Załącznik nr 2. Terminy oraz opisy modułów Stypendium Santander | Podstawy cyberbezpieczeństwa z Politechniką Poznańską 2023

Terminy szkoleń:

Nr grupy	I moduł	II moduł	III moduł
1	30.06.2023, piątek, godz. 17:00-21:00	01.07.2023, sobota, godz. 10:00-16:00	02.07.2023, niedziela, godz. 10:00-16:00
2	07.07.2023, piątek, godz. 17:00-21:00	08.07.2023, sobota, godz. 10:00-16:00	09.07.2023, niedziela, godz. 10:00-16:00
3	21.07.202, piątek, godz. 17:00-21:00	22.07.2023, sobota, godz. 10:00-16:00	23.07.2023, niedziela, godz. 10:00-16:00
4	28.07.2023, piątek, godz. 17:00-21:00	29.07.2023, sobota, godz. 10:00-16:00	30.07.2023, niedziela, godz. 10:00-16:00
5	04.08.2023, piątek, godz. 17:00-21:00	05.08.2023, sobota, godz. 10:00-16:00	06.08.2023, niedziela, godz. 10:00-16:00
6	11.08.2023, piątek, godz. 17:00-21:00	12.08.2023, sobota, godz. 10:00-16:00	13.08.2023, niedziela, godz. 10:00-16:00
7	18.08.2023, piątek, godz. 17:00-21:00	19.08.2023, sobota, godz. 10:00-16:00	20.08.2023, niedziela, godz. 10:00-16:00
8	25.08.2023, piątek, godz. 17:00-21:00	26.08.2023, sobota, godz. 10:00-16:00	27.08.2023, niedziela, godz. 10:00-16:00
9	01.09.2023, piątek, godz. 17:00-21:00	02.09.2023, sobota, godz. 10:00-16:00	03.09.2023, niedziela, godz. 10:00-16:00
10	08.09.2023, piątek, godz. 17:00-21:00	09.09.2023, sobota, godz. 10:00-16:00	10.09.2023, niedziela, godz. 10:00-16:00
11	15.09.2023, piątek, godz. 17:00-21:00	16.09.2023, sobota, godz. 10:00-16:00	17.09.2023, niedziela, godz. 10:00-16:00
12	22.09.2023, piątek, godz. 17:00-21:00	23.09.2023, sobota, godz. 10:00-16:00	24.09.2023, niedziela, godz. 10:00-16:00
13	29.09.2023, piątek, godz. 17:00-21:00	30.09.2023, sobota, godz. 10:00-16:00	01.10.2023, niedziela, godz. 10:00-16:00
14	06.10.2023, piątek, godz. 17:00-21:00	07.10.2023, sobota, godz. 10:00-16:00	08.10.2023, niedziela, godz. 10:00-16:00
15	13.10.2023, piątek, godz. 17:00-21:00	14.10.2023, sobota, godz. 10:00-16:00	15.10.2023, niedziela, godz. 10:00-16:00
16	20.10.2023, piątek, godz. 17:00-21:00	21.10.2023, sobota, godz. 10:00-16:00	22.10.2023, niedziela, godz. 10:00-16:00

Moduł	Zakres tematyczny
I. Hasła i sieci (4h)	1. Bezpieczne hasła: zasady tworzenia i ćwiczenia 2. Częstość zmiany haseł a bezpieczeństwo 3. Menadżerzy haseł: czym są, prezentacja wybranych narzędzie (KeePass, KeePassXC, Bitwarden, LastPass), ćwiczenia w zakresie konfiguracji i użytkowania 4. Serwisy agregujące dane z wycieków: prezentacja i ćwiczenia 5. Zalety i wady logowania dwuskładnikowego – przedstawienie różnych metod logowania dwuskładnikowego omówienie kluczy u2f (konfiguracja oraz użytkownie) 6. Praktyczny pokaz łamania haseł na żywo 7. Przybliżenie tematyki sieciowej – budowa domowej sieci 8. Rodzaje zabezpieczeń sieci domowych 9. VPN – kto, kiedy i do czego powinien używać: prezentacja i ćwiczenia 10. Zagrożenia wynikające z korzystania z publicznych sieci Wi-Fi 11. Prawidłowe zabezpieczenie domowych urządzeń sieciowych: prezentacja i ćwiczenia 12. Pokaz łamania zabezpieczeń sieci bezprzewodowej
II. Zasady bezpieczeństwa i prawidłowego korzystania z komputera (6h)	1. Zasady bezpiecznego korzystania z komputera – przykłady ataków (phishing, scam, ransomware, socjotechnika, kradzież tożsamości) oraz metody przeciwdziałania 2. Ćwiczenia z rozpoznawania phishingu 3. Oprogramowanie antywirusowe – przedstawienie wybranych rozwiązań 4. Właściwe korzystanie z komputera – omówienie dobrych/złych praktyk i nawyków a. Publikowanie zdjęć z miejsca pracy – dlaczego należy unikać b. Blokowanie ekranu komputera – kiedy należy to robić i dlaczego c. Bezpieczeństwo komunikacji, przedstawienie komunikatów zapewniających szyfrowanie wiadomości, konfiguracja klienta pocztowego pozwalającego na szyfrowanie i podpisywanie wiadomości d. Wskazanie niebezpieczeństw związanych z pracą na koncie z uprawnieniami administratora – ćwiczenia z tworzenia kont użytkowników i zarządzania nimi e. Tworzenie kopii zapasowych: zasady oraz ćwiczenia f. Szyfrowania danych: zasady i ćwiczenia
III. Bezpieczeństwo danych i zagrożenia dla ich bezpieczeństwa (6h)	1. Omówienie zasad prawidłowego przekazywania i przenoszenia danych wraz z przykładami naruszeń bezpieczeństwa 2. Ćwiczenia w zakresie tworzenia zaszyfrowanych dysków przenośnych i sejfów 3. Bezpieczeństwo biznesowe: zagrożenia dla firm, wpływ działań pracownika 4. Uświadomienie zagrożeń związanych z korzystaniem z zewnętrznych serwisów do przekazywania plików 5. Omówienie niebezpieczeństw związanych z podłączaniem niezaufanych urządzeń peryferyjnych 6. Uświadomienie konieczności zabezpieczania użytkowanych systemów i przeprowadzania aktualizacji 7. Ryzyka prawne – omówienie różnych typów licencji oprogramowania, praw autorskich 8. Zagrożenia wynikające z instalowania aplikacji z niezaufanych źródeł, nieautoryzowanych aplikacji, pirackiego oprogramowania

WYMAGANIA W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA:

- komputer/laptop z działającym mikrofonem i kamerą,
- system Windows 10/11,
- dostęp do Internetu z zainstalowaną przeglądarką,
- zainstalowana aplikacja Zoom.

PROWADZĄCY:

mgr inż. Piotr Kontowicz - pracownik Instytutu Sieci Teleinformatycznych Politechniki Poznańskiej. Absolwent kierunku Informatyka na Politechnice Poznańskiej. Zakres zainteresowań obejmuje szeroko pojęte kwestie bezpieczeństwa systemów informatycznych. Opiekun koła naukowego PUTrequest, wraz z którym organizuje otwarte prelekcje mające na celu przybliżenie tematu bezpieczeństwa w sieci zainteresowanym słuchaczom. Aktualnie prowadzone badania obejmują obszar bezpieczeństwa urządzeń Internetu Rzeczy. Wolny czas poświęca na rozwój zainteresowań oraz sport.

mgr inż. Michał Weissenberg- absolwent kierunku Elektronika i Telekomunikacja na Politechnice Poznańskiej aktualnie zatrudniony na stanowisku Asystenta w Instytucie Sieci Teleinformatycznych Politechniki Poznańskiej. Do obszaru jego głównych zainteresowań naukowych należą zagadnienia związane z modelowaniem złożonych systemów teleinformatycznych, Cyberbezpieczeństwo oraz zarządzenie projektami w IT. W ramach pracy na Uczelni prowadzi wykłady oraz zajęcia laboratoryjne z takich przedmiotów jak: Kryminalistyka Cyfrowa, Wojny Cybernetyczne, Przemysłowy Internet Rzeczy, Lokalne Sieci Teleinformatyczne, Systemy Operacyjne oraz Programowanie. Posiada rozliczne certyfikaty oraz ukończył szereg kursów realizowanych m.in. w ramach Prince, Check Point, Palo Alto, Cisco, Huawei, Sans Institute itp. Jest liderem Pakietów Roboczych w dwóch projektach europejskich oraz pracownikiem wielu projektów zarówno na Uczelni jak i przy współpracy z przemysłem w takich obszarach jak edukacja, Cyberbezpieczeństwo oraz wykorzystanie sztucznej inteligencji dla różnych zastosowań.