CYBERBEZPIECZEŃSTWO

w Publicznej Szkole Podstawowej im. Jana Pawła II w Stobiernej

Dbając o bezpieczeństwo naszych uczniów, rodziców i nauczycieli, Publiczna Szkoła Podstawowa im. Jana Pawła II w Stobiernej stawia na wysoki poziom cyberbezpieczeństwa. W dzisiejszych czasach internet jest nieodłącznym elementem edukacji i życia codziennego, dlatego chcemy zapewnić, że korzystanie z zasobów online odbywa się w sposób bezpieczny i odpowiedzialny.

Dyrektor Publicznej Szkoły Podstawowej im. Jana Pawła II w Stobiernej *Zarządzeniem nr 11A/2023 z dnia 01.09.2023r. wprowadza w życie* **PROCEDURĘ ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM** - *załącznik nr 1 do zarządzenia*

Szanowni Państwo,

realizując zadania wynikające z art. 22 ust. 1 pkt. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j.Dz.U.2023.913) przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie 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.

Zrozumienie zagrożeń cyberbezpieczeństwa to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- 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).

Stosowanie zasad bezpiecznego poruszania się w cyberprzestrzeni- to sposób zabezpieczenia się przed zagrożeniami.

Zasady bezpiecznego poruszania się w cyberprzestrzeni

1. Zawsze korzystaj z oprogramowania antywirusowego stosującego ochronę w czasie rzeczywistym.
2. Pamiętaj o uruchomieniu firewalla.

3. Stosuj bezpieczne, unikalne hasła oraz pamiętaj o ich cyklicznej zmianie.
4. Regularnie, bez zbędnej zwłoki aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów.
5. Regularnie, bez zbędnej zwloki, aktualizuj system operacyjny oraz aplikacje.
6. Regularnie skanuj komputer w celu wykrycia niebezpiecznego oprogramowania oraz działających procesów mogących narazić cię na wykradzenie danych, jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować.
7. Nie otwieraj plików nieznanego pochodzenia- plików od nieznanych osób, firm lub instytucji, gdyż często są to sfabrykowane wiadomości w celu wyłudzenia danych lub zainstalowania niebezpiecznego oprogramowania.
8. Pamiętaj, że żaden bank, czy urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
9. Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu bezpieczeństwa chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
10. Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny, innym kanałem komunikacji. Jeżeli już musisz to zrobić to staraj się zabezpieczyć plik przed odczytaniem przez osoby niepowołane.
11. Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich,
12. Nie używaj niesprawdzonych programów zabezpieczających, czy też programów do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
13. Każdy pobrany plik z internetu sprawdzaj za pomocą skanera antywirusowego.
14. Staraj się nie odwiedzać stron, które oferują niesamowite atrakcje (pieniądze, darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
15. Pracuj na najniższych możliwych uprawnieniach użytkownika.
16. Cyklicznie wykonuj kopie zapasowe danych, których utrata przyniosła by dla Ciebie duże straty.
17. Unikaj kontaktów z osobami podającymi się za przedstawicieli firm, instytucji, którzy żądają od nas podania danych autoryzacyjnych lub nakłaniają nas do instalowania aplikacji zdalnego dostępu, unikaj korzystania z otwartych sieci Wi-Fi.
18. Tam, gdzie to możliwe (konta społecznościowe, konto email, usługi e-administracji, usługi finansowe) stosuj dwuetapowego uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego, faceID.
19. Czytaj regulaminy.

Powyższe informacje nie stanowią zamkniętego katalogu zagrożeń oraz porad jak ich uniknąć.

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

Porady bezpieczeństwa dla użytkowników komputerów dostępne są na:

- stronach serwisu Rzeczypospolitej Polskiej Baza wiedzy – Cyberbezpieczeństwo
- portalu CERT Polska

Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty (z ang. Computer Emergency Response Team).

- witrynie internetowej polskich wydań OUCH!

OUCH! To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację. Zobacz wszystkie polskie wydania OUCH! na stronie CERT Polska.

- stronie OSE IT-szkoła w poradniku „ABC Cyberbezpieczeństwa”
- stronie internetowej kampanii STÓJ. POMYŚL. POŁĄCZ

Zgłaszanie incydentów bezpieczeństwa: https://incydent.cert.pl/

NASZE PRIORYTETY W ZAKRESIE CYBERBEZPIECZEŃSTWA:

1. **Ochrona danych osobowych**

Zapewniamy, że wszystkie dane uczniów, rodziców oraz pracowników szkoły są chronione zgodnie z przepisami RODO. Stosujemy odpowiednie procedury i technologie, aby minimalizować ryzyko ich nieuprawnionego dostępu.

2**. Bezpieczne korzystanie z internetu**

Uczymy naszych uczniów, jak świadomie i odpowiedzialnie korzystać z internetu. Organizujemy warsztaty i szkolenia na temat ochrony prywatności, rozpoznawania zagrożeń w sieci, takich jak phishing czy cyberprzemoc, oraz zachowywania odpowiednich standardów etycznych w kontaktach online.

3. **Kontrola dostępu do zasobów internetowych**

W szkolnej sieci komputerowej wprowadziliśmy odpowiednie filtry, które blokują dostęp do stron zawierających nieodpowiednie treści. Dzięki temu uczniowie mogą korzystać z internetu w celach edukacyjnych w bezpiecznym środowisku.

4. **Bezpieczeństwo urządzeń cyfrowych**

Nasza szkoła dba o to, aby urządzenia, z których korzystają uczniowie i nauczyciele, były odpowiednio zabezpieczone. Regularnie aktualizujemy oprogramowanie, instalujemy systemy antywirusowe oraz dbamy o bezpieczne hasła do szkolnych kont.

5. **Reagowanie na incydenty**

W przypadku zagrożeń w cyberprzestrzeni, takich jak ataki hakerskie, incydenty związane z naruszeniem danych czy cyberprzemoc, szkoła posiada jasne procedury reagowania. Współpracujemy z rodzicami oraz odpowiednimi instytucjami, aby zapewnić jak najszybsze i skuteczne rozwiązanie problemu.

6. **Edukacja w zakresie cyberbezpieczeństwa**

W ramach programu nauczania informatyki oraz dodatkowych zajęć, dzieci uczą się, jak unikać zagrożeń związanych z korzystaniem z sieci, jak chronić swoją tożsamość oraz jak reagować w przypadku cyberprzemocy. Stawiamy na rozwijanie umiejętności cyfrowych, które przygotują naszych uczniów na bezpieczne funkcjonowanie w nowoczesnym świecie.

7. Współpraca z rodzicami

Zapewniamy także wsparcie rodzicom, organizując spotkania informacyjne i warsztaty na temat tego, jak mogą wspierać swoje dzieci w bezpiecznym korzystaniu z internetu w domu. Wierzymy, że współpraca z rodzicami jest kluczowa w zapewnianiu pełnej ochrony naszych uczniów.

Razem dbajmy o bezpieczne i odpowiedzialne korzystanie z technologii cyfrowych!!!