESCUE

Czego unikać?

Pamiętaj, żeby nie tworzyć prostych ani oczywistych haseł, jak: data urodzenia, imię dziecka/wnuka/zwierzątka, 1234, etc. Bardzo łatwo je złamać, więc nie stanowią właściwie żadnego zabezpieczenia konta.

Koniecznie używaj różnych haseł w różnych miejscach: osobnego do bankowości, Facebooka, poczty elektronicznej i każdej strony, na jakiej posiadasz konto! Dzięki temu, jeśli jedno z Twoich haseł wycieknie, szkoda zostanie w jednym miejscu.

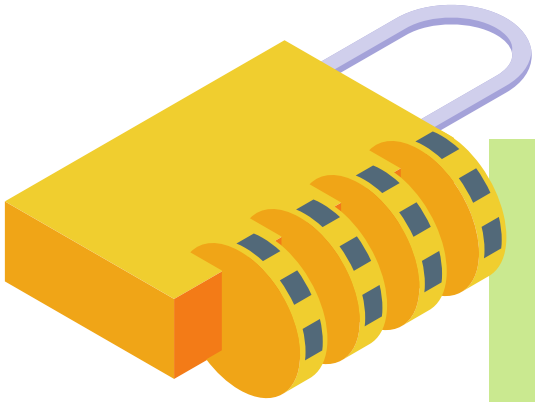
Nie zapisuj swoich haseł w niestrzeżonych miejscach, szczególnie na karteczce, przyklejonej do biurka czy w notatniku, do którego każdy może zajrzeć. Nie klikaj też ok, jeśli Twoja przeglądarka Internetowa zapyta Czy zapisać to hasło?, szczególnie jeśli używasz urządzenia, do którego mają dostęp inne osoby.

No dobrze, to jak mam zapamiętać te wszystkie różne, długaśne hasła do różnych miejsc i się nie pomylić?

CYBER RESCUE

Menadżer haseł

Z odsieczą może przyjść specjalny program, który bezpiecznie przechowa wszystkie Twoje hasła! Możesz go używać zarówno w telefonie (aplikację znajdziesz w sklepie Play dla telefonów z systemem Android lub w App Store dla iPhone'ów), jak i na komputerze!



ZAUFANE PROGRAMY, KTÓRE POLECAMY:

BITWARDEN I KEEPASS

JAK TO DZIAŁA?

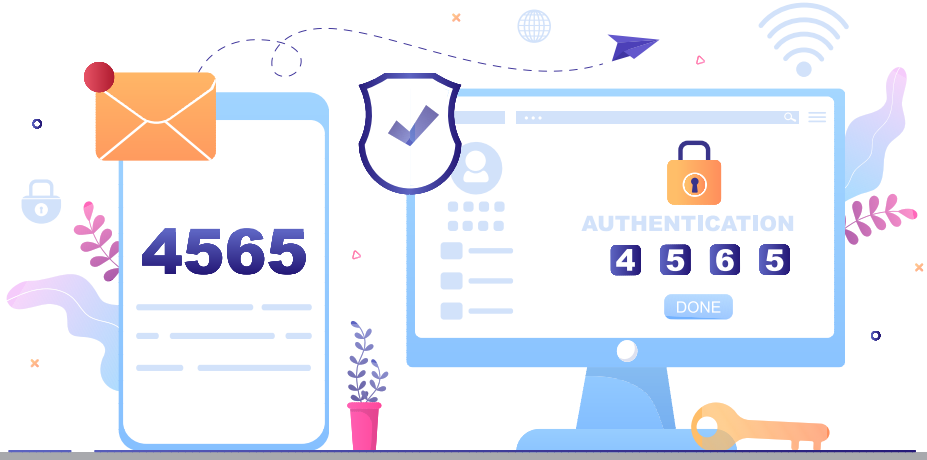
Twój Menadżer będzie sejfem, w którym zapiszesz hasło do każdej witryny i aplikacji. Program szyfruje dane, jakie w nim przechowujesz. Dodatkowo posiada opcję generowania naprawdę trudnych do złamania haseł, które możesz wykorzystać na swoich kontach i profilach. A teraz najlepsze! Wystarczy, że zapamiętasz jedno, jedyne hasło główne - to, którym będziesz logować się do Menadżera. Dobrze już wiesz jak je stworzyć, prawda? Wszystkie niezbędne wskazówki możesz w każdej chwili sprawdzić, wracając do strony 4.

CYBER RESCUE

WERYFIKACJA DWUETAPOWA 4

Co to takiego?

To dwustopniowa metoda logowania, w której, oprócz podania loginu i hasła (pierwszy etap), musisz je dodatkowo potwierdzić, np. kodem przesłanym w SMSie, mailu lub w aplikacji do autoryzowania (drugi etap).



Dwuetapowa weryfikacja logowania, zwana też uwierzytelnianiem dwuskładnikowym, w świecie online jest niczym dwa zamki w drzwiach Twojego domu! Jeśli pierwszy zawiedzie, nadal chroni Cię drugi.

Praktycznie wszystkie najpopularniejsze serwisy internetowe posiadają opcję włączenia dwuetapowej weryfikacji, jednak nie każdy o tym wie! Możesz ją uruchomić na Facebooku, Instagramie, Allegro, Google, a nawet w swoim programie pocztowym. Dzięki temu, nawet jeśli ktoś wykradnie Twoje hasło i spróbuje zalogować się na Twoje konto, nie będzie w stanie potwierdzić tożsamości w drugim etapie. Takie powiadomienie trafi tylko do Ciebie, wybranym kanałem.

CYBER RESCUE

WŁĄCZANIE W POPULARNYCH SERWISACH:

Najczęściej opcję włączenia Dwuetapowej weryfikacji logowania znajdziesz w ustawieniach swojego Konta, w sekcji Bezpieczeństwo lub Zabezpieczenia - niezależnie od portalu czy poczty, z jakich korzystasz.

- W prawnym, górnym rogu kliknij ikonkę ze swoim foto
- Dalej wybierz Ustawienia i Prywatność i Ustawienia
- Następnie Hasło i zabezpieczenia
- Uwierzytelnianie dwuskładnikowe i voilà!
- Dalej postępuj zgodnie z instrukcjami FB

- W prawnym, górnym rogu kliknij ikonkę ze swoim foto
- Następnie Zarządaj kontem Google
- Dalej wybierz zakładkę Bezpieczeństwo
- Potem Weryfikacja dwuetapowa i Włącz

- Zaloguj się do swojego konta
- W prawym, górnym rogu kliknij na swoje imię
- Wybierz Konto, dalej Moje Konto
- Zjedź do sekcji Bezpieczeństwo i wybierz Dwustopniowe logowanie
- Tutaj wybierasz rodzaj drugiego etapu zabezpieczenia: kod, otrzymany SMSem czy kod z aplikacji Google Authenticator. Po wyborze metoda staje się aktywna.

CYBER RESCUE

ANTYWIRUS 5

Buszując regularnie w sieci, a szczególnie korzystając z bankowości online, warto dodatkowo zabezpieczyć swoje urządzenia, korzystając z programów antywirusowych. Ich zadaniem jest wykrywanie, blokowanie i usuwanie złośliwego oprogramowania. Możesz skorzystać z darmowych programów lub ich bardziej rozbudowanych, płatnych wersji - w zależności od swojego poziomu sieciowego zaawansowania.

Czym grozi wirus na moim urządzeniu?

Zawirusowane programy możesz pobrać na swój komputer, tablet czy telefon zupełnie nieświadomie. Wystarczy wejść w link, który dostaniesz od nieznajomego, otworzyć podejrzany mail lub niechcący kliknąć na nachalnie wyskakujące na jakiejś stronie okienko. Złośliwe programy mają różne cele, jednak najczęściej wykradają wrażliwe dane (np. kart płatniczych lub logowania do konta bankowego). Mogą też trwale uszkodzić system, a nawet zaszyfrować Twoje pliki, co wykorzysta cyberprzestępca, próbując wyłudzić od Ciebie okup za ich odblokowanie!

Dlatego, jeśli tylko możesz - używaj antywirusa. Taki program skutecznie ochroni Cię przed sieciowymi zagrożeniami!

Jeśli posiadasz program antywirusowy, pamiętaj, żeby na bieżąco go aktualizować.

To bardzo ważne, żeby baza wirusów, jaką zawiera, była jak najświeższa. Nie ignoruj komunikatów i alertów, jakie wysyła antywirus, zawsze uważnie je czytaj i stosuj się do podanych zaleceń.

CYBER RESCUE

GDY PISZE NIEZNAJOMY...

6

Zaglądasz na Messenger, WhatsApp albo pocztę i widzisz nową wiadomość od nieznanego wcześniej nadawcy? A może pod jednym z Twoich postów w mediach społecznościowych pojawił się komentarz, np. z komplementem od obcej osoby?

Zachowaj ostrożność!

NAWET JEŚLI WIADOMOŚĆ JEST SUPERPOZYTYWNA, WSKAZANA JEST CZUJNOŚĆ. NIESTETY W WIRTUALNYM ŚWIECIE PRZEWIJA SIĘ WYJĄTKOWO WIELE OSÓB, KTÓRE NIE MAJĄ DOBRYCH ZAMIARÓW. OSZUŚCI BARDZO CZĘSTO KORZYSTAJĄ Z TECHNIK MANIPULACYJNYCH. BĘDĄ PRÓBOWALI WZBUDZIĆ TWOJĄ CIEKAWOŚĆ, TROSKĘ, A NAWET OBURZENIE - BYLE TYLKO NAKŁONIĆ CIĘ DO NAWIĄZANIA KONTAKTU.

A po co tyle zachodu?

Najczęściej żeby wyłudzić od Ciebie kasę! Mogą zachęcać do lewych inwestycji (zwłaszcza w kryptowaluty), błagać o pomoc, pozując na ciężko chorych lub podszywać się pod żołnierzy, a nawet celebrytów, udających, że potrzebują Twojej pomocy w transferze pieniędzy zza granicy.

CYBER RESCUE

Parę przykładów:

1 **Dostajesz maila od Pracownika nieznanej Ci firmy. W treści info o korekcie faktury za prąd/gaz/wodę. W wiadomości jest załącznik, w który klikasz, żeby sprawdzić o co chodzi...**

W pliku nie ma żadnej faktury, to wirus! Możesz poważnie zainfekować urządzenie, np. programem, który będzie wykradał Twoje prywatne dane.

Nigdy nie otwieraj załączników z nieznanych źródeł. W swojej skrzynce mailowej oznaczaj je kategorią SPAM, następnie usuwaj. Zapamiętaj: nieznany nadawca = niebezpieczeństwo!

2 **Dzwoni do Ciebie nieznany numer. Osoba po drugiej stronie słuchawki podaje się za pracownika Banku. Wierzysz, bo zna Twoje imię i nazwisko. Dzwoniący prosi o dane Twojej karty...**

To przestępca. Podając dane karty, wręczasz mu dostęp do swoich pieniędzy. Jeśli dasz się namówić na instalację programu, oszust będzie mógł śledzić wszystko, co robisz na swoim urządzeniu.

Pamiętaj, że Pracownik Banku nigdy nie poprosi Cię o podanie danych logowania lub karty. Nie będzie też nakłaniał do instalacji żadnych programów. Natychmiast się rozłącz! Jeśli nie masz pewności czy rzeczywiście dzwoni Pracownik danej firmy, przerwij rozmowę, potem zadzwoń na oficjalną infolinię, by potwierdzić wcześniejsze połączenie.

3

Nowo poznana osoba potrzebuje Twojej pomocy w przeniesieniu pieniędzy za granicę. W nagrodę oferuje procent od transakcji. Zanim dojdzie do transferu, prosi o podanie Twoich danych i opłacenie niewielkich kosztów (np. podatkowych lub administracyjnych).

Celem oszusta jest zdobycie dostępu do Twojej kasy. Może prosić o dane osobowe, karty, logowania do Banku lub kod BLIK. Kiedy je udostępnisz - znika bez śladu.

Nigdy nie reaguj na wiadomości (maile, SMSy czy na komunikatorach), w których obcy obiecuje Ci gratyfikację finansową. Odbiorcę zawsze blokuj i zgłaszaj do portalu.

4

Przychodzi do Ciebie SMS z informacją, że wygrywasz świetną nagrodę. Żeby ją odebrać, wystarczy opłacić drobne koszty przesyłki. Transakcję musisz wykonać na podanej przez organizatora stronie, uzupełniając swoje dane.

To sposób na wyłudzenie dostępu do Twojego konta i pieniędzy. Strona, jaką wysyła przestępca, jest podrobiona i zapisuje wszystko, co na niej podasz.

Żeby nie stracić oszczędności i dostępu do konta, nigdy nie ufaj SMSom od nieznanych nadawców, szczególnie jeśli zawierają link oraz obiecują nagrody i proszą o pokrycie jakichkolwiek kosztów.

5 W oko wpada Ci post na portalu społecznościowym, w którym znana i zaufana osoba (np. polityk, celebryta) zachęca do wyjątkowo intratnej inwestycji.

Wszystkie tego typu reklamy są fałszywe i nielegalnie wykorzystują wizerunek znanych osób. Celem jest nabranie czytelników i przejęcie ich pieniędzy.

W żadnym przypadku nie ufaj ofertom, które obiecują szybki i duży zarobek. Takie cuda niestety nie istnieją. Nawet gdy znana twarz zapewnia, że to pewny zysk.

6 Dostajesz maila od Interpolu/Policji/FBI lub innych służb. Nadawca informuje, że jesteś osobą poszukiwaną w prowadzonym śledztwie, dotyczącym np. pedofilii. Proponuje układ: żeby wyciszyć sprawę, musisz wpłacić kaucję.

Cyberłobuz, próbując wpędzić Cię w panikę, chce wyłudzić Twoje wrażliwe dane i/lub pieniądze. Jeśli przekażesz mu jakiekolwiek środki, nie będzie możliwości ich odzyskania.

Maile zastraszające i szantażujące w ten sposób mają wywołać u Ciebie strach, przez który się ugniesz i wpłacisz kasę. Tego typu wiadomości nigdy nie są prawdziwe. Oznaczaj je w skrzynce jako SPAM i usuwaj.

CYBER RESCUE

SIECI WIFI 7

Sieć WiFi to technologia, pozwalająca na bezprzewodowe połączenie się Twoich urządzeń z Internetem, za pomocą wysyłanego przez router sygnału. Router to urządzenie, które pewnie znasz ze swojego domu: mała skrzynka z antenkami. To właśnie dzięki niemu możesz korzystać na swoim komputerze czy telefonie z Internetu, bez użycia kabla.

Jeśli zdarza Ci się korzystać z WiFi kiedy jesteś poza domem, np. w restauracji, pociągu lub autobusie, bibliotece, kawiarni, centrum handlowym, a nawet u znajomych - zachowaj szczególną ostrożność. Musisz założyć, że kiedy to nie Ty jesteś właścicielem takiego połączenia, nigdy nie wiesz jak dobrze jest zabezpieczone.

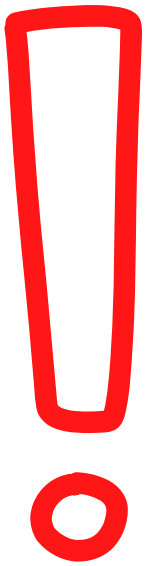
Najbardziej niebezpieczne są tzw. sieci publiczne, czyli te ogólnodostępne dla wszystkich. Kiedy je użytkujesz, nigdy nie odwiedzaj stron ani aplikacji, zawierających jakiekolwiek wrażliwe informacje, np. www Twojego Banku lub stron rządowych, na których znajdują się Twoje szczegółowe dane osobowe. Staraj się też wtedy powstrzymać od płatności Internetowych, logowania do konta pocztowego i mediów społecznościowych.

Właściwie dlaczego?

Niestety publiczne sieci zazwyczaj nie są zbyt dobrze zabezpieczone i posiadają wiele podatności na ewentualne ataki CyberPrzestępców. Hakerzy często mają chrapkę, by się do nich włamywać, bo ogólnodostępne WiFi to dla nich łatwy cel!

Cyberłobuzy potrafią swobodnie panoszyć się w sieci, z której korzystasz w miejscach publicznych. Zdarza się, że je forsują, żeby np. manipulować danymi i informacjami, jakie pojawiają się na urządzeniach nieświadomych użytkowników, podrzucać na nie programy szpiegujące lub przejmujące kontrolę nad telefonami czy komputerami. Stąd już tylko rzut beretem do wykradania haseł, loginów i poufnych informacji!

Ostrożność na wagę złota!



Przestępcy mogą Tworzyć własne klony publicznych WiFi i podszywać się pod market, hotel czy inne miejsce, w którym akurat jesteś. Haker z łatwością kradnie informacje, na jakich mu zależy, a Ty nie masz nawet świadomości takiego zdarzenia.

Nawet jeśli łączysz się z siecią, dostępną w placówce publicznej, cieszącej się społecznym zaufaniem, np. w urzędzie, banku czy muzeum, nigdy nie masz gwarancji jej bezpieczeństwa! Pamiętaj, że każdy - tak samo jak Ty - ma do niej dostęp!

CYBER RESCUE

AKTUALIZACJE... 8

...TWOJEGO OPROGRAMOWANIA

Zdarzyło Ci się podczas korzystania z komputera lub telefonu nagle zobaczyć wyskakujące powiadomienie, krzyczące Najnowsza aktualizacja oprogramowania jest już dostępna? Okropnie denerwujące, prawda? A zdarzyło Ci się takie powiadomienie zamknąć bez czytania i wrócić do przerwanych zajęć, zapominając o sprawie?

NIE BĘDZIEMY OWIJAĆ W BAWEŁNĘ. TO NAPRAWDĘ NIEBEZPIECZNE!

Czemu aktualizowanie jest tak istotne?

Wbrew pozorom z bardzo prostej przyczyny. Aktualizacje to poprawki, które przygotowują twórcy systemów, programów i aplikacji. Posiadanie ich najnowszej wersji jest nie tylko klawe, ale przede wszystkim bardzo rozsądne.

Instalując aktualizacje, pozbywasz się ze swoich urządzeń wszystkich wykrytych wad, luk i podatności. Dzięki temu posiadasz bieżącą ochronę przed potencjalnymi niebezpieczeństwami. Producenci często podkreślają, że nie wspierają starszych wersji oprogramowania, niż najnowsza. To dlatego, że mogą generować zagrożenie, np. wycieku Twoich danych!

Dlatego... aktualizuj ile wlezie!

Bardzo prosta zasada: jeśli chcesz być z cyberbezpieczeństwem za pan brat, nigdy nie ignoruj powiadomień o aktualizacjach! Staraj się nie odkładać ich na później - zazwyczaj nie trwają dłużej niż kilka minut. Wystarczy, że przeczytasz komunikat i wyrazisz zgodę na ich instalację na urządzeniu. Po chwili możesz cieszyć się nie tylko bezpieczniejszym, ale i sprawniej działającym telefonem, tabletem czy komputerem!

AKTUALIZACJA...

Trik wart uwagi

Jeśli wiadomość o aktualizacji pojawia się w niedogodnym momencie, bo np. akurat nie ma Cię w domu - nic straconego!

Twoje urządzenie bardzo często pozwoli Ci wybrać czas, w którym zainstaluje aktualizację.

Wystarczy uważnie przeczytać komunikat i postępować zgodnie z wytycznymi, ustawiając konkretny dzień i godzinę instalacji.

Pamiętaj tylko, że im szybciej, tym lepiej!

CYBER RESCUE

KOPIA ZAPASOWA 9

Ale po co?

Najpierw nieco teorii o tym dobrym zwyczaju. Kopia zapasowa nazwą tłumaczy samą siebie. To kopiowanie zawartości Twojego dysku, czyli tak naprawdę całej biblioteki danych, plików i materiałów, jakie trzymasz na swoim urządzeniu. Pewnie zastanawiasz się po co, gdzie i dla kogo ta kopia?

Oczywiście dla Ciebie! Na wszelki wypadek. Możliwe, że to truizm, ale i tak go napiszemy: Twoje urządzenia nie są nieśmiertelne! Komputery, tablety i telefony - dokładnie tak samo jak żelazka, suszarki czy odkurzacze - także się psują, a w końcu dokonują swego żywota. Właśnie na taką okoliczność się zabezpieczasz, robiąc regularnie kopię zapasową swoich danych. Jeśli sprzęt nagle odmówi posłuszeństwa albo - o zgrozo! - zgubisz go, czy zostanie podle przez kogoś przejęty lub zablokowany, Ty nie tracisz bezpowrotnie przepastnych galerii zdjęciowych, żadnych filmików ze wspomnieniami, ani innych materiałów, które na nim trzymasz.

Swoje dane możesz skopiować i przechowywać na innym urządzeniu, na zewnętrznym dysku pamięci lub nawet w tzw. chmurze, czyli na dysku wirtualnym. Ta ostatnia opcja jest szczególnie wygodna, bo nie wymaga żadnego dodatkowego fizycznego nośnika. Wirtualny dysk jest dla Ciebie dostępny np. u dostawców takich jak Google lub Microsoft - do pewnej wielkości zupełnie za darmo! Wystarczy założyć konto online u jednego z tych usługodawców.

CYBER RESCUE

INTERNETOWE SKLEPY

10

Kupować czy nie kupować - oto jest pytanie!

Z jednej strony - zakupy online są wyjątkowo wygodne. Często Internetowe sklepy proponują lepsze niż stacjonarnie ceny, a i wybór asortymentu jest zdecydowanie bardziej rozbudowany. Z drugiej strony, sieć aż huczy od historii oszukanych przez e-sklepy, którzy zamawiając coś świetnego w prawdziwie okazyjnej cenie, nigdy nie doczekali się przesyłki albo dostali towar, który niczym nie przypominał tego ze zdjęcia. Jak tu być mądrym?

Wszystko dla ludzi... tylko rozsądnych

Jak w wielu aspektach życia i na szosach, także tutaj sprawdzi się zasada ograniczonego zaufania. Szkoda byłoby nie korzystać z przepastnych propozycji zakupowych online, jednak należy do takich ofert podchodzić przede wszystkim ostrożnie.

Na co zwracać uwagę podczas zakupów?

Sprawdzaj Regulaminy!

Teoretycznie to przecież... oczywiste, a jednak praktycznie - mało kto to robi! Zanim dodasz produkty do swojego wirtualnego koszyka, poszukaj na stronie Regulaminu. To w nim muszą być zawarte podstawowe informacje o samym sprzedawcy, ale również bardzo istotne fakty, dotyczące zakupów, przede wszystkim:

- Jaki koszt i czas wysyłki deklaruje sprzedawca
- Skąd jest wysyłany towar (unikaj sklepów z dostawą ze Wschodu, np. z Chin - to najczęściej fałszywki albo rzeczy o wątpliwej jakości!)
- Jak długo trwa realizacja zamówienia
- Jakie są zasady odstąpienia, reklamacji i zwrotu

Jeśli na stronie sklepu brak Regulaminu, cóż... uciekaj gdzie pieprz rośnie!

Sprawdź dane sprzedawcy

Znajdziesz je na początku Regulaminu. Upewnij się, np. korzystając z dedykowanych wyszukiwarek na stronach rządowych (CEIDG, KRS), że właściciel sklepu rzeczywiście istnieje! Wiele fałszywych stron nie podaje tych danych w ogóle lub je zmyśla - w takim przypadku na pewno nie rób zakupów.

CYBER RESCUE

Zerknij na dane kontaktowe

Wiarygodny sklep zawsze udostępnia na swojej stronie w widocznym miejscu sposoby i formy kontaktu. Upewnij się, że wybrana witryna klarownie wskazuje swój fizyczny adres, numer telefonu i maila, na którego można wysyłać zapytania, związane z zakupami.

Jeśli sklep nie podaje takich informacji, a jedyna forma kontaktu to formularz na stronie albo wiadomość mailowa, firma prawdopodobnie próbuje coś ukryć i nie chce być przez Ciebie namierzona.

Zweryfikuj opinie

Wystarczy, że wpiszesz w wyszukiwarkę, np. Google, nazwę sklepu. Zobaczysz wtedy opinie innych Klientów. Dobrze sprawdzać je na zaufanych stronach, np. Opineo, Ceneo lub Trustpilot. Jeśli okaże się, że inni kupujący nie są zadowoleni ze swoich zakupów, a sklep ma niską ocenę - nie warto ryzykować.

Wrażenia innych nabywców możesz sprawdzić też w mediach społecznościowych sklepu. Jeśli np. na Facebooku nie widzisz żadnych opinii ani komentarzy - to też konkretny znak, że firma nie chce udostępniać ocen swoich Klientów. Najczęściej dlatego, że są wyjątkowo kiepskie. Uważaj też, jeśli zauważysz, że kilka opinii ma taką samą treść, a zostały wystawione w krótkim po sobie czasie - mogą być nieprawdziwe i np. kupione przez sklep!

CYBER RESCUE

Jej wysokość... karta płatnicza

Jeśli każdy z poprzednich punktów skończy się pozytywną konkluzją, a Ty zdecydujesz się na zakupy w tak sprawdzonym sklepie - i tak warto dmuchać na zimne. Wybierając sposób płatności, zawsze decyduj się na swoją kartę płatniczą. To obecnie najbezpieczniejsza forma finalizowania transakcji finansowych online.

Jeśli z zakupami coś pójdzie nie tak, np. nie dostaniesz towaru albo okaże się kiepską podróbką, a kontakt ze sklepem się urwie - jeszcze nie wszystko stracone. Wybierając płatność kartą, masz możliwość złożenia w swoim Banku tzw. reklamacji chargeback. To procedura, która pozwoli Ci odzyskać kasę, nawet kiedy nie będziesz w stanie dogadać się ze sprzedawcą.

Jeśli chcesz bardziej wnikliwie zgłębić tajniki analizy internetowych przybytków - koniecznie zajrzyj na naszego bloga:

https://.pl.cyberrescue.me/jak-weryfikowac-sklepy-internetowe-e-book-do-pobrania-za-darmo

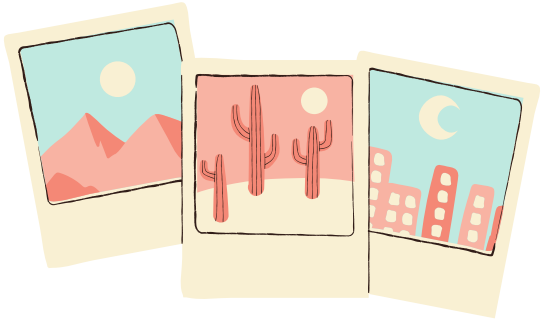
Znajdziesz tam całego e-booka, poświęconego tej kwestii! Dowiesz się z niego m.in. jak rozpoznać fałszywy e-sklep oraz jak nie dać się złapać w pułapki, zastawiane przez Cyberłobuzów.

MEDIA SPOŁECZNOŚCIOWE 11

Na co szczególnie uważać, kiedy korzystam z social mediów?

Informacje o Tobie

Pamiętaj, że Twój profil w portalu to nie pamiętnik! Ograniczaj informacje, jakie o sobie udostępniasz. Nigdy nie podawaj na swoim koncie miejsca zamieszkania, pracy, członków rodziny ani nawet info dokąd wybierasz się na wakacje. To może być sygnał dla przestępców, którzy połączą fakty i np. obrabują Twój dom pod Twoją nieobecność.



Fałszywe profile

Wpadło Ci zaproszenie do znajomych od obcego? Ostrożnie! Oczywiście od Ciebie zależy czy je przyjmiesz, jednak pamiętaj, że nigdy nie wiesz kto naprawdę siedzi po drugiej stronie komputera. CyberPrzestępcy szczególnie często zakładają nieprawdziwe konta, próbując nawiązać jak najwięcej znajomości. Po zyskaniu Twojego zaufania, mogą próbować Cię oszukać i wyłudzić od Ciebie pieniądze.

CYBER RESCUE

Ustawienia prywatności

Koniecznie dostosuj je do swoich wymagań. Na Facebooku możesz dokładnie określić kto widzi Twoje publikacje, komentarze i reakcje, np. wszyscy bez wyjątku, tylko Twoi znajomi lub wyłącznie bliscy znajomi. Dzięki temu możesz kontrolować jaka grupa osób ma dostęp do Twoich informacji, co jest szczególnie ważne. Pamiętaj: w Internecie nic nie ginie! Raz dodane zdjęcie, nawet później usunięte, mogło już zostać udostępnione lub skopiowane. Musisz liczyć się z tą myślą każdorazowo, gdy tylko coś publikujesz.

Sprawdź jak je dostosować na Facebooku:

- Po zalogowaniu się do swojego konta, kliknij ikonkę ze swoim zdjęciem - znajdziesz ją w prawym górnym rogu.
- Wybierz opcję Ustawienia i prywatność, dalej Kontrola prywatności.
- Masz do wyboru kilka kategorii: Kto może zobaczyć to, co udostępniasz, Jak inni mogą Cię wyszukać na FB i Ustawienia Twoich danych na FB.
- Zajrzyj w każdy kafelek. Obok wszystkich informacji, jakie podajesz, będzie opcja wybrania jaka grupa osób zobaczy udostępnione dane.

CYBER RESCUE

Fake newsy

W sieci wpadł Ci w oko sensacyjny nagłówek? Aż prosi się, żeby go kliknąć i przeczytać! Ostrożnie. Pamiętaj, żeby nie ufać każdej informacji znalezionej w Internetowych odmętach. Większość takich skandalizujących artukułów to tzw. fake newsy (z angielskiego fałszywe wiadomości), tworzone i udostępnianie tylko dla zdobycia wielu odsłon lub nawet żeby Cię na coś naciągnąć.

Pro Porada

Zawsze stosuj Zasadę 3 Potwierdzeń: spróbuj wyszukać kontrowersyjną informację w innych źródłach. Jeśli znajdziesz ją w trzech niezależnych, wiarygodnych i zaufanych portalach - może faktycznie coś w tym jest!

CYBER RESCUE

BEZPIECZNY BANK 12

Konto online bez tajemnic

Korzystanie z bankowości internetowej jest naprawdę wygodne. Nie musisz marnować czasu, zastanawiając się w placówce za czym stoi ta kolejka, możesz opłacić wszystkie rachunki i zrobić zakupy bez wychodzenia z domu, a nawet wziąć kredyt lub pożyczkę albo rozłożyć płatność na wygodne raty - a to wszystko sprzed swojego komputera!

Nie możesz jednak zapominać o podstawowych zabezpieczeniach! To czy Twoja kasa jest bezpieczna, zależy też przecież od Ciebie!

Bezpieczne logowanie

Bank solidnie zabezpiecza Twoje konto, dając Ci wybór najnowocześniejszych rozwiązań. Warto z nich korzystać. Jednym z nich jest oczywiście dodatkowe zabezpieczenie logowania, w postaci jego dwuetapowej weryfikacji. Jeśli wcześniej włączenie tej funkcjonalności nie wydawało Ci się niezbędne, mamy nadzieję, że po tej lekturze zmienisz zdanie! Pamiętaj też o ustawieniu naprawdę silnego hasła do bankowej aplikacji - jeśli potrzebujesz przypomnieć sobie, z czego powinno się składać, możesz zawsze wrócić do Rozdziału 3. i wykorzystać zdobytą wiedzę w praktyce!

Jeśli chcesz zapłacić za coś online, pamiętaj, żeby wystrzegać się linków do rzekomej płatności, jakie możesz dostawać od potencjalnych sprzedawców i sklepów. Żeby pozostać ultrabezpiecznym, wchodząc na stronę internetową swojego Banku, każdorazowo dokładnie sprawdzaj czy jej adres jest poprawny i nie zawiera żadnych literówek, dziwnych, dodatkowych znaków czy cyfr. O podrobione witryny dziś nie trudno. Taki nawyk pozwoli Ci ustrzec się przed potencjalnymi oszustami.

Telefon od Pracownika Banku

Wyjątkowo popularny jest teraz przekręt, w którym oszuści podszywają się pod Pracowników Twojego Banku. Wstępnie w rozmowie mogą zrobić porządne wrażenie, bo np. będą znali Twoje nazwisko. Jednak nie daj się podejść.

Jeśli rzekomy Pracownik Banku prosi Cię przez telefon o podanie: loginu i hasła do konta, kodu uwierzytelniającego logowanie, kodu BLIK, numeru karty płatniczej albo namawia Cię do instalacji nieznanego oprogramowania na Twoim urządzeniu - natychmiast się rozłącz! To przestępca! Próbuje dostać się do Twojej kasy, a nawet podrzucić Ci aplikację szpiegującą, żeby wykraść Twoje dostępy.

Zapamiętaj, że prawdziwy Konsultant nigdy nie poprosi Cię o podanie takich danych!

Zgubiony telefon z apką banku

Jeśli spotka Cię ta przykra sytuacja, że bezpowrotnie stracisz swoje urządzenie, na którym zdarzało Ci się korzystać z aplikacji bankowej, nie zwlekaj! Od razu zadzwoń na oficjalną infolinię Banku i daj znać co się stało. Urządzenia mobilne, na których korzystasz z bankowości, zapamiętują się na Twoim koncie jako sprzęty zaufane. W przypadku ich zgubienia lub kradzieży - na stronie Banku można takie telefony i komputery w prosty sposób odpiąć od swojego profilu. Konsultant Banku na pewno pomoże w weryfikacji i realizacji tego punktu.

Jak zadbać o kartę płatniczą?

Jak wyjaśnialiśmy w Rozdziale o zakupach, płatności kartą są w tej chwili najbezpieczniejsze. Jednak sama forma transakcji, umożliwiająca ewentualne odzyskanie środków, nie jest przecież gwarantem, że dane Twojej karty albo sam plastik nie dostaną się w niepowołane ręce.

Szczególnie zwracaj uwagę, by nie podawać danych Twojej karty na nieznanych Ci stronach internetowych. W sieci roi się od konkursów i ofert, w których organizator prosi o udostępnienie tych informacji. Bardzo często podstępem oszuści podpinają wtedy pod Twoją kartę tzw. płatną subskrypcję, która będzie regularnie pobierać środki z Twojego konta. Jeśli podasz numer, datę ważności i kod swojej karty, niestety może zostać wykorzystana przez przestępców do nieautoryzowanej płatności.

Ustalanie limitów

Niezależnie od Banku, na każdej karcie płatniczej możesz ustalić tzw. limity płatności, m.in. na transakcje bezgotówkowe - czyli np. właśnie te, realizowane online. To bardzo fajna i sprytna metoda dodatkowego zabezpieczenia. Jeśli na swojej karcie ustawisz dzienny limit z konkretną kwotą, jaka może być wydana na tego typu płatności - nawet jeśli zgubisz kartę albo jej dane wpadną w czyjeś ręce - nie stracisz wszystkich oszczędności.

Pamiętaj, że jeśli jednak dojdzie do udostępnienia danych karty osobom trzecim lub jej kradzieży - niezwłocznie skontaktuj się ze swoim bankiem! Na takiej karcie należy jak najszybciej wyzerować limity i ją zastrzec, żeby przestępcy nie mogli dostać się do kasy na Twoim koncie! W załatwieniu tych spraw pomoże konsultant bankowy, kiedy zadzwonisz na oficjalną infolinię.

PODZIĘKOWANIE 13

Drogi Czytelniku, a właściwie już CyberBezpieczny Omnibusie!

Ufamy, że spora dawka wiedzy została w Twojej głowie po tej lekturze. Mamy też nadzieję, że udało się nam w przystępny sposób wyjaśnić zarówno te bardziej oczywiste, jak i nieco trudniejsze zagadnienia, które mogą dotyczyć bezpośrednio Twojej sieciowej egzystencji!

Masz ochotę poznać więcej szczegółów z CyberŚwiata? Koniecznie zaglądaj na naszego bloga (https://cyberrescue.info), gdzie regularnie publikujemy pomocne materiały. Znajdziesz tam m.in. nasze pozostałe e-booki: Jak weryfikować sklepy internetowe? i Poradnik CyberBezpieczny Dzieciak., a także aktualizowaną na bieżąco listę podejrzanych sklepów internetowych!

Masz pytania lub potrzebę doprecyzowania? Odezwij się do nas na Messengerze (facebook.com/cyberrescue.me).

Dziękujemy Ci za poświęcony nam czas!

Team CyberRescue