„Projekt współfinansowany ze środków PFRON
będących w dyspozycji
Samorządu Województwa Wielkopolskiego”

MODUŁ EDUKACYJNY

„KOMPETENCJE PRZYSZŁOŚCI 4.0”

CYBERBEZPIECZEŃSTWO

I HIGIENA CYFROWA

Cyberbezpieczeństwo to umiejętność ochrony siebie, swoich danych i swoich urządzeń w Internecie. W dzisiejszym świecie każde nasze kliknięcie zostawia ślad, a każdy – niezależnie od wieku, doświadczenia i aktywności – może stać się celem ataku.

Niniejszy materiał podsumowuje najważniejsze zasady bezpiecznego korzystania z Internetu, omawiane podczas warsztatów.

1. OSINT – biały wywiad

OSINT to wyszukiwanie informacji o osobach i firmach z publicznie dostępnych źródeł, takich jak:

- wyszukiwarki internetowe,
- media społecznościowe,
- ogólnodostępne bazy i portale.

To, co publikujemy w sieci, może zostać łatwo przez kogoś odnalezione i zinterpretowane. Dlatego warto dbać o to, jakie informacje o sobie udostępniamy.

2. Ochrona danych i prywatności

Wszystko, co trafia do Internetu, zostaje tam na zawsze. Zdjęcia, komentarze, opisy i reakcje często zawierają więcej danych, niż nam się wydaje – np. lokalizację, dane urządzenia czy datę wykonania zdjęcia.

Warto zwrócić uwagę szczególnie na:

- ustawienia prywatności w mediach społecznościowych,
- to, komu udostępniamy zdjęcia i posty,
- jakie informacje pojawiają się na naszych profilach (np. szkoła, miejsce pracy, adres zamieszkania).

3. Silne hasła i ochrona kont

Dobre hasło to podstawa bezpieczeństwa. Najważniejsze zasady:

- Długie hasło – minimum 14 znaków.
- Inne hasło do każdej usługi – nie powtarzamy tych samych haseł.
- Menedżer haseł – narzędzie, które zapamiętuje i szyfruje hasła za nas.

Przykłady: KeePass, Bitwarden.

Dwuskładnikowe uwierzytelnianie (2FA) – dodatkowy kod z SMS-a lub aplikacji.

Najpopularniejsze hasła typu „123456”, „qwerty”, „misiek” czy imiona to dla hakera kilka sekund pracy. Dobre hasła, np. „MlekoZKsiężycowegoDrzewa:)”, mogą być trudne do złamania przez lata.

4. Adres IP – Twoje „miejsce w Internecie”

Adres IP może ujawniać:
- kraj,
- region,
- miasto,
- dostawcę Internetu.

Przykłady pokazują, że nie jesteśmy w sieci tak anonimowi, jak nam się wydaje.

5. RODO w Internecie

RODO chroni nasze dane osobowe: imię, nazwisko, adres, PESEL, a także adres IP.

Pamiętaj:

- Klikając „zgadzam się”, faktycznie wyrażasz zgodę na przetwarzanie danych.
- Masz prawo wiedzieć, jakie dane są zbierane i w jakim celu.
- Możesz zażądać usunięcia swoich danych („prawo do bycia zapomnianym”).

6. Dlaczego warto chronić dane?

Ochrona danych pomaga uniknąć:
- Kradzieży tożsamości – np. zaciągania kredytów na nasze nazwisko.
- Spamu i oszustw – po wycieku danych pojawia się więcej podejrzanych wiadomości.
- Nadmiernej wiedzy o nas – firmy i obce osoby mogą gromadzić informacje o naszych zachowaniach.
- Utraty prywatności – kontrola nad tym, co o nas krąży w sieci.

7. Rozpoznawanie zagrożeń

Phishing – oszustwa na linki i wiadomości

Źródła:
- linki i załączniki,
- SMS-y i telefony,
- fałszywe sklepy i reklamy.

Skutki:
- utrata pieniędzy,
- przejęcie kont (e-mail, Facebook, bank).

Jak się bronić:
- nie klikaj podejrzanych linków,
- weryfikuj wiadomości w innym kanale (np. zadzwoń do nadawcy),
- poproś zaufaną osobę o sprawdzenie,
- zgłaszaj ataki do CERT Polska,

- zastrzeż PESEL po wycieku.

Malware i ransomware – szkodliwe oprogramowanie

Źródła:
- niepewne aplikacje,
- błędy w oprogramowaniu,
- udostępnianie komputera osobom trzecim.

Skutki:
- utrata danych,
- koszty odzyskiwania,
- upublicznienie prywatnych plików.

Jak unikać:
- antywirus,
- firewall,
- aktualizacje,
- pobieranie tylko z pewnych źródeł,
- regularne kopie zapasowe.

Zagrożenia wewnętrzne
- Czasem zagrożeniem jest… człowiek. Celowo lub nieświadomie.

Skutki:
- kradzież danych,
- utrata zaufania i reputacji.

Jak się chronić:

- ograniczenia dostępu do danych,
- blokada nośników zewnętrznych,
- kontrola uprawnień w systemie.

DDoS – ataki na dostępność usług

Skutki:

- brak dostępu do strony,
- przerwy w sprzedaży lub usługach.

Jak unikać:

- narzędzia ochronne typu Cloudflare,
- dodatkowe warstwy weryfikacji (captcha).

8. Higiena cyfrowa – zachowanie równowagi

Internet jest potrzebny, ale łatwo go nadużyć. Warto:

- Wyłączyć powiadomienia nieistotnych aplikacji.
- Wprowadzić zasadę „1 godzina bez ekranu przed snem”.
- Robić cyfrowy detoks – np. jeden dzień bez mediów społecznościowych.
- Sprawdzać statystyki czasu przed ekranem.
- Dbać o ruch i przerwy w ciągu dnia.

9. Fake news – jak je rozpoznawać?

- Sprawdź źródło informacji.
- Zwróć uwagę na datę.
- Porównaj wiadomość z innymi źródłami.
- Uważaj na sensacyjne nagłówki typu „szok!”, „niewiarygodne!”.
- Nie udostępniaj, jeśli nie masz pewności.

10. Kopie bezpieczeństwa

Kopie zapasowe ratują przed utratą danych po awarii, kradzieży lub ataku.

Co warto wiedzieć:

- Jakie dane archiwizować? Dokumenty, zdjęcia, ważne pliki.
- Jak często? Najlepiej regularnie – co tydzień lub po każdej zmianie.

Gdzie?

- lokalnie: pendrive, dysk USB, dysk sieciowy,
- w chmurze: Dropbox, Proton Drive, OneDrive, Google Drive.

Zasada 3-2-1:

3 kopie danych,
2 różne nośniki,
1 kopia poza domem.