Karta Pracy Studenta – Zajęcia 4

Temat: Cyfrowy Sejf – Hasła, Szyfrowanie i Uwierzytelnianie

Cel: Nauczę się tworzyć silne hasła, dowiem się, jak nimi bezpiecznie zarządzać i zrozumiem, czym jest uwierzytelnianie dwuskładnikowe oraz szyfrowanie.

Wprowadzenie: Hasła to klucze do naszego cyfrowego życia. Słabe hasło jest jak zostawienie drzwi do domu na oścież. Dziś nauczymy się, jak wykuć klucze nie do podrobienia i jak zbudować cyfrowy sejf.

Ćwiczenie 1: Test siły hasła (25 min)

Wejdź na stronę wskazaną przez prowadzącego (np. password.kaspersky.com). Pamiętaj, aby nie wpisywać tam swoich prawdziwych haseł! Eksperymentuj z różnymi hasłami i zapisz, ile czasu zajęłoby komputerowi ich złamanie.

Rodzaj hasła (przykład) Szacowany czas złamania

Słowo ze słownika (np. sloneczko)

Popularne hasło z cyframi (np. ania2005)

Hasło z dużą literą i znakiem (np. Zima!)

Hasło z 4 losowych słów (np. biurko most chmura telefon)

Hasło długie i skomplikowane (np. MojeSuperTajneHaslo!123)

Pytanie: Co ma większy wpływ na bezpieczeństwo hasła: jego skomplikowanie czy długość?

Ćwiczenie 2: Menedżer haseł i 2FA – teoria (20 min)

Wysłuchaj prowadzącego i odpowiedz na pytania:

Czym jest menedżer haseł i jaki problem rozwiązuje?

Czym jest uwierzytelnianie dwuskładnikowe (2FA) i dlaczego tak skutecznie chroni nasze konta?

Ćwiczenie 3: Szyfrowanie w praktyce (15 min)

Wejdź na stronę aesencryption.net.

W górnym polu wpisz dowolną, krótką wiadomość (np. "Kryminologia jest ciekawa").

Poniżej wpisz hasło, które będzie "kluczem" do szyfru, np. tajne. Kliknij "Encrypt".

Skopiuj tekst, który pojawił się w dolnym polu. To jest Twoja zaszyfrowana wiadomość.

Odśwież stronę. Wklej zaszyfrowany tekst do dolnego pola, wpisz swoje hasło (tajne) i kliknij "Decrypt".

Co się stało? Czy udało się odzyskać oryginalną wiadomość?

Spróbuj ponownie, ale przy deszyfrowaniu wpisz błędne hasło (np. tajne123). Co się stało tym razem?

Zasada bezpieczeństwa

Stosuj długie i unikalne hasła dla każdego serwisu. Używaj menedżera haseł, aby nimi zarządzać. Wszędzie, gdzie to możliwe, włącz uwierzytelnianie dwuskładnikowe (2FA).