SYSBIT.IT

5 SPOSOBÓW NA TWOJE BEZPIECZEŃSTWO W SIECI

https://sysbit.it

CZEŚĆ!

Jest mi bardzo miło, że poświęcasz chwilę swojego dnia, aby przeczytać ten dokument. Starałem się, aby informacje w nim zawarte były zrozumiałe dla osób, które nie są biegłe w obsłudze komputera.

Tematem tego dokumentu jest Twoje bezpieczeństwo w sieci. Niestety, od rozpoczęcia pandemii ilość ataków hakerskich, dotyczących przejęcia danych znacznie wzrosła. Jednocześnie ich wykrywalność utrzymuje się na niskim poziomie.

Cyberbezpieczeństwo nie musi być drogie i skomplikowane. Wystarczy przestrzegać kilku zasad, a ryzyko, że ktoś znajdzie się w posiadaniu Twoich danych znacząco spadnie. Dlatego zapraszam Cię do przeczytania poniższego tekstu. Jeżeli coś jest dla Ciebie niejasne, lub chcesz się dowiedzieć jak coś wykonać technicznie, nie krępuj się i napisz do mnie.

Z przyjemnością Ci pomogę.

Wszystkiego dobrego,
Zespół SYSBIT

SYSBIT.IT

1) UWIERZYTELNIANIE DWUSKŁADNIKOWE

Wszystkie Twoje konta na social mediach czy na skrzynkach e-mail powinny mieć włączone logowanie się za pomocą dodatkowego składnika. Dlaczego? Ponieważ zapewni to podwójne zabezpieczenie Twoich danych.

Uwierzytelnianie dwuskładnikowe (2FA) zapewnia dodatkową ochronę w trakcie logowania. Podczas uzyskiwania dostępu przeprowadzasz dodatkową weryfikację tożsamości poprzez np. skanowanie odcisku palca, wprowadzenie kodu trzymanego w wiadomości SMS, wpisanie jednorazowego kodu z aplikacji, czy użycie specjalnego klucza sprzętowego.

Daje Ci to dodatkową ochronę na wypadek wycieku Twojego hasła. Cyberprzestępca, nawet jeżeli będzie znał Twoje hasło, podczas próby dostępu do Twojego konta, będzie musiał wprowadzić dodatkowy kod, w zależności od metody uwierzytelnienia, jaka została przez Ciebie wybrana.

Uzyskanie dodatkowego kodu nie jest niestety niemożliwe, ale za to jest dosyć trudne do zdobycia technicznie, dzięki czemu zdecydowana większość hakerów odpuści, a Twoje dane pozostaną bezpieczne.

Czym prędzej włącz dwuskładnikowe uwierzytelnienie (2FA) wszędzie, gdzie jest to tylko możliwe! I najlepiej zrób to teraz!

SYSBIT.IT

2) SILNE HASŁA

Konta w serwisach internetowych, oprogramowanie na komputerze, sieci Wifi wymagają od Ciebie ustawienia hasła. Dlatego tak ważne jest, aby to hasło było bezpieczne. Silne hasło jest kluczowym elementem Twojego bezpieczeństwa w sieci. Jest ono także najczęściej pierwszą linią ochrony przed atakami hakerów.

Co znaczy „bezpieczne i silne" hasło?

Silne hasło to takie, które:
▶ po pierwsze, nie da się go łatwo złamać,
▶ po drugie nie da się go łatwo odgadnąć.

Dzisiejsze możliwości sprzętowe pozwalają w ciągu kilku minut na złamanie dowolnego hasła o długości 8 znaków. A dzięki informacjom, jakie wrzucasz na swoje social media, potencjalny atakujący może stworzyć bogatą listę haseł związanych bezpośrednio z Tobą!

O co dokładnie chodzi? Jakie informacje, które publikujesz pomagają hakerom?

Zastanów się:
▶ czy w Twoich hasłach do banku, kont w social mediach lub do poczty elektronicznej nie ma informacji na temat Twoich dzieci (np. imię, zdrobnienie, nick), informacji na temat Twojego ulubionego zwierzaka, ulubionego artysty, klubu piłkarskiego, zespołu muzycznego, itp.,
▶ czy Twój PIN do karty nie zawiera daty Twoich urodzin, urodzin Twoich bliskich lub jakieś jego wariacji?

Pomyśl, ile tego typu informacji zawierają hasła do Twoich kont w social mediach?

SYSBIT.IT

JAK WIĘC WYMYŚLIĆ SILNE, BEZPIECZNE I ŁATWE DO ZAPAMIĘTANIA HASŁO?

Twórz długie frazy z tego, co lubisz i znasz. Może to być fragment jakieś ulubionej książki, albo czynność, którą lubisz robić. Może to być cokolwiek, co jest dla Ciebie ważne. Będzie Ci to łatwiej zapamiętać. Nie musisz wymyślać skomplikowanych haseł złożonych z liter, cyfr i znaków specjalnych, których zapamiętanie sprawi Ci trudność.

Przykład: Jeżeli jesteś wielkim fanem, np. zespołu Metallica, Twoim hasłem może być fraza: **MetallicaSkonczylaSieNaKillEmAll1983%**. Można takie hasło jeszcze bardziej zmodyfikować, aby było trudniejsze do odgadnięcia (aktualnie nie da się złamać takiego hasła w rozsądnym czasie): literę E zamienić na 3, zamiast o wpisać 0 (zero), zamiast l wpisać !. Tak zmodyfikowane hasło może brzmieć: **M3ta!!icaSk0nczy!aSi3NaKi!!3mA!!.**

SYSBIT.IT

3) ZARZĄDZANIE HASŁAMI

W dzisiejszych czasach mamy mnóstwo różnego rodzaju kont, gdzie musimy ustawić sobie jakieś hasło. Jeżeli stworzysz sobie bezpieczne hasło, zgodnie ze wskazówkami zawartymi powyżej, to czy możesz go używać wszędzie? Absolutnie NIE!

Podstawową zasadą bezpieczeństwa jest nieużywanie tych samych haseł w różnych serwisach. No dobrze, a czy to znaczy, że musisz za każdym razem wymyślać nowe, długie i trudne do odgadnięcia hasło? Na szczęście nie. Tu z pomocą przychodzi menadżer haseł.

Menadżer haseł to oprogramowanie, które przechowuje w bezpieczny sposób Twoje hasła. Wystarczy, że stworzysz jedno, silne i bezpieczne hasło za pomocą którego zalogujesz się do menadżera haseł. Wtedy możesz z łatwością skopiować dowolne hasło i użyć go w celu zalogowania się do jakiegoś serwisu.

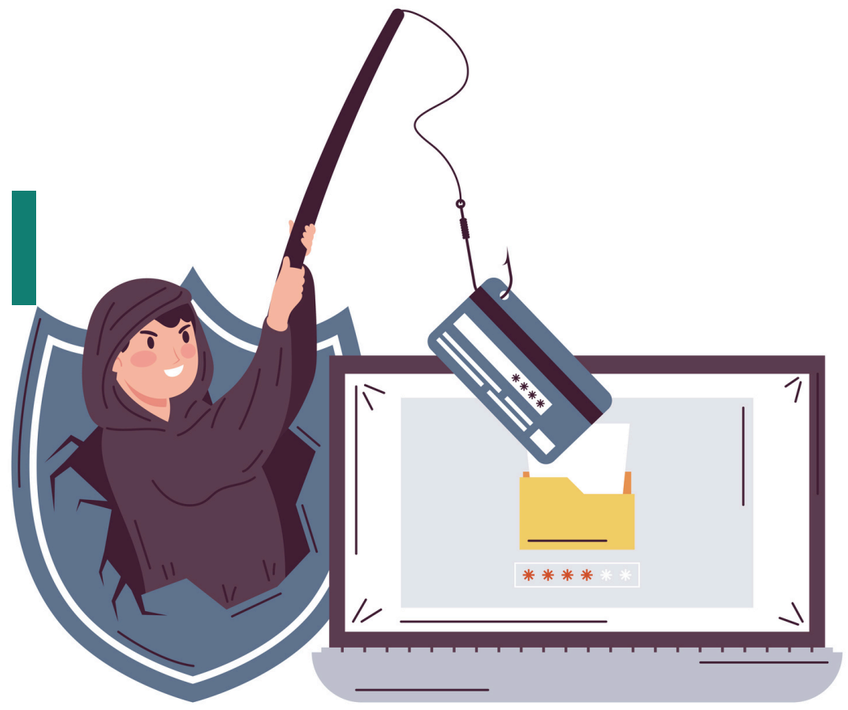
Tak naprawdę wystarczy, że stworzysz i zapamiętasz 4 różne hasła:
- ▶ hasło do komputera
- ▶ hasło do banku
- ▶ hasło do menadżera haseł
- ▶ hasło do głównej poczty elektronicznej.

Cała reszta haseł powinna być trzymana w menadżerze haseł lub w samej przeglądarce. Chyba, że konto w danym serwisie nie jest szczególnie ważne i nie trzymasz tam żadnych poufnych informacji, np. forum. Wtedy ustawiasz sobie dowolne hasło (nowe przeglądarki same podpowiadają silne hasła) i zapisujesz w przeglądarce.

Jeżeli zapomnisz hasło, to możesz skorzystać z funkcji “zapomniałem hasła” i na Twoją główną pocztę (z silnym hasłem i włączonym 2FA) dostaniesz wiadomość e-mail z informacją dotyczącą zresetowania hasła.

SYSBIT.IT

3) PHISHING I ATAKI SOCJOTECHNICZNE



Ataki socjotechniczne odpowiadają za ponad 60% incydentów bezpieczeństwa. Dlaczego tak się dzieje? Ponieważ ataki te wykorzystują najsłabszy punkt w całym procesie cyberbezpieczeństwa. Człowieka.

Ataki phishingowe odwołują się do słabości ludzkiej psychiki. Wykorzystują fakt, że jesteśmy z natury ciekawi, zmotywowani, pomocni, mamy obawy przed kłopotami, które mogą nas spotkać. Niestety, bardzo często reagujemy emocjonalnie na to, co nam się przydarza i właśnie ten fakt wykorzystują hakerzy.

Cyberprzestępcom chodzi o to, aby przekonać Cię do uruchomienia złośliwego pliku, który otrzymasz w załączniku lub aby podać na fałszywej stronie interesujące ich dane dotyczące np. logowania do banku, do konta w social mediach czy do konta poczty elektronicznej.

Oczywiście ataki socjotechniczne są nie tylko związane z pocztą elektroniczną i wiadomościami e-mail. Coraz częściej można usłyszeć o innych rodzajach ataków:

- ▶ fałszywych wiadomościach SMS dotyczących np. informacji o niedopłacie do przesyłki zakupu online
- ▶ spoofingu (podszycie się) numeru telefonu zaufanej instytucji (np. banku)
- ▶ fałszywe profile na social mediach.

Niestety, możliwości jest bardzo dużo

SYSBIT.IT

NA CO NALEŻY ZWRACAĆ UWAGĘ, ABY NIE PAŚĆ OFIARĄ TEGO TYPU ATAKU?

Przede wszystkim nie reaguj emocjonalnie, ale postępuj zgodnie z poniższymi wskazówkami, gdy otrzymasz:

▶ **Sprawdzaj nadawcę.**
Zawsze upewnij się, że wiesz, kto wysłał wiadomość. Podejrzane adresy e-mail, literówki w nazwach firm – to sygnały ostrzegawcze. W razie wątpliwości, skontaktuj się z nadawcą inną, zaufaną drogą.

▶ **Uważaj na linki i załączniki.**
Nie klikaj w podejrzane linki ani nie otwieraj załączników z nieznanych źródeł. Zawsze najedź kursorem na link, żeby zobaczyć pełen adres – fałszywe strony często mają bardzo podobne adresy do prawdziwych.

▶ **Nie daj się sprowokować emocjom.**
Cyberprzestępcy często grają na czas, strach czy ciekawość. Pilne komunikaty o zablokowaniu konta czy rzekome wygrane to częste sztuczki. Zachowaj spokój i zdrowy rozsądek.

▶ **Chroń swoje dane logowania.**
Nigdy nie podawaj haseł, numerów kart czy kodów PIN, klikając w linki z e-maili. Zawsze weryfikuj, czy strona, na której się logujesz, jest bezpieczna (https:// i ikona kłódki).

SYSBIT.IT

4) MALWARE

Termin “malware” (z ang. malicious software) odnosi się do złośliwego oprogramowania, które celowo zostało zaprojektowanie tak, aby wyrządzić szkody w systemie, na którym zostanie uruchomiony. W zależności od rodzaju (a jest ich cała masa), może chodzić o wyłączenie, zakłócenie, zniszczenie lub przejęcie kontroli nad systemem.

Jednym z najgroźniejszych typów złośliwego oprogramowania w ostatnim czasie jest oprogramowanie typu **ransomware**. Malware ten najczęściej ma za zadanie zaszyfrować dane na dysku. Następnie użytkownik dostaje informację na temat opłaty za możliwość odszyfrowania tych danych oczywiście, jeżeli wcześniej za to zapłaci za pomocą kryptowalut.

Czasami przed rozpoczęciem szyfrowania dane te zostają przesłane na serwer cyberprzestępców w celu wyłudzenia dodatkowych pieniędzy.

Znane są przypadki, gdzie z powodu ataku ransomware trzeba było ewakuować szpital, a podczas tej operacji umarł jeden z pacjentów. W USA zabrakło paliwa na stacjach benzynowych po udanym ataku na jedną z największych firm zajmujących się dystrybucją paliwa. Niestety tego typu ataki mogą być bardzo destrukcyjne, dlatego tak ważne jest, aby wiedzieć jak temu zapobiec.

Jak to zrobić? Przede wszystkim:

▶ **uważaj co uruchamiasz na swoim komputerze** – nigdy nie uruchamiaj programu, co do którego nie masz pewności
▶ **miej zainstalowany program antywirusowy**, który jest stale aktualizowany
▶ **aktualizuj system** – jeżeli widzisz, że Twój system czy program, którego używasz chce zainstalować aktualizację, nie czekaj – zrób to od razu
▶ **twórz regularne kopie zapasowe** – nawet, jeżeli Twoje dane zostaną zaszyfrowane, będziesz w stanie je łatwo odtworzyć bez żadnego płacenia.

SYSBIT.IT

5) URZĄDZENIA MOBILNE

W dzisiejszych czasach ciężko spotkać osobę, która nie posiada przy sobie małego komputera jakim jest smartphone. Ponad połowa ruchu w Internecie odbywa się za pomocą urządzeń mobilnych, takich jak smartphone czy tablet.

Niestety, wiedzą o tym także cyberprzestępcy. Trzymamy w naszych telefonach wiele danych na nasz temat: instalujemy aplikacje swojego banku czy social mediów, pocztę e-mail, zapisujemy hasła, dokumenty, podpinamy karty kredytowe i wrzucamy wiele innych, poufnych informacji.

Pewnie większość z Was kojarzy sprawę Pegazusa – złośliwego oprogramowania, które wykorzystując błąd w jednej z aplikacji było w stanie przejąć cały telefon. Dzięki temu atakujący mieli praktycznie nieograniczony dostęp do wszelkich danych. Mogli podsłuchiwać rozmowy, czytać SMS-y, wiadomości z komunikatorów, modyfikować je i wykonywać wiele innych działań dotyczących kradzieży danych.

Codziennie powstaje kilkadziesiąt tysięcy złośliwych aplikacji mobilnych. Często przybierają formę bardzo łudząco podobną do aplikacji banku, komunikatora czy innej popularnej aplikacji. Niestety nie mamy możliwości, aby zabezpieczyć się przed tego typu zdarzeniami w 100%. Ale możemy je maksymalnie zminimalizować. Jak możesz to zrobić?

▶ **Ustaw trudny do odgadnięcia PIN** lub wzór do odblokowania (PIN typu 1234,0000,0852 raczej nie jest dobrym wyborem)
▶ **Ustaw możliwość uwierzytelnienia za pomocą odcisku palca**, jeżeli Twój telefon na to pozwala
▶ **Nie uruchamiaj** aplikacji z niewiadomych źródeł
▶ **Kontroluj uprawnienia, jakie chce uzyskać aplikacja** – jeżeli aplikacja latarki potrzebuje dostępu do kontaktów, połączeń, plików, kamery, internetu to raczej nie jest to bezpieczna aplikacja
▶ **Rób kopie zapasowe danych w telefonie**
▶ **Nie przekładaj aktualizacji na później** – jeżeli dostaniesz informację odnośnie aktualizacji systemu czy jakiegoś programu – zrób to od razu.

SYSBIT.IT

Jeżeli po przeczytaniu tego dokumentu nadal coś jest dla Ciebie niejasne, lub chcesz się dowiedzieć jak wykonać technicznie którąś z czynności opisanych powyżej, nie krępuj się i napisz do mnie. Z przyjemnością Ci pomogę.

Wszystkiego bezpiecznego
Zespół SYSBIT

KONTAKT@SYSBIT.IT

WWW.SYSBIT.IT

SYSBIT.IT