

## **Informacje o szczególnych zagrożeniach związanych z korzystaniem usługi świadczonej drogą elektroniczną**

Zgodnie z art. 6 Ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002r. Nr 144 poz. 1204 z późn. zm.) Sklep informuje o szczególnych zagrożeniach związanych z korzystaniem usługi świadczonej drogą elektroniczną.

Informacje te wskazują zagrożenia, które mogą wystąpić jedynie potencjalnie, jednak winny być brane pod uwagę przez Kupującego, pomimo stosowania przez Sklep środków zabezpieczających przed nieuprawnionym działaniem osób trzecich.

Do podstawowych zagrożeń, o których mowa powyżej należą między innymi:

- spam – niechciane, niezamawiane wiadomości elektroniczne rozsyłane do wielu odbiorców;
- oprogramowanie szpiegujące (tzw. spyware) – programy komputerowe, których celem jest gromadzenie informacji o użytkowniku oraz przesyłanie danych i informacji użytkownika lub o użytkowniku bez jego wiedzy autorowi programu lub innej osobie.<sup>1</sup>
- Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji (np. danych logowania)<sup>2</sup>;
- Hacking – zachowanie polegające na nieuprawnionym uzyskaniu dostępu do informacji w wyniku przełamania systemu zabezpieczeń<sup>3</sup>;
- Malware (skrót od “malicious software”) jest uważany za uciążliwy lub szkodliwy typ oprogramowania, który ma na celu potajemnie uzyskać dostęp do urządzenia bez wiedzy użytkownika. Rodzaje złośliwego oprogramowania obejmują oprogramowanie szpiegujące (spyware), adware, phishing, wirusy, trojany, rootkity, zagrożenia typu ransomware oraz porwaczy przeglądarki.<sup>4</sup>

Aby uniknąć ww. zagrożeń przede wszystkim:

- należy zaopatrzyć swój komputer oraz inne urządzenia elektroniczne, które Kupujący wykorzystuje podłączając się do Internetu, w program antywirusowy z aktualną bazą wirusów;
- należy otwierać załączników poczty elektronicznej niewiadomego pochodzenia;
- nie należy przysyłać mailowo żadnych loginów i haseł;
- należy mieć włączoną zaporę sieciową tzw. firewall;
- należy regularnie aktualizować używane przeglądarki internetowe, system oraz oprogramowanie.

Sklep, działając stosownie do art. 6 pkt. 2 Ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002r. Nr 144 poz. 1204 z późn. zm.) informuje, że funkcja i cel oprogramowania lub danych niebędących składnikiem treści usług wprowadzanych przez Sklep do systemu teleinformatycznego, którym posługuje się Klient określone zostały w Polityce cookies zamieszczonej na stronie internetowej Sklepu

---

<sup>1</sup> Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną. Komisja Nadzoru Finansowego s. 7 [https://www.knf.gov.pl/knf/pl/komponenty/img/Bezp\\_finansowe\\_39005.pdf](https://www.knf.gov.pl/knf/pl/komponenty/img/Bezp_finansowe_39005.pdf)

<sup>2</sup> Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną. Komisja Nadzoru Finansowego s. 7 [https://www.knf.gov.pl/knf/pl/komponenty/img/Bezp\\_finansowe\\_39005.pdf](https://www.knf.gov.pl/knf/pl/komponenty/img/Bezp_finansowe_39005.pdf)

<sup>3</sup> Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną. Komisja Nadzoru Finansowego s. 7 [https://www.knf.gov.pl/knf/pl/komponenty/img/Bezp\\_finansowe\\_39005.pdf](https://www.knf.gov.pl/knf/pl/komponenty/img/Bezp_finansowe_39005.pdf)

<sup>4</sup> <https://www.avast.com/pl-pl/c-malware>