Karta Pracy Studenta – Zajęcia 2

Temat: Anatomia Oszustwa – Phishing i Inżynieria Społeczna

Cel: Nauczę się rozpoznawać próby oszustwa w internecie i dowiem się, jak na nie reagować, aby chronić swoje dane.

Wprowadzenie: Oszuści internetowi często nie "hakują" komputerów, tylko... ludzi. Używają psychologicznych sztuczek, aby skłonić nas do dobrowolnego oddania haseł i pieniędzy. Ta metoda to inżynieria społeczna, a jej najczęstsza forma to phishing.

Ćwiczenie 1: Na tropie oszusta (30 min)

Przeanalizujcie w grupie wiadomości e-mail przedstawione przez prowadzącego. Waszym zadaniem jest znalezienie jak największej liczby "czerwonych flag" – sygnałów ostrzegawczych.

Cecha do sprawdzenia Przykład 1: Co jest nie tak? Przykład 2: Co jest nie tak?

Adres e-mail nadawcy

Błędy językowe, literówki

Forma powitania (np. bezosobowa)

Wzbudzanie presji/strachu

Adres linku (po najechaniu myszką)

Typ załącznika (jeśli jest)

Inne podejrzane elementy

Ćwiczenie 2: Test wiedzy o phishingu (30 min)

Wejdź na stronę: phishingquiz.withgoogle.com

Uważnie czytaj każdą wiadomość i zdecyduj, czy jest prawdziwa (Legitimate), czy fałszywa (Phishing).

Po każdej odpowiedzi przeczytaj wyjaśnienie, aby zrozumieć, na co zwracać uwagę.

Jaki był Twój końcowy wynik? ... / 8

Pytania do dyskusji:

Który przykład z testu był dla Ciebie najtrudniejszy do rozpoznania i dlaczego?

Jak myślisz, dlaczego ludzie wciąż nabierają się na tego typu oszustwa?

Jaka jest najważniejsza zasada, którą należy stosować przy odbieraniu niespodziewanych wiadomości?

Zasada bezpieczeństwa

Zatrzymaj się. Pomyśl. Zweryfikuj. Zanim klikniesz w link lub podasz swoje dane, daj sobie chwilę na analizę. W razie wątpliwości skontaktuj się z daną firmą oficjalnym kanałem.