CYBERBEZPIECZEŃSTWO

FILHARMONIA PODKARPACKA
IM. ARTURA MALAWSKIEGO
W RZESZOWIE

Szanowni Państwo !

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369, z późn.zm.), przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

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 w cyberprzestrzeni możemy zaliczyć:

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

Sposoby zabezpieczenia się przed zagrożeniami:

1. Chronić urządzenia używając programów antywirusowych.
2. Zawsze posiadać aktualny system operacyjny w swoim komputerze/laptopie.

3. Nie instalować aplikacji oraz **oprogramowania pochodzącego z niepewnego źródła** oraz takiego, które chce się zainstalować, gdy wejdziemy na jakąś stronę internetową.
4. Regularnie skanować komputer/telefon w celu wykrycia niebezpiecznego oprogramowania/aplikacji.
5. Stosować szyfrowanie (zabezpieczenie kryptograficzne) wobec urządzeń przenośnych typu laptop, pendrive itp.
6. Szyfrować pamięć wewnętrzną telefonu. Koniecznie ustawić PIN lub/oraz znak graficzny do odblokowywania telefonu, a także skorzystać z funkcji biometryki (odcisk palca, skan twarzy).
7. Uważać na telefony, wiadomości SMS, e-mail, które nakłaniają do podania danych osobowych czy kliknięcia w link w celu skorzystania z usług.
8. Nie korzystać z tzw. „otwartych" sieci Wi-Fi.
9. Przy płatnościach drogą elektroniczną warto upewnić się, że transmisja danych jest szyfrowana.
10. Stosować hasła o wysokim poziomie skomplikowania (najlepiej co najmniej 12 znaków, wielka, mała litera, cyfra i znak specjalny).
11. Stosować uwierzytelnianie dwuskładnikowe (np. za pośrednictwem np. PIN, SMS, klucza fizycznego, tokena).
12. Zmieniać cyklicznie hasła (np. co 30 dni).
13. Nie udostępniać swoich haseł innym osobom/podmiotom.
14. Warto używać tzw. menedżerów haseł służących do ich przechowywania.
15. Nie podłączać do swoich urządzeń magnetycznego/półprzewodnikowego nośnika danych (np. pendrive, dysk twardy, karta pamięci) lub optycznego nośnika danych (np. płyta CD, DVD, BluRay) niepewnego pochodzenia.
16. Nie zostawiać danych osobowych w niesprawdzonych serwisach i na stronach internetowych.
17. Czytać regulaminy.

Informacje o cyberbezpieczeństwie

https://stojpomyslpolacz.pl/

https://cert.pl/

https://akademia.nask.pl/

https://www.saferinternet.pl/