

ZAŁĄCZNIK NR 5 DO REGULAMINU
INFORMACJA O SZCZEGÓLNYCH ZAGROŻENIACH ZWIĄZANYCH Z
KORZYSTANIEM PRZEZ UŻYTKOWNIKÓW Z USŁUG ŚWIADCZONYCH DROGĄ
ELEKTRONICZNĄ

Użyte w niniejszym załączniku pojęcia pisane wielką literą, o ile nie zdefiniowano ich odmiennie poniżej, mają znaczenie nadane im w Regulaminie. Usługodawcą w rozumieniu niniejszego załącznika jest Sprzedawca, to jest SZKOLENIA360 Sp. z o.o. z siedzibą w Łodzi. Użytkownikiem jest osoba korzystająca z usług świadczonych drogą elektroniczną za pośrednictwem Sklepu lub Platformy (usługobiorca w rozumieniu ustawy o świadczeniu usług drogą elektroniczną).

Usługodawca, wykonując obowiązek wynikający z art. 6 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2024 r. poz. 1513 ze zm.), informuje o szczególnych zagrożeniach związanych z korzystaniem przez Użytkowników z usług świadczonych drogą elektroniczną za pośrednictwem Sklepu oraz Platformy. Informacja niniejsza dotyczy zagrożeń, które mają charakter potencjalny i które należy brać pod uwagę mimo stosowania przez Usługodawcę środków zabezpieczających przed nieuprawnionym działaniem osób trzecich.

Do podstawowych zagrożeń związanych z korzystaniem z usług świadczonych drogą elektroniczną za pośrednictwem sieci Internet należą:

- złośliwe oprogramowanie: aplikacje lub skrypty o szkodliwym, przestępczym lub złośliwym działaniu wobec systemu teleinformatycznego wykorzystywanego przez Użytkownika, takie jak wirusy, robaki, konie trojańskie, keyloggers oraz dialery;
- programy szpiegujące (spyware): programy śledzące działania Użytkownika, które gromadzą informacje o nim i wysyłają je autorowi programu bez wiedzy i zgody Użytkownika;
- spam: niechciane i niezamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców, często zawierające treści o charakterze reklamowym;
- wyludzanie poufnych informacji (phishing): pozyskiwanie danych osobistych, w szczególności haseł, przez podszywanie się pod godną zaufania osobę lub instytucję;
- włamania do systemu teleinformatycznego Użytkownika z wykorzystaniem narzędzi takich jak exploit oraz rootkit.

W celu zminimalizowania ryzyka wystąpienia powyższych zagrożeń Użytkownik powinien zainstalować oraz na bieżąco aktualizować program antywirusowy na komputerze lub innym urządzeniu wykorzystywanym podczas korzystania ze Sklepu oraz Platformy.

Ochronę przed zagrożeniami związanymi z korzystaniem z usług świadczonych drogą elektroniczną zapewniają także:

- włączona zapora sieciowa (firewall);
- bieżąca aktualizacja systemu operacyjnego oraz oprogramowania wykorzystywanego na urządzeniu Użytkownika;
- nieotwieranie załączników poczty elektronicznej otrzymanych od nieznanych nadawców;
- zapoznavanie się z treścią informacji zamieszczanych w oknach instalacyjnych aplikacji, a także z treścią ich licencji;
- nieudostępnianie osobom nieuprawnionym haseł ani innych danych dostępowych do Platformy oraz poczty elektronicznej Użytkownika;
- regularne, całościowe skanowanie systemu operacyjnego programem antywirusowym;

- korzystanie z połączenia szyfrowanego (VPN), w szczególności w publicznych sieciach bezprzewodowych;
- używanie oryginalnego systemu operacyjnego oraz aplikacji pochodzących z legalnego źródła.