INFORMACJA O ZAGROŻENIACH ZWIĄZANYCH Z USŁUGAMI ELEKTRONICZNYMI

1. CZEGO DOTYCZY INFORMACJA

Informacja dotyczy szczególnych zagrożeń związanych z korzystaniem przez użytkowników z usług świadczonych drogą elektroniczną.

2. DLACZEGO INFORMUJEMY O ZAGROŻENIACH

Taki obowiązek wynika z obowiązujących przepisów (art. 6 pkt 1 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną). Powinien go wykonać każdy podmiot świadczący usługi drogą elektroniczną.

3. CZY KORZYSTANIE Z USŁUG MSPADEK JEST BEZPIECZNE

Korzystanie ze strony internetowej www.mspadek.pl nie powoduje większych zagrożeń niż zwykłe korzystanie z Internetu oraz dokonywanie zakupów w sklepach internetowych i portalach aukcyjnych. W naszym przypadku wykorzystujemy środki zabezpieczające naszą infrastrukturę informatyczną przed nieuprawnionym dostępem osób trzecich, żeby zapewnić Ci bezpieczeństwo.

4. JAKIE ZAGROŻENIA MOGĄ WYSTĄPIĆ I NA CO TRZEBA UWAŻAĆ

Jeżeli korzystasz z Internetu i usług wykonywanych drogą elektroniczną to potencjalnie występują ryzyka, które powinno się brać pod uwagę. Takimi ryzykami mogą być:

- złośliwe oprogramowanie (ang. malware) – są to różne aplikacje lub skrypty (np. wirusy, robaki, trojany, keyloggery, dialery) infekujące system teleinformatyczny użytkownika sieci
- programy szpiegujące (ang. spyware) – są to programy śledzące działania użytkownika, gromadzące informacje o użytkowniku i wysyłające je bez jego wiedzy i zgody
- spam - są to niechciane i niezamawiane wiadomości elektroniczne najczęściej zawierające treści o charakterze reklamowym i rozsyłane jednocześnie do wielu odbiorców
- wyłudzanie poufnych informacji osobistych (ang. phishing) – jest to podszywanie się pod godną zaufania instytucję lub stronę www najczęściej w celu kradzieży hasła
- włamania do systemu informatycznego użytkownika przy użyciu różnych narzędzi hakerskich

5. JAK SIĘ CHRONIĆ

Ochrona przed zagrożeniami związanymi z korzystaniem z usług świadczonych drogą elektroniczną polega przede wszystkim na korzystaniu z Internetu w sposób świadomy:

- używaj programu antywirusowego na urządzeniu, które wykorzystujesz korzystając z Internetu
- aktualizuj program antywirusowy
- włącz zaporę sieciową (ang. firewall)
- aktualizuje oprogramowanie, którego używasz
- nie otwieraj załączników poczty elektronicznej niewiadomego pochodzenia
- czytaj okna instalacyjne aplikacji, a także ich licencji
- wyłącz makra w plikach MS Office nieznanego pochodzenia
- regularnie skanuj system programem antywirusowym i antymalware
- stosuj szyfrowanie transmisji danych

- używaj programów do wykrywania i zapobiegania włamaniom