PROJEKTY SPOŁECZNE
STUDENTÓW
UNIWERSYTETU VIZJA

Cyberświadomy pracownik jako pierwsza linia obrony firmy

- [x] Checklista 1: Czym jest cyberbezpieczeństwo i dlaczego dotyczy każdego?
- [ ] Rozumiem, czym jest cyberbezpieczeństwo i dlaczego jest ważne w mojej pracy.
- [ ] Wiem, że cyberzagrożenia mogą dotyczyć każdego – nie tylko działu IT.
- [ ] Znam przykłady typowych zagrożeń: phishing, złośliwe oprogramowanie, wycieki danych.
- [ ] Zdaję sobie sprawę, że moje codzienne decyzje mają wpływ na bezpieczeństwo firmy.
- [ ] Czuję się odpowiedzialny za ochronę informacji i systemów, z których korzystam.

- [x] Checklista 2: Jak tworzyć i zarządzać bezpiecznymi hasłami?
- [ ] Używam silnych, unikalnych haseł do każdego konta.
- [ ] Moje hasła zawierają małe i wielkie litery, cyfry oraz znaki specjalne.
- [ ] Nie zapisuję haseł na kartkach ani w plikach tekstowych.
- [ ] Korzystam z menedżera haseł do bezpiecznego ich przechowywania.
- [ ] Używam uwierzytelniania dwuskładnikowego (2FA), gdzie to możliwe.

- [x] Checklista 3: Phishing i oszustwa socjotechniczne – jak nie dać się nabrać?
- [ ] Rozpoznaję oznaki wiadomości phishingowych (błędy, podejrzane adresy, presja czasu).
- [ ] Nie klikam w linki ani załączniki z nieznanych źródeł.
- [ ] Weryfikuję nadawcę przed odpowiedzią na nietypowe prośby.
- [ ] Zgłaszam podejrzane e-maile do działu IT.
- [ ] Potrafię zachować ostrożność w rozmowach telefonicznych i osobistych.

- [x] Checklista 4: Praca zdalna – wygoda, która wymaga ostrożności
- [ ] Korzystam wyłącznie ze sprzętu służbowego do pracy zdalnej.
- [ ] Mam zaktualizowane oprogramowanie i system operacyjny.
- [ ] Blokuję ekran komputera, gdy odchodzę od biurka.
- [ ] Korzystam z bezpiecznego połączenia internetowego (VPN, hasło do Wi-Fi).
- [ ] Nie pracuję w miejscach publicznych, gdzie ekran jest widoczny dla innych.

- [x] Checklista 5: Ochrona dokumentów i danych firmowych
- [ ] Nie przechowuję dokumentów firmowych na prywatnym sprzęcie.
- [ ] Udostępniam pliki tylko przez zatwierdzone platformy (np. chmura firmowa).
- [ ] Przestrzegam zasady minimalizacji dostępu – tylko upoważnione osoby mają wgląd.
- [ ] Regularnie usuwam dane, które nie są już potrzebne.
- [ ] Chronię dokumenty przed dostępem osób trzecich (szyfrowanie, hasła).

- [x] Checklista 6: Media społecznościowe – prywatne? Nie do końca
- [ ] Ustawienia prywatności w moich mediach społecznościowych są odpowiednio skonfigurowane.
- [ ] Nie publikuję zdjęć ani informacji mogących ujawnić dane firmowe.
- [ ] Nie udostępniam danych o używanym sprzęcie, systemach ani procesach firmy.
- [ ] Weryfikuję zaproszenia do znajomych i kontaktów (LinkedIn, Facebook).
- [ ] Wiem, że informacje z social mediów mogą być wykorzystywane w atakach socjotechnicznych.

- [x] Checklista 7: Błędy, które powtarzamy najczęściej
- [ ] Nie zapisuję haseł w przeglądarce ani na kartkach.
- [ ] Zawsze blokuję komputer po odejściu od biurka.
- [ ] Sprawdzam załączniki i linki zanim je otworzę.
- [ ] Nie ignoruję komunikatów systemowych i aktualizacji.
- [ ] Unikam instalowania aplikacji z nieznanych źródeł.

- [x] Checklista 8: Co robić, gdy coś pójdzie nie tak?
- [ ] Wiem, jak szybko odłączyć urządzenie od sieci.
- [ ] Potrafię zrobić zrzut ekranu z incydentu i zebrać informacje.
- [ ] Znam procedurę zgłaszania incydentów bezpieczeństwa.
- [ ] Nie próbuję samodzielnie „naprawiać” incydentu – zgłaszam go odpowiednim osobom.
- [ ] Wiem, że szybka reakcja ogranicza skutki incydentu.

- [x] Checklista 9: Dobre nawyki na co dzień
- [ ] Codziennie blokuję ekran komputera po odejściu od stanowiska.
- [ ] Regularnie sprawdzam swoją skrzynkę mailową i usuwam spam.
- [ ] Co miesiąc zmieniam hasła lub przynajmniej je weryfikuję.
- [ ] Raz na kwartał robię kopie zapasowe ważnych plików.
- [ ] Przypominam innym o zasadach cyberbezpieczeństwa – to nasza wspólna odpowiedzialność.