“Trudne sprawy” w prosty sposób.

Materiał uzupełniajacy szkolenie

** CHROŃ DANE • MYŚL KRYTYCZNIE • REAGUJ ŚWIADOMIE**



.

Paweł Kręt zakres **: Cyberbezpieczeństwo.**

Jak korzystać z broszury?

Nie musisz być informatykiem, żeby dobrze rozumieć cyberbezpieczeństwo. Najważniejsze jest rozpoznawanie sytuacji, w których ktoś próbuje Cię oszukać, wyłudzić dane albo przejąć konto.

W broszurze znajdziesz proste definicje, przykłady z życia, sygnały ostrzegawcze oraz wskazówki, jak reagować na zagrożenia.

Motto szkolenia : **ZATRZYMAJ SIĘ → SPRAWDŹ → DOPIERO DZIAŁAJ.**

Spis treści

- 1. Cyberbezpieczeństwo – podstawowe pojęcia i zagrożenia
- 2. Silne hasła i ochrona kont
- 3. Phishing i socjotechnika
- 4. Bezpieczeństwo urządzeń i prywatność
- 5. Reagowanie na incydenty
- 6. Szybka lista kontrolna bezpieczeństwa

1. Cyberbezpieczeństwo – co to właściwie jest?

Cyberbezpieczeństwo to działania, które pomagają chronić urządzenia, konta, sieci i informacje przed kradzieżą, uszkodzeniem, utratą lub nieuprawnionym dostępem. Dotyczy nie tylko firm i instytucji, ale także każdego użytkownika smartfona, komputera czy mediów społecznościowych.

Co warto chronić?

- Dane osobowe – np. imię i nazwisko, adres, numer telefonu, PESEL, zdjęcia.
- Konta – poczta e-mail, dziennik elektroniczny, media społecznościowe, gry i bankowość.
- Urządzenia – telefon, laptop, komputer szkolny, tablet.
- Dostęp do usług – hasła, kody jednorazowe, sesje logowania i kopie zapasowe.

Najczęstsze zagrożenia

Zagrożenie	Na czym polega?
Phishing	Fałszywa wiadomość lub strona, która ma skłonić do podania danych albo kliknięcia linku.
Złośliwe oprogramowanie (malware)	Program, który może kraść dane, szpiegować, uszkadzać pliki lub przejąć kontrolę nad urządzeniem.
Ransomware	Rodzaj złośliwego oprogramowania, który blokuje lub szyfruje pliki i żąda okupu.
Kradzież tożsamości	Wykorzystanie cudzych danych do podszywania się pod tę osobę.
Przejęcie konta	Uzyskanie dostępu do konta bez zgody właściciela, np. przez wyłudzone hasło.
Cyberprzemoc	Krzywdzenie, nękanie, ośmieszanie lub zastraszanie kogoś z użyciem narzędzi cyfrowych.

Zapamiętaj
Cyberatak nie zawsze zaczyna się od zaawansowanego włamania. Często wystarczy pośpiech, zaufanie do fałszywej wiadomości albo ujawnienie hasła.

2. Silne hasła i ochrona kont

Hasło jest jednym z podstawowych zabezpieczeń konta. Powinno być trudne do odgadnięcia, a jednocześnie nie może być używane wszędzie.

Jakie hasło jest bezpieczniejsze?

- Długie – najlepiej składające się z kilku losowych słów lub długiej, unikalnej frazy.
- Unikalne – inne dla każdego ważnego konta.
- Nieoczywiste – bez imienia, daty urodzenia, nazwy szkoły czy prostych ciągów typu 123456.
- Nieudostępniane – nie wysyłaj hasła znajomym ani osobom podającym się za administratora.

Przykład
Zamiast krótkiego, przewidywalnego hasła wybierz długą frazę złożoną z niepowiązanych słów. Nie używaj przykładów z broszury jako własnego hasła.

Menedżer haseł

Menedżer haseł to aplikacja, która bezpiecznie przechowuje i pomaga tworzyć unikalne hasła. Użytkownik zapamiętuje przede wszystkim jedno silne hasło główne. Wybieraj sprawdzone rozwiązania i zabezpieczaj je MFA.

Czym jest MFA?

Uwierzytelnianie wieloskładnikowe (MFA) wymaga potwierdzenia logowania dodatkowym elementem, np. aplikacją uwierzytelniającą, kluczem bezpieczeństwa lub kodem. Dzięki temu samo poznanie hasła może nie wystarczyć do przejęcia konta.

- Włącz MFA przede wszystkim na poczcie e-mail, kontach społecznościowych i innych ważnych usługach.
- Nigdy nie podawaj kodów jednorazowych osobie, która do Ciebie dzwoni lub pisze.
- Nie zatwierdzaj powiadomienia logowania, którego samodzielnie nie rozpocząłeś.

Zasady ochrony kont

1. Używaj unikalnego hasła do każdego ważnego konta.
2. Włącz MFA, jeśli usługa je udostępnia.
3. Sprawdzaj aktywne sesje i wylogowuj nieznane urządzenia.
4. Aktualizuj dane odzyskiwania konta i zabezpiecz skrzynkę e-mail.
5. Nie zapisuj haseł w widocznym miejscu ani w niezabezpieczonym pliku.

3. Phishing i socjotechnika

Phishing to próba wyłudzenia informacji lub skłonienia użytkownika do niebezpiecznego działania. Oszust może podszywać się pod bank, kuriera, szkołę, serwis społecznościowy, znajomego lub administratora.

Rodzaje oszustw

- Phishing – najczęściej fałszywe e-maile lub strony internetowe.
- Smishing – oszustwa za pomocą SMS-ów lub komunikatorów.
- Vishing – oszustwa telefoniczne, w których rozmówca próbuje wyłudzić dane lub pieniądze.
- Podszywanie się – przejęte konto znajomego lub fałszywy profil prosi o kod, pieniądze albo pilną pomoc.

Sygnały ostrzegawcze

- Wiadomość wywołuje strach lub presję czasu: „natychmiast”, „ostatnia szansa”, „konto zostanie zablokowane”.
- Nadawca ma nietypowy adres, literówkę w nazwie lub nieoczekiwaną domenę.
- Link prowadzi do adresu, który nie pasuje do oficjalnej strony usługi.
- Ktoś prosi o hasło, kod MFA, dane karty albo zainstalowanie programu.
- Wiadomość zawiera nieoczekiwaną fakturę, nagrodę, dopłatę do przesyłki lub prośbę o pilny przelew.
- Załącznik lub prośba pojawia się bez kontekstu i nie była wcześniej zapowiedziana.

Ważne
Błędy językowe mogą być sygnałem ostrzegawczym, ale poprawna polszczyzna nie oznacza, że wiadomość jest prawdziwa.

Jak bezpiecznie sprawdzić wiadomość?

6. Nie klikaj od razu linku ani załącznika.
7. Sprawdź pełny adres nadawcy i domenę, ale pamiętaj, że można je podszyć.
8. Otwórz stronę usługi samodzielnie, wpisując jej adres lub używając oficjalnej aplikacji.
9. Skontaktuj się z nadawcą innym, znanym kanałem, np. zadzwoń na zapisany numer.
10. Zgłoś podejrzaną wiadomość zgodnie z zasadami szkoły lub danej usługi.

Socjotechnika – manipulowanie człowiekiem

Socjotechnika wykorzystuje emocje i zaufanie, np. autorytet („jestem z działu IT”), strach („stracisz konto”), ciekawość („zobacz kompromitujące zdjęcie”) albo presję („zrób to natychmiast”). Zatrzymaj się i zweryfikuj prośbę, szczególnie gdy dotyczy pieniędzy, haseł lub kodów.

4. Bezpieczeństwo urządzeń i prywatność

Jak zabezpieczyć komputer i smartfon?

- Instaluj aktualizacje systemu i aplikacji – naprawiają one m.in. znane luki bezpieczeństwa.
- Korzystaj z blokady ekranu: silnego kodu, hasła lub biometrii.
- Pobieraj aplikacje z oficjalnych sklepów i programy z zaufanych źródeł.
- Nie otwieraj nieoczekiwanych załączników i nie uruchamiaj nieznanych plików.
- Włącz wbudowane zabezpieczenia systemu, takie jak zapora i ochrona antywirusowa.
- Twórz kopie zapasowe ważnych plików i sprawdzaj, czy można je odtworzyć.
- Nie pozostawiaj odblokowanego urządzenia bez nadzoru.

Bezpieczne Wi-Fi

- Korzystaj z zaufanych sieci i unikaj przesyłania wrażliwych danych przez nieznane, otwarte Wi-Fi.
- Sprawdzaj nazwę sieci – oszust może utworzyć punkt dostępowy o podobnej nazwie.
- Wyłącz automatyczne łączenie z nieznanymi sieciami.
- Po użyciu wyloguj się z kont na współdzielonym komputerze.
- W razie wątpliwości użyj transmisji komórkowej do ważnych operacji.

Prywatność w mediach społecznościowych

- Ogranicz widoczność postów i danych profilu do zaufanych odbiorców.
- Nie publikuj adresu zamieszkania, planów wyjazdu ani danych dokumentów.
- Zastanów się, czy zdjęcie lub komentarz nie ujawnia informacji o Tobie lub innych osobach.
- Przeglądaj uprawnienia aplikacji – np. dostęp do lokalizacji, mikrofonu i kontaktów.
- Nie akceptuj automatycznie zaproszeń od nieznanych osób.

Ślad cyfrowy

Ślad cyfrowy to informacje pozostawiane podczas aktywności w sieci: publikacje, komentarze, zdjęcia, reakcje czy dane zbierane przez usługi. Usunięcie posta nie zawsze oznacza, że zniknęły wszystkie kopie lub zrzuty ekranu. Przed publikacją pomyśl o konsekwencjach dla siebie i innych.

Zasada prywatności
Udostępniaj tylko te informacje, które są potrzebne. To, że aplikacja prosi o dostęp do danych, nie oznacza, że musisz go przyznać.

5. Reagowanie na incydenty

Incydent bezpieczeństwa to zdarzenie, które może naruszyć poufność, integralność lub dostępność danych i systemów. Przykłady: przejęcie konta, utrata urządzenia, kliknięcie fałszywego linku, ujawnienie hasła lub podejrzana aktywność.

Kliknąłem podejrzany link – co robić?

11. Nie wpisuj kolejnych danych i nie zatwierdzaj żadnych próśb o logowanie.
12. Jeśli podałeś hasło, zmień je jak najszybciej, korzystając z oficjalnej strony lub aplikacji. Zmień je również wszędzie tam, gdzie było używane.
13. Wyloguj nieznane sesje, włącz MFA i sprawdź dane odzyskiwania konta.
14. Jeśli pobrałeś plik lub uruchomiłeś program, odłącz urządzenie od sieci, jeśli podejrzewasz infekcję, i poproś o pomoc zaufaną osobę lub administratora.
15. Zachowaj wiadomość, zrzuty ekranu i inne informacje potrzebne do zgłoszenia incydentu.
16. Jeśli ujawniono dane płatnicze lub doszło do transakcji, pilnie skontaktuj się z bankiem.

Konto zostało przejęte

- Użyj oficjalnej procedury odzyskiwania konta.
- Zmień hasło z bezpiecznego urządzenia i zabezpiecz powiązaną pocztę e-mail.
- Usuń nieznane sesje, aplikacje i metody odzyskiwania.
- Ostrzeż znajomych, jeśli z Twojego konta wysyłano podejrzane wiadomości.
- Zgłoś sprawę administratorowi usługi lub szkolnemu opiekunowi IT, jeśli dotyczy konta szkolnego.

Cyberprzemoc lub publikacja prywatnych materiałów

- Nie odpowiadaj agresją i nie rozpowszechniaj dalej krzywdzących treści.
- Zabezpiecz dowody: zrzuty ekranu, daty, nazwy kont i linki – o ile można to zrobić bez narażania się.
- Zablokuj i zgłoś konto lub treść w serwisie.
- Powiedz zaufanej osobie dorosłej, wychowawcy, pedagogowi lub psychologowi szkolnemu.
- W przypadku bezpośredniego zagrożenia bezpieczeństwa skontaktuj się z odpowiednimi służbami.

Gdzie szukać pomocy w Polsce?

- Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT NASK – zgłaszanie incydentów i materiały edukacyjne.
- CERT Polska – informacje o zagrożeniach i sposobach zgłaszania podejrzanych wiadomości.
- W szkole: nauczyciel informatyki, administrator IT, wychowawca, pedagog lub dyrekcja.

Oficjalne serwisy: cert.pl oraz incydent.cert.pl. W razie podejrzenia oszustwa finansowego skontaktuj się również z bankiem.

6. Szybka lista kontrolna bezpieczeństwa

Zaznacz, które zasady już stosujesz. Wróć do listy regularnie i po zmianie urządzenia lub konta.

☐ Mam unikalne hasła do ważnych kont.

☐ Korzystam z menedżera haseł lub innego bezpiecznego sposobu ich przechowywania.

☐ Mam włączone MFA na poczcie i najważniejszych kontach.

☐ Nie udostępniam nikomu haseł ani kodów jednorazowych.

☐ Aktualizuję system i aplikacje.

☐ Mam blokadę ekranu na telefonie i komputerze.

☐ Wiem, jak zgłosić podejrzaną wiadomość.

☐ Sprawdzam linki i prośby o pieniądze lub dane innym kanałem.

☐ Ograniczam publiczny dostęp do danych w mediach społecznościowych.

☐ Wiem, do kogo w szkole zgłosić incydent.

☐ Wykonuję kopie zapasowe ważnych plików.

Pięć pytań przed kliknięciem

1. Czy znam nadawcę? 2. Czy spodziewam się tej wiadomości? 3. Czy adres strony jest prawidłowy? 4. Czy ktoś wywiera presję? 5. Czy mogę potwierdzić prośbę innym kanałem?