Zespół Szkół Ekonomicznych w Pile

CYBERBEZPIECZEŃSTWO

Cyberbezpieczeństwo zgodnie z obowiązującymi przepisami to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzania 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).

Udostępniamy Państwu najważniejsze zagadnienia dot. niebezpieczeństw, które mogą Państwo napotkać w szeroko rozumianej cyberprzestrzeni.
Ponadto informujemy Państwa o efektywnych metodach radzenia sobie i zapobiegania tego typu niebezpieczeństwom.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

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

Sposoby zabezpieczania się przed zagrożeniami:

- Zainstaluj i używaj oprogramowania antywirusowego.
- Aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów.
- Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.
- Unikaj stosowania haseł typu: „1234", „qwerty", „abc".
- Używaj haseł zbudowanych przynajmniej z 8 znaków i stosuj złożoność hasła (małe, wielkie litery, cyfry lub znaki specjalne). Im dłuższe hasło, tym trudniej je złamać.
- Używaj złożonego hasła do zabezpieczenia WiF-i w domu.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
- Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz, poproś o sprawdzenie kogoś, kto się na tym zna.
- Sprawdzaj pliki pobierane z Internetu za pomocą skanera programu antywirusowego.
- Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany, i inne zagrożenia.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
- Nie otwieraj linków do stron www z mail niewiadomego pochodzenia.
- Nie otwieraj plików nieznanego pochodzenia np. przysyłanych w mailu – zwłaszcza jeśli nie

znasz adresata, a pliki mają dziwne rozszerzenie np. wezwanie.zip, faktura.vbs, faktura.exe, zdjęcie.jpg.exe, przypomnienie.pdf.exe.
• Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – zabezpiecz je np. hasłem i szyfruj – hasło przekazuj w sposób bezpieczny innym kanałem komunikacyjnym np. przez SMS.
• Pamiętaj o uruchomieniu firewalla.
• Wykonuj kopie zapasowe ważnych danych.
• Pamiętaj, że żadne banku, urzędy czy Sądy nie wysyłają e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

Dodatkowe informacje i porady dotyczące cyberbezpieczeństwa.

Warto również zapoznać się z informacjami poniżej:
1. STÓJ. POMYŚL. POŁĄCZ To polska wersja międzynarodowej kampanii STOP. THINK. CONNECT.TM, mającej na celu podnoszenie poziomu świadomości społecznej w obszarze cyberbezpieczeństwa. https://stojpomyslpolacz.pl
2. Zapoznaj się z dobrymi praktykami, które znajdziesz na stronie https://stojpomyslpolacz.pl oraz z dostępnymi na niej materiałami do pobrania.
3. OUCH! To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Dostępne są wszystkie polskie wydania, które zawierają krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie i swoich najbliższych oraz swoją organizację. https://www.cert.pl/ouch/

DYREKTOR SZKOŁY
M. Michalska
mgr Magdalena Michalska