

INFORMACJA O ZAGROŻENIACH

Niniejsza Informacja („**Informacja**”) o szczególnych zagrożeniach związanych z korzystaniem przez Użytkownika („**Użytkownik**”) z usług świadczonych drogą elektroniczną przez uczelnię wyższą pod nazwą **Wyższa Szkoła Ekonomii i Innowacji w Lublinie** z siedzibą w Lublinie przy ul. Projektowej 4, wpisana do Rejestru Wyższych Szkół Zawodowych prowadzonego przez Ministerstwo Nauki i Szkolnictwa Wyższego pod numerem 196. - MNiSW, NIP 712-26-52-693, REGON 432260703, adres elektroniczny: sekretariat@wsei.lublin.pl („**WSEI**”):

- a. dotyczy wszystkich portali internetowych („Portale”), których operatorem jest WSEI, w tym w szczególności Portalu LIKEFINANCE.EU dostępnego pod adresem www.likefinance.eu.
- b. publikowana jest przez WSEI stosownie do dyspozycji art. 6 pkt. 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2013 r., poz. 1422), celem zapewnienia Użytkownikom aktualnego źródła danych o szczególnych zagrożeniach związanych z korzystaniem przez nich z usług świadczonych drogą elektroniczną przez WSEI.

Informacja dotyczy zagrożeń, które WSEI ocenia za zagrożenia potencjalne, wobec czego powinny być one w ocenie WSEI brane pod uwagę, pomimo stosowania przez WSEI systemów zabezpieczających infrastrukturę WSEI przed nieuprawnionym oddziaływaniem osób trzecich.

Do mogących potencjalnie wystąpić zagrożeń WSEI zalicza:

1. możliwość naruszenia chronionych prawem praw własności intelektualnej, w tym w szczególności autorskich praw majątkowych, poprzez ich nieuprawnione wykorzystywanie (w tym: kopiowanie) bez wiedzy i/lub zgody podmiotu uprawnionego;
2. możliwość instalowania oprogramowania używanego do korzystania z usług świadczonych za pomocą Portali ze źródeł innych niż źródła autoryzowane przez WSEI, które mimo podejmowanych przez WSEI działań, mających na celu zminimalizowanie możliwości udostępniania modyfikowanych przez osoby trzecie wersji oprogramowania, może zawierać oprogramowanie złośliwe;
3. możliwość otrzymania niezamówionej informacji handlowej (spamu) przekazywanej drogą elektroniczną;
4. możliwość działania szkodliwego oprogramowania (np. oprogramowanie malware, robaki internetowe) w środowisku sieciowym, rozpowszechnianego poprzez replikację kodu;
5. możliwość łamania zabezpieczeń w celu pozyskania osobistych i poufnych informacji oraz kradzieży tożsamości, poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających wiadomości autentyczne;
6. możliwość odnalezienia słabości systemu kryptograficznego, a tym samym umożliwienia jego złamania lub obejścia, a w konsekwencji możliwość pozyskania osobistych i poufnych informacji w celu kradzieży tożsamości;
7. możliwość łowienia haseł (phishing) poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających do złudzenia autentyczne i w konsekwencji pozyskanie osobistych i poufnych informacji dotyczących Użytkownika;

8. możliwość niedozwolonego podsłuchu polegającego na wykorzystaniu programu komputerowego, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci (spyware).