KURS STACJONARNY

KOMPETENCJE CYFROWE I BEZPIECZEŃSTWO ONLINE

NOWE UMIEJĘTNOŚCI, REALNA PRACA

ORGANIZATOR
InvertArt IFG

Plan dydaktyczny

1. Informacje ogólne:

- **Tryb zajęć:** stacjonarna lub online (zdalna synchroniczna)
- **Forma zajęć:** zajęcia praktyczne
- **Czas trwania:** 16 godzin dydaktycznych (z możliwością rozszerzenia)
- **Liczba miejsc:** -
- **Poziom kursu:** podstawowy lub średniozaawansowany
- **Wymagania wstępne:** brak

2. Cele kursu:

Celem kursu jest rozwinięcie umiejętności cyfrowych niezbędnych we współczesnym środowisku pracy. Uczestnicy nauczą się konfigurować urządzenia mobilne, bezpiecznie korzystać z Internetu i narzędzi Google, a także poznają podstawy sztucznej inteligencji oraz jej praktyczne zastosowania.

3. Dla kogo jest przeznaczony:

Kurs jest przeznaczony dla osób ponownie wchodzących na rynek pracy, które chcą zdobyć lub odświeżyć praktyczne umiejętności cyfrowe, zwiększając tym samym swoją konkurencyjność zawodową.

4. Literatura / materiały

- Materiały własne trenera
- Poradniki online dotyczące bezpieczeństwa cyfrowego
- Dokumentacja Google Workspace i aplikacji mobilnych

Certyfikat ukończenia kursu zgodny ze Standardem Usług Szkoleniowych SUS 3.0 oraz zaświadczenia o ukończeniu kursu.

5. Program kursu:

Moduł 1: Obsługa urządzeń i ustawienia sprzętowe

Cele kształcenia:

- Uczestnik zna podstawowe ustawienia systemu Android i potrafi je skonfigurować.
- Potrafi bezpiecznie połączyć urządzenie z sieciami oraz korzystać z funkcji udostępniania Internetu.
- Rozpoznaje zagrożenia związane z nieautoryzowanym dostępem i niewłaściwym użyciem kodów QR.

Zakres tematyczny:

- Ustawienia systemowe Android
- Łączenie z Wi-Fi i Bluetooth
- Tethering – funkcje i zastosowanie
- Zagrożenia bezpieczeństwa (publiczne sieci, złośliwe aplikacje)
- Skanowanie kodów QR – dobre praktyki
- Aplikacja mObywatel – instalacja i funkcje
- Różnice: podpis kwalifikowany vs. podpis cyfrowy
- **Podstawowe zabezpieczenia urządzeń (PIN, biometryka, aktualizacje, antywirusy)**

Efekty uczenia się:

- Uczestnik potrafi skonfigurować urządzenie mobilne pod kątem użytkowym i bezpieczeństwa.
- Potrafi zainstalować i bezpiecznie korzystać z aplikacji mObywatel.
- Rozumie zasady bezpiecznego korzystania z Internetu mobilnego i kodów QR.

Metody prowadzenia:

- Prezentacja z pokazem na żywo
- Demonstracja funkcji urządzenia
- Ćwiczenia indywidualne (na telefonach/tabletach)
- Dyskusja moderowana

Moduł 2: Przestrzeń robocza Google jako narzędzie pracy i bezpieczeństwa

Cele kształcenia:

- Uczestnik zna funkcje konta Google i potrafi je wykorzystać do organizacji pracy i danych.
- Rozumie zasady synchronizacji i zarządzania urządzeniami.
- Potrafi wykorzystywać narzędzia Google w codziennych zadaniach zawodowych i prywatnych.

Zakres tematyczny:

- Tworzenie i konfiguracja konta Google i Gmail
- Synchronizacja danych, urządzeń i kontaktów
- Zarządzanie bezpieczeństwem konta (logowanie, weryfikacja dwuetapowa)
- Znajdowanie zagubionego telefonu
- Google Drive – organizacja plików
- Google Meet – zasady wideokonferencji
- Dokumenty, Arkusze, Prezentacje Google
- Mapy i Kalendarz – planowanie i lokalizacja
- **Rozpoznawanie podejrzanych e-maili (phishing, załączniki, linki)**
- **Polityka bezpiecznych haseł (menedżery haseł, unikanie słabych kombinacji)**

Efekty uczenia się:

- Uczestnik potrafi założyć i skonfigurować konto Google.
- Potrafi synchronizować dane i korzystać z podstawowych aplikacji Google Workspace.
- Zna metody organizacji i udostępniania danych z użyciem Google Drive.
- **Rozpoznaje próby wyłudzenia danych i stosuje podstawowe zasady ochrony konta.**

Metody prowadzenia:

- Instruktaż krok po kroku (na ekranie trenera)
- Praca z dokumentami w parach/grupach
- Mini-case studies: „rozwiąż problem użytkownika”
- Ćwiczenia indywidualne z kalendarzem, dokumentami i mapami

Moduł 3: Wprowadzenie do sztucznej inteligencji (AI)

Cele kształcenia:

- Uczestnik zna podstawowe pojęcia związane z AI.
- Potrafi korzystać z narzędzi opartych o AI (np. ChatGPT).
- Rozumie zalety i ograniczenia AI w kontekście pracy i życia codziennego.

Zakres tematyczny:

- Wprowadzenie do AI: rodzaje, zastosowanie
- ChatGPT – wprowadzenie, jak działa
- Komendy, przykłady interakcji
- Praktyczne wykorzystanie:
  - wyszukiwanie informacji
  - tworzenie treści (tekst, grafika)
  - analiza danych w Excelu
  - praca z załącznikami
- **Bezpieczeństwo w użyciu AI – krytyczne podejście do treści generowanych**

Efekty uczenia się:

- Uczestnik rozumie, czym jest AI i jak działa w praktyce.
- Potrafi samodzielnie wykonać podstawowe operacje z wykorzystaniem ChatGPT.
- Zna zastosowania AI w pracy biurowej i edukacji.
- **Zachowuje ostrożność przy udostępnianiu danych AI i rozpoznaje potencjalne ryzyka.**

Metody prowadzenia:

- Miniwykład z interaktywnym quizem
- Demonstracja działania AI na żywo
- Warsztat praktyczny (tworzenie treści)
- Praca w grupach nad zadaniami A

Moduł 4: Bezpieczeństwo cyfrowe – praktyczne aspekty

Cele kształcenia:

- Uczestnik zna najczęstsze zagrożenia w sieci i sposoby ich unikania.
- Potrafi ocenić wiarygodność stron i wiadomości.
- Rozumie zasady bezpiecznego korzystania z komputera i telefonu.

Zakres tematyczny:

- Phishing: jak rozpoznać fałszywe e-maile i strony internetowe
- Podejrzane załączniki i linki – analiza przykładów
- Certyfikaty bezpieczeństwa SSL – jak sprawdzić stronę
- Polityka tworzenia i przechowywania haseł (2FA, menedżery haseł)
- Bezpieczne przeglądanie stron internetowych – jak rozpoznać oszustwo
- Aplikacje zabezpieczające: firewalle, antywirusy, blokery reklam
- Szyfrowanie danych i komunikacji (SSL, komunikatory z E2EE)
- Bezpieczeństwo na urządzeniach mobilnych (aktualizacje, blokady, lokalizacja)

Efekty uczenia się:

- Uczestnik potrafi zidentyfikować i zareagować na próby oszustw cyfrowych.
- Zna podstawowe narzędzia ochrony komputera i telefonu.
- Stosuje zasady higieny cyfrowej na co dzień.

Metody prowadzenia:

- Analiza przykładów phishingu
- Ćwiczenia praktyczne z identyfikacją zagrożeń
- Miniwarsztaty z konfiguracji zabezpieczeń
- Dyskusja i wymiana doświadczeń

Moduł 5: Zajęcia praktyczne

Cele kształcenia:

- Utrwalenie nabytej wiedzy poprzez praktyczne zastosowanie narzędzi.
- Zwiększenie pewności siebie w korzystaniu z technologii cyfrowych.

Zakres tematyczny:

- Scenariusze z życia codziennego i pracy (np. organizacja wydarzenia, plan podróży, udostępnienie dokumentów, rozmowa online)
- Synchroniczne wykorzystanie kilku narzędzi (Google + AI)
- Rozwiązywanie problemów: co zrobić, gdy…?
- **Symulacja sytuacji niebezpiecznych (podejrzany e-mail, fałszywa strona, brak dostępu do konta)**

Efekty uczenia się:

- Uczestnik potrafi zastosować zdobytą wiedzę w realnych sytuacjach.
- Samodzielnie rozwiązuje proste problemy techniczne.
- Umie połączyć kilka narzędzi cyfrowych w celu realizacji zadania.
- **Reaguje świadomie na cyfrowe zagrożenia.**

Metody prowadzenia:

- Praca projektowa (indywidualna lub zespołowa)
- Symulacje sytuacyjne
- Analiza przypadków (case studies)
- Omówienie z trenerem i wzajemna ewaluacja

6. Podsumowanie efektów uczenia się (całościowych):

Po zakończeniu szkolenia uczestnik:

- Potrafi bezpiecznie obsługiwać urządzenia mobilne.
- Rozumie zasady ochrony danych i kont online.
- Wykorzystuje podstawowe narzędzia Google i AI w pracy/zadaniach prywatnych.
- Potrafi samodzielnie rozwiązywać typowe problemy cyfrowe.
- Zna podstawowe zagrożenia cyfrowe i umie ich unikać.
- Rozpoznaje próby phishingu i stosuje dobre praktyki bezpieczeństwa cyfrowego.

7. Zakres wsparcia pokursowego:

- Każdy uczestnik kursu ma możliwość skorzystania z bezpłatnego wsparcia pokursowego przez okres 1 miesiąca od zakończenia szkolenia.
- W ramach wsparcia uczestnicy mogą kontaktować się mailowo lub telefonicznie z trenerem w celu wyjaśnienia wątpliwości, doprecyzowania materiałów lub uzyskania wskazówek do dalszego rozwoju.

8. System oceniania i zaliczenia

Kurs doszkalający – brak egzaminów i zaliczeń. Ocena osiągnięć uczestników oparta na aktywności, pracy warsztatowej i realizacji ćwiczeń praktycznych.

3 wykładowców z dziedziny informatyki, analityki i marketingu

Kursy prowadzone przez praktyków