

Załącznik nr 1 do Regulaminu Serwisu II: www.malarstwoity.net, pro-vie.pl, skoko.pl, about-win-win.pl, laetarianie.eu, zycie-tak.net

Usługodawca, wykonując obowiązek z art. 6 pkt 1) ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204 z późn. zm.), informuje o szczególnych zagrożeniach związanych z korzystaniem przez Użytkowników z usług świadczonych drogą elektroniczną za pośrednictwem Serwisu II: www.malarstwoity.net, pro-vie.pl, skoko.pl, about-win-win.pl, laetarianie.eu, zycie-tak.net

Zagrożenie mogą wystąpić jedynie potencjalne, jednakże powinny być brane pod uwagę, pomimo stosowania przez Usługodawcę środków zabezpieczających infrastrukturę Usługodawcę przed nieuprawnionym działaniem osób trzecich.

Do podstawowych zagrożeń związanych z korzystaniem z sieci Internet należą:

- złośliwe oprogramowanie (ang. *malware*) – różnego rodzaju aplikacje lub skrypty mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do systemu teleinformatycznego Użytkownika sieci, takie jak wirusy, robaki, trojany (konie trojańskie), keylogery, dialery;
- programy szpiegujące (ang. *spyware*) – programy śledzące działania Użytkownika, które gromadzą informacje o Użytkowniku i wysyłają je – zazwyczaj bez jego wiedzy i zgody - autorowi programu;
- spam – niechciane i niezamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców, często zawierające treści o charakterze reklamowym;
- wyłudzenie poufnych informacji osobistych (np. hasła) przez podszywanie się pod godną zaufania osobę lub instytucję (ang. *phishing*);
- włamania do systemu teleinformatycznego Użytkownika z użyciem m.in. takich narzędzi hackerskich jak exploit i rootkit.

Użytkownik, aby uniknąć powyższych zagrożeń, powinien zaopatrzyć swój komputer i inne urządzenia elektroniczne, które wykorzystuje podłączając się do Internetu, w program antywirusowy. Program taki winien być stale aktualizowany. Ochronę przed zagrożeniami związanymi z korzystaniem przez Użytkowników z usług świadczonych drogą elektroniczną zapewniają także:

- włączona zapora sieciowa (ang. *firewall*),
- aktualizacja wszelkiego oprogramowania,
- nieotwieranie załączników poczty elektronicznej niewiadomego pochodzenia,
- czytanie okien instalacyjnych aplikacji, a także ich licencji, – wyłączenie makr w plikach MS Office nieznanego pochodzenia,
- regularne całościowe skany systemu programem antywirusowym i antymalware,
- szyfrowanie transmisji danych,
- instalacja programów prewencyjnych (wykrywania i zapobiegania włamaniom),
- używanie oryginalnego systemu i aplikacji, pochodzących z legalnego źródła.