BEZPIECZEŃSTWO W WIRTUALNYM ŚWIECIE

BEZPIECZEŃSTWO W WIRTUALNYM ŚWIECIE.

Internet jest miejscem, w którym nie tylko możemy korzystać z rozrywki, ale także możemy przekazywać różne informacje, porozumiewać się i kontaktować . Możemy robić to wszystko nie wychodząc z domu, pijąc w tym czasie kawę lub słuchać ulubionej muzyki. To bardzo ułatwia nam życie i jest jak najbardziej pożądane.

Ale niestety są także złe tego strony, wirtualny świat nie daje pełnego poczucia bezpieczeństwa, daje natomiast złudne poczucie, że łatwo można kontrolować, kto ma dostęp do naszych informacji czy danych. Nie jest to jednak takie proste i oczywiste.

Najważniejsze aby zdawać sobie sprawę, że takie zagrożenie istnieje i że trzeba się przed nim dobrze zabezpieczyć. Niestety nigdy nie możemy być w stu procentach pewni , że nasze informacje i dane są bezpieczne.

W wielu sytuacjach z treścią umieszczonych w internecie danych i wiadomości mogą zapoznać się osoby postronne czy nieupoważnione do ich posiadania. Należy zatem pamiętać aby tą drogą nie przekazywać informacji niejawnych oraz takich, które mają charakter informacji wrażliwych.

Ryzyko zapoznania się osób postronnych z naszymi informacjami możemy obniżyć stosując odpowiednie środki zabezpieczające, chociażby szyfrowaną pocztę elektroniczną. Służą do tego celu specjalne narzędzia kryptograficzne.

Możemy je także obniżyć stosując kilka prostych, podstawowych zasad:

1. Nigdy nie podawaj swoich danych jeśli nie musisz. Im mniej informacji o Tobie jest w sieci, tym Twoje bezpieczeństwo jest wyższe.
2. Nie przekazuj informacji poufnych (np. haseł) pocztą elektroniczną, SMS-ami, czatem.
3. Staraj się zawsze, jeśli to możliwe, korzystać z protokołu *HTTPS*. W czasie logowania i przesyłania danych sprawdź, czy adres w przeglądarce zaczyna się od „https” i czy obok widnieje symbol kłódki. Istnieje możliwość

zainstalowania w przeglądarce wtyczki *HTTPS Everywhere*, wtedy automatycznie będziesz łączyć się przez ten protokół.

4. Staraj się nie korzystać z niezabezpieczonego Wi-Fi. Jeśli nie masz innych możliwości połączenia z internetem, unikaj logowania się prawdziwymi danymi i nie wykonuj ważnych, wrażliwych operacji (np. finansowych).
5. Zawsze zabezpieczaj swoje konta w internecie hasłami. Dobre hasło powinno składać się z co najmniej 8-10 znaków, małych i wielkich liter, znaków specjalnych, bez używania popularnych słów. Zawsze używaj różnych haseł do różnych usług i regularnie je zmieniaj (podobnie jak w systemach bankowych).
6. Korzystając z poczty elektronicznej nie otwieraj linków niewiadomego pochodzenia;
7. Chroń swoje hasła – nie udostępniaj osobom postronnym, raczej nie zapisuj , nie zapamiętuj w komputerze.
8. Zabezpiecz hasłem (blokadą) dostęp do komputera, tabletu.
9. Pamiętaj - wyloguj się, kiedy skończysz korzystać z danej usługi.
10. Koniecznie używaj programu antywirusowego w komputerze. Pamiętaj o jego aktualizacji.
11. Nigdy nie używaj w swoim komputerze przypadkowo znalezionych nośników elektronicznych np. typu pendrive.

Przestrzegając powyższych zasad zwiększasz swoje bezpieczeństwo oraz bezpieczeństwo swoich informacji i danych.

Zagrożenia wynikające z funkcjonowania w wirtualnym świecie istnieją nie tylko podczas korzystania z komputerów czy laptopów ale także z telefonów komórkowych. Nie tak dawno było to urządzenie, z którego korzystali nieliczni, dzisiaj nikt nawet sobie nie wyobraża aby nie posiadać telefonu komórkowego. To podstawowy środek komunikacji. Obecny rynek telefonów komórkowych to głównie smartfony, które podobnie jak komputery narażone są na ataki i próby uzyskania informacji w sposób nielegalny. Smartfon z androidem to praktycznie taki przenośny komputer z duża ilością informacji i danych, dlatego konieczne jest stosowanie podobnych zasad bezpieczeństwa, jak podczas używania komputera czy tabletu.

Zasady, które zwiększają bezpieczeństwo korzystania z telefonu komórkowego.

1. Używaj zabezpieczenia blokady ekranu.

   W telefonach poprzedniej generacji blokada ekranu miała zapobiegać przypadkowemu i niepożądanemu naciśnięciu klawiszy, dzisiaj zyskała dodatkową funkcję, zabezpiecza telefon przed nieuprawnionym dostępem. Taką blokadę może stanowić hasło, kod PIN lub rysowany symbol na ekranie. Zwykłe przeciągnięcie palcem po ekranie praktycznie nie daje żadnej ochrony.

2. Zaszyfruj telefon.

   Po zaszyfrowaniu telefonu tylko osoba znająca hasło lub kod PIN ma dostęp do danych znajdujących się w telefonie. W przypadku kradzieży telefonu Twoje dane są bezpieczne.

   Proces szyfrowania nie jest długi a sposób jego przeprowadzenia znajdziesz w internecie.

3. Aktualizuj oprogramowanie, ale rozsądnie.

   Szczególną uwagę należy zwrócić na aktualizowanie systemu operacyjnego i programów, które mają dostęp do Internetu**.**

   Uważaj jednak na aktualizacje, w których aplikacja będzie żądała większych uprawnień niż te, które miała do tej pory. Staraj się zrozumieć dlaczego nowe uprawnienia są wymagane i czy aby nie stwarzają zagrożenia dla Twoich danych w telefonie.

4. Korzystaj rozważnie z sieci bezprzewodowych.

   Pamiętaj, że niezabezpieczona lub publiczna sieć WiFi może być źródłem wycieku Twoich poufnych lub wrażliwych danych.

5. Uważaj na instalowane aplikacje.

   Sprawdź czy to co instalujesz jest rzeczywiście tym, co chcesz zainstalować. Nie instaluj nigdy aplikacji pochodzących z niezaufanych źródeł. Pamiętaj, aby dokładnie przejrzeć i zrozumieć uprawnienia jakich wymaga aplikacja.

   Z pewnością aplikacja do włączania latarki w telefonie nie musi mieć np. możliwości wysyłania wiadomości SMS.

6. Nie klikaj bezmyślnie na słowo „dalej” lub „instaluj”.

Gdy masz jakiekolwiek wątpliwości po prostu nie instaluj aplikacji.

Niestety nawet przestrzeganie wszystkich powyższych zasad nie daje pełnej gwarancji bezpieczeństwa w wirtualnym świecie.

Kolejnym zagrożeniem dla naszej prywatności jest funkcjonowanie w świecie portali społecznościowych. Portale społecznościowe w dzisiejszych czasach cieszą się ogromną popularnością,. Pojawiło się nawet stwierdzenie, że osoba która nie korzysta z żadnego portalu po prostu nie istnieje. Portale pozwalają na wzajemną komunikację, wymianę myśli, poglądów i spostrzeżeń, dyskusję na określone tematy. Za ich pomocą można nie tylko pogłębić relacje z dotychczasowymi znajomymi, ale również nawiązać nowe kontakty nie wychodząc z domu.

Niestety funkcjonowanie na portalu podobnie jak w przypadku korzystania z komputera czy telefonu komórkowego wiąże się z pewnymi zagrożeniami. Uniknąć ich można posiadając odpowiednią wiedzę, zachowując daleko idące środki ostrożność oraz stosując zabezpieczenia minimalizujące ryzyko utraty danych.

Korzystając z portali społecznościowych należy pamiętać o następujących podstawowych środkach ostrożności:

1. Pamiętaj, w wirtualnym świecie nie jesteś anonimowy;
2. Dokładnie zapoznaj się z zasadami korzystania z portalu, czy nie ma tam zapisów tzw. „małym druczkiem” , które w jakiś sposób mogłyby być dla Ciebie niebezpieczne;
3. Unikaj umieszczania informacji, które mogą zdradzać zbyt wiele szczegółów z Twojego życia;
4. Nie umieszczaj danych, które są dla Ciebie wrażliwe;
5. Nie nawiązuj zbyt szybkich kontaktów z osobami przypadkowymi zwłaszcza z takimi , które wręcz nachalnie próbują taki kontakt z Tobą nawiązać;
6. Pamiętaj o najmłodszych, dzieci nie zawsze są świadome swoich poczynań, rozmawiaj z nimi, ucz je, przestrzegaj.

Nie stosując powyższych zasad narażamy siebie oraz swoich najbliższych na niebezpieczeństwo utraty danych, które następnie mogą być wykorzystywane do różnych celów nawet przestępstw.

Przedstawienie zagrożeń, które pojawiają się przy korzystaniu z Internetu za pomocą różnych urządzeń, nie ma na celu przestraszyć użytkowników lub spowodować że nagle ograniczone zostanie korzystanie z tego środka. Zdaję sobie sprawę, że nie jest to ani możliwe, ani pożądane. Świat idzie do przodu, wszystko się rozwija, my także powinniśmy dotrzymać kroku.

Chciałbym jedynie aby po zapoznaniu się z zasadami bezpieczeństwa, które przedstawiłem powyżej, wzrosła nasza świadomość, nasza wiedza na temat bezpiecznego funkcjonowania w wirtualnym świecie

„Wszystko jest dla ludzi, ale korzystajmy z tego w rozsądny i bezpieczny sposób”.

Praca zbiorowa – Zespół Stratpoints