

Informacja o zagrożeniach związanych z cyberbezpieczeństwem

W związku z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023, poz. 913) przekazujemy informację o zagrożeniach oraz sposobach zabezpieczeń stosowanych w celu minimalizacji ryzyk związanych z funkcjonowaniem w środowisku internetowym.

Cyberbezpieczeństwo, zgodnie z obowiązującymi przepisami, to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy” (art. 2 pkt 4) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Do najpopularniejszych zagrożeń związanych z funkcjonowaniem w sieci internetowej możemy zaliczyć

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, itp.),
- kradzieże tożsamości,
- modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- podszywanie się pod inne usługi
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. phishing, czyli wyłudzenie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję.

Postępowanie w celu minimalizacji ryzyka związanego z użytkowaniem sieci komputerowej, komputera, telefonu:

- Używaj oprogramowania antywirusowego,
- Regularnie aktualizuj oprogramowanie antywirusowe,
- Skanuj komputer, pamięci przenośne USB oprogramowaniem antywirusowym,
- Aktualizuj systemy operacyjne oraz zainstalowane oprogramowanie,
- Nie pobieraj i nie otwieraj plików, dokumentów nieznanego pochodzenia,
- Nie pobieraj załączników poczty elektronicznej od nieznanych nadawców, zawsze weryfikuj adres z którego przyszedł e-mail,
- Uważaj na telefony od osób podszywających się pod urzędy, policję, członków rodziny, proszących o pilne przesłanie pieniędzy,
- Uważaj na telefony oraz e-maile informujące o zwrotach podatku, informacjach o spadku – najprawdopodobniej są to próby wyłudzenia,
- Nie otwieraj plików nieznanego pochodzenia,

- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu SSL,
- Nigdy nie podawaj hasła lub loginu do swojego konta bankowego, konsultant banku nigdy nie poprosi o takie dane w celu weryfikacji,
- Nie wysyłaj e-maili zawierających poufne informacje (takie dane zawsze zabezpieczaj hasłem),
- Nie wpisuj swoich danych na nieznanym serwisach (nie podawaj numerów kart kredytowych, numeru pesel),
- Wykonuj kopie zapasowe ważnych danych i przechowuj je w innym miejscu niż na komputerze z którego zostały wykonane, aby w przypadku infekcji nie utracić zgromadzonych plików.
- Regularnie zapoznawaj się z zestawem porad publikowanym przez ekspertów z Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: <https://www.cert.pl/ouch/>

Przeglądaj poradniki, m.in.:

- Strona internetowa Ministerstwa Cyfryzacji: <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>
- Fundacja Instytut Cyberbezpieczeństwa: <https://instytutcyber.pl/category/artykuly/>
- Fundacja Bezpieczna Cyberprzestrzeń – podcasty: <https://www.youtube.com/user/cybsecurity> .