Co-funded by the Erasmus+ Programme of the European Union

Scenariusz 1
Technologia i IT (np. materiały, procesy, organizacja produkcji, IT)

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nazwa Partnera: Foro de Formacion y Ediciones

Open Educational Resources

CC BY NC SA

Niniejszy materiał powstał w ramach projektu BRAIN "BringING STRM into Active AgING" (UMOWA GRANTOWA 2020-1-PL01-KA204-081805). Projekt ten został sfinansowany przy wsparciu Komisji Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autora i Komisja Europejska nie ponosi odpowiedzialności za umieszczoną w niej zawartość merytoryczną.

Akademia WSEI LUBLIN

Mine Vaganti NGO

FFE Foro de Formación y Ediciones S.L.

HORIZONT X PROCONSULT

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nazwa Partnera: Foro de Formacion y Ediciones

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

Co-funded by the
Erasmus+ Programme
of the European Union

Ice Breaker

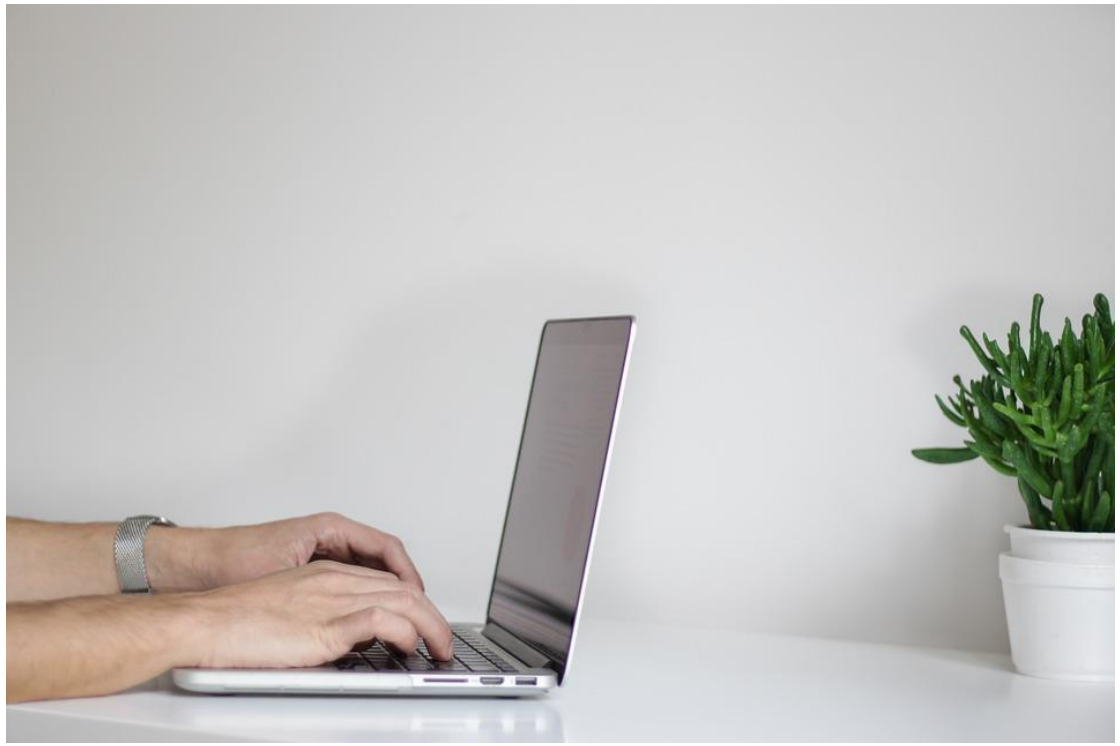
Stańmy w kręgu. Następnie zacznijmy od wypowiedzenia swojego imienia i słowa związanego z IT, które zaczyna się na tę samą literę. Np. Adam Aplikacja, Bartek Banner, Celine Ciasteczka, Darek Domena, etc....

Następnie kolejna osoba podaje swoje imię i nazwisko. Następnie trzecia osoba podaje swoje imię, imię drugiej osoby i imię pierwszej osoby oraz słowo związane z informatyką. Następnie przechodzi się w dół linii, tak aby ostatnia osoba musiała zrobić to samo ze wszystkimi w grupie. Można grać w różne warianty tej gry, ale jest to świetny sposób na poznanie się grupy i imion.

Co-funded by the
Erasmus+ Programme
of the European Union

Wprowadzenie

Internet stał się czynnikiem determinującym rozwój dzisiejszego społeczeństwa. Został wykorzystany jako główny środek interakcji ludzi i komputerów, wymiany informacji i promowania szybkiego przekazywania doświadczeń i wiedzy niezależnie od położenia geograficznego.



Co-funded by the
Erasmus+ Programme
of the European Union

Wprowadzenie

Od swoich początków w latach sześćdziesiątych XX wieku do dnia dzisiejszego Internet jest podstawowym składnikiem rozwoju technologicznego, edukacji, komunikacji, medycyny, nauki, sztuki i praktycznie wszystkich dyscyplin i zawodów w zglobalizowanym świecie. Chociaż początkowo był przeznaczony do użytku wojskowego, jego zalety zostały radykalnie rozszerzone na praktycznie każdą dziedzinę.

Co-funded by the
Erasmus+ Programme
of the European Union

Wprowadzenie

Handel to kolejna przestrzeń, w której Internet zdołał wywrzeć pozytywny wpływ, zarówno na sprzedawców, jak i kupujących. Duże supermarkety i sieci sklepów, oprócz posiadania swoich punktów sprzedaży, opracowały platformy do sprzedaży online, dzięki czemu udało im się obniżyć niektóre koszty, na przykład koszty personelu sprzedaży i lokalizacji. Handel elektroniczny umożliwia firmom przekraczanie granic bez konieczności fizycznego przebywania w jednym miejscu. Doprowadziło to do zwiększenia wydajności biznesowej i otworzyło nowe możliwości handlu.

Co-funded by the
Erasmus+ Programme
of the European Union

Wprowadzenie

Ponadto handel elektroniczny nie jest już zarezerwowany wyłącznie dla dużych marek. Wszechstronność tego biznesu pozwoliła małym i średnim firmom również na rozpoczęcie działalności, a sieci społecznościowe wniosły interesujący wkład w tę dynamikę.

Co-funded by the
Erasmus+ Programme
of the European Union

Wprowadzenie

Internet jest zatem dziś globalnym środkiem komunikacji, który pozwala nam na interakcję w różnych przestrzeniach. Od komunikowania się za pośrednictwem połączenia wideo lub czatu z inną osobą oddaloną o tysiące kilometrów, dostępu do wysokiej jakości edukacji w instytutach i na uniwersytetach w różnych częściach świata, kupowania produktów lub usług online, czytania gazet, czasopism lub książek, słuchania muzyki, oglądania filmów lub interakcji w sieciach społecznościowych. To tylko kilka z wielu możliwości, jakie nam oferuje.

Co-funded by the
Erasmus+ Programme
of the European Union

Wprowadzenie

To w naszych rękach leży racjonalne i obiektywne wykorzystanie narzędzia tak potężnego, jak byśmy tego chcieli.

Sposób, w jaki internet ewoluował od czasu jego wynalezienia, jest fantastyczny i pozwolił nam zobaczyć, że będzie on nadal ewoluował tak szybko, że nie przestanie nas zadziwiać.

Co-funded by the
Erasmus+ Programme
of the European Union

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.
Flipchart z fałszywymi wiadomościami

Materiały

telefony/tablety/laptopy z dostępem do Internetu, rzutnik multimedialny, długopisy, markery, flipchart, karteczki samoprzylepne, arkusze papieru A4

Kierunki

Prowadzący zapisuje termin "FAKE NEWS" na środku flipcharta. Rozdaj uczestnikom 3 karteczki samoprzylepne i poproś ich o zapisanie swoich skojarzeń z tym terminem i przyklejenie ich do flipcharta. Przeczytaj zapisane skojarzenia, grupując je razem, jeśli to możliwe. Omów każde skojarzenie i porównaj je z definicją fake news (załącznik poniżej).

Dodatek

Termin "fałszywe wiadomości"

Fake news to "nieprawdziwe, fałszywe wiadomości, zwykle rozpowszechniane przez tabloidy w celu wywołania sensacji lub zniesławienia kogoś (zwykle polityka)". Słownik Cambridge Dictionary podaje, że są to (w tłumaczeniu) "fałszywe historie, które wydają się być wiadomościami, rozpowszechniane w Internecie lub za pośrednictwem innych mediów, zwykle tworzone w celu wpłynięcia na poglądy polityczne lub jako żart".

Co-funded by the
Erasmus+ Programme
of the European Union

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.
Flipchart z fałszywymi wiadomościami

Termin "fake news" jest neologizmem i trudno go ująć w ramy definicyjne. Oznacza wiadomości medialne, które nie są ani prawdziwe, ani fałszywe w tym samym czasie i opierają się na dezinformacji, często zawierając prawdziwe elementy. Fake newsy są zwykle oparte na dezinformacji lub żartach, często zawierających prawdziwe elementy. Fake newsy mogą udawać prawdziwe informacje, artykuły, posty w mediach społecznościowych, memy itp. Mogą być tworzone w różnych intencjach, od oszustwa, przez narzędzia propagandy, tworzenie sensacji, po żart.
Fake news to "manipulacja faktami, chętnie wykorzystywana przez dziennikarzy, których celem podczas przygotowywania publikacji jest wzbudzenie jak największego zainteresowania tematem, a nie jego zgodność z rzeczywistością".
Internet jest obecnie najpopularniejszym źródłem komunikacji. Do publikowanych w nim treści należy jednak podchodzić z ostrożnością. Badanie IAB "Dezinformacja w sieci. Analiza wiarygodności kanałów informacyjnych" wynika, że liderem w rozpowszechnianiu fake newsów są media społecznościowe. Na drugim miejscu znajdują się portale internetowe.

Rodzaje fałszywych wiadomości:
Całkowita nieprawda - podane informacje są sfabrykowane, sprzeczne,
prawda jest dyskusyjna - fakty przedstawiane są wybiórczo lub w odpowiednim kontekście, co skutkuje wprowadzeniem odbiorcy w błąd,
manipulacja cytatem - wypowiedź jest umieszczana w odpowiednim kontekście lub usuwane są zdania lub ich fragmenty, co zmienia sens wypowiedzi, a w konsekwencji wspiera określoną tezę.

Co-funded by the
Erasmus+ Programme
of the European Union

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.
Fałszywe wiadomości wideo

- zwracać uwagę na to, czy użyte zdjęcia są osadzone w rzeczywistym kontekście
zweryfikować wiarygodność strony internetowej - czy adres URL jest poprawny i prowadzi do właściwej, prawdziwej strony internetowej
- sprawdzić datę i aktualność informacji
- zweryfikować autora - czy jest wiarygodny, jakie są jego cele i intencje, czy publikował już inne materiały online
- sprawdzić, czy obrazy nie wyglądają dziwnie lub czy nie zostały zmanipulowane - można to zrobić np. za pomocą opcji odwrotnego wyszukiwania obrazów dostępnej w wyszukiwarkach

FAKE NEWSY - ZASADY OGÓLNE:
Dominują w nich obrazy/zdjęcia i krótki tekst.
Przekaz jest silnie nacechowany emocjonalnie: wykorzystuje mowę nienawiści, pokazuje brutalne, poruszające sceny i obrazy.
Często udaje, że jest z pierwszej ręki.
Używają ogólnie znanych prawd i przekonań.
Często pokazują półprawdy, przeinaczają fakty w taki sposób, że nie wiadomo, gdzie zaczyna się weryfikowana informacja, a gdzie kończy. Opierają się na założeniu, że częściowa prawda potwierdza prawdę całości.
Czasami opisują prawdziwe wydarzenia, ale zmieniają ich kontekst.
Prawie zawsze zawierają one zdjęcia lub filmy, które pomagają szybko zwiększyć zasięg.
Nie informują, że podane informacje mogą nie być pewne.
Unikają niuansów i różnych punktów widzenia.

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Co możesz mi powiedzieć o prywatności online?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Definicja prywatności online to poziom ochrony prywatności, jaki dana osoba ma podczas połączenia z Internetem. Obejmuje ona poziom bezpieczeństwa online dostępny dla danych osobowych i finansowych, komunikacji i preferencji. Prywatność w Internecie jest ważna, ponieważ daje kontrolę nad tożsamością i danymi osobowymi. Bez tej kontroli każdy, kto ma zamiar i środki, może manipulować twoją tożsamością, aby służyć swoim celom, niezależnie od tego, czy sprzedaje ci droższe wakacje, czy kradnie twoje oszczędności.

Co-funded by the
Erasmus+ Programme
of the European Union

Znaczenie haseł

Hasła są kluczem, który otwiera drzwi do korzystania ze wszystkich naszych usług. Jeśli nasze hasła zostaną ujawnione, cyberprzestępcy będą mogli wykorzystać je, aby wejść do nich i podszyć się pod nas, dokonać płatności w naszym imieniu, zmienić lub uzyskać dostęp do innych rodzajów informacji lub innych osób, między innymi, dlatego zaleca się podjęcie szeregu środków w celu naszej ochrony.

Co-funded by the
Erasmus+ Programme
of the European Union

Znaczenie haseł

Hasło musi być silne i składać się z co najmniej 8 znaków:

-Wielkie litery (A, B, C...)

-Liczby (1, 2, 3...)

-Małe litery (a, b, c...)

-Znaki specjalne ($, &, #...)

Ważne jest, aby używać haseł, które nie są łatwe do odgadnięcia. Na przykład: "123456789", "qwerty", "aaaaa", imiona własne, daty urodzin itp.

Co-funded by the
Erasmus+ Programme
of the European Union

Znaczenie haseł

Hasła nie powinny być nikomu udostępniane, hasło musi należeć wyłącznie do użytkownika, który je utworzył i być używane tylko przez niego. Udostępnianie go sprawi, że będziemy narażeni na niebezpieczeństwo, a tym bardziej, jeśli sposobem, w jaki je udostępniamy, jest sieć komunikacyjna, taka jak (WhatsApp, Telegram, Facebook), ponieważ informacje są przechowywane na serwerach tych usług.

Co-funded by the
Erasmus+ Programme
of the European Union

Znaczenie haseł

Staraj się unikać używania tego samego hasła do wszystkich usług za wszelką cenę, ponieważ jeśli cyberprzestępca zdobędzie to hasło, będzie mógł uzyskać dostęp do wszystkich z nich.

Co-funded by the
Erasmus+ Programme
of the European Union

Znaczenie haseł

Hasła należy zmieniać okresowo, a nie na zawsze. Dobrym sposobem na zapamiętanie, kiedy powinniśmy zmienić nasze hasła, jest pamiętanie o porach roku. Hasło zmienia się dla każdej stacji, więc zawsze będzie aktualizowane co 3 miesiące.

Co-funded by the
Erasmus+ Programme
of the European Union

Znaczenie haseł

Jako rada na dużą liczbę haseł, które musiałyby być zarządzane w przypadku posiadania jednego na usługę, istnieją menedżery haseł, które ułatwiają życie, jeśli chodzi o zapamiętywanie ich wszystkich.

Co-funded by the
Erasmus+ Programme
of the European Union

Uwierzytelnianie dwuetapowe

Czasami posiadanie hasła nie wystarcza, bez względu na to, jak silne może ono być, lub po wykonaniu wszystkich poprzednich kroków.

Cyberprzestępcy mogą zdobyć je za pomocą różnych technik, takich jak "phishing" lub niektóre wirusy zaprojektowane do tego celu, które zobaczymy później.

Co-funded by the
Erasmus+ Programme
of the European Union

Uwierzytelnianie dwuetapowe

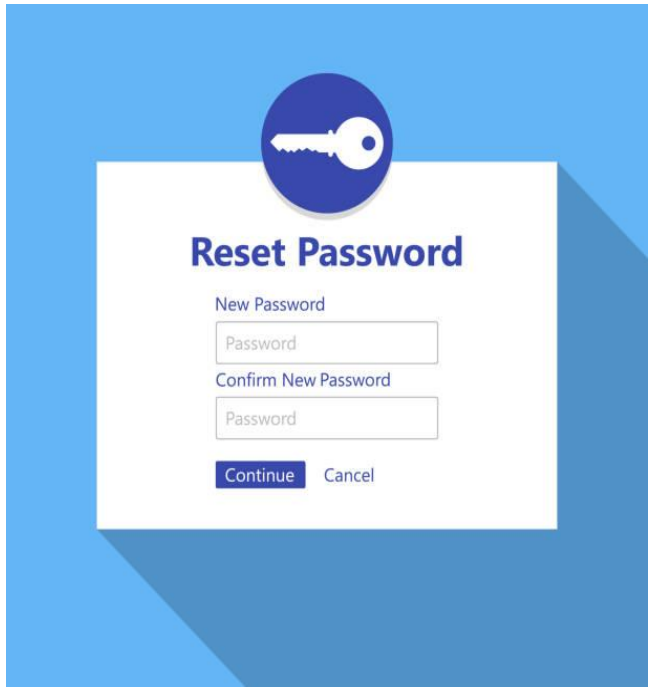
Dlatego wiele usług oferuje już uwierzytelnianie dwuetapowe. Dzięki tej metodzie użyjemy naszego hasła do usługi w normalny sposób, a następnie zostaniemy poproszeni o dodanie drugiego kodu.

Najczęstszym sposobem na otrzymanie tego kodu jest otrzymanie go jako SMS na nasz smartfon, chociaż może to być również połączenie telefoniczne za pośrednictwem automatu lub posiadanie aplikacji serwisowej, która aktywnie zmienia kody co 5 minut.

Co-funded by the
Erasmus+ Programme
of the European Union

Uwierzytelnianie dwuetapowe

Najwyraźniej usługa musiała zostać wcześniej skonfigurowana, aby połączyć z nią nasz smartfon i otrzymywać kody. W ten sposób, nawet jeśli cyberprzestępca uzyska twoje hasło, nie będzie w stanie uzyskać dostępu do usługi, ponieważ będzie potrzebował tego drugiego kodu, aby wejść.



Jeśli w dowolnym momencie dojdzie do próby uzyskania dostępu do konta, ponieważ otrzymałeś podwójny kod uwierzytelniający i to nie byłeś ty, powinieneś rozważyć zmianę hasła, ponieważ jest bardzo prawdopodobne, że nie jest to już bezpieczny klucz.

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czym jest szpiegowanie / podsłuchiwanie?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Gdy jesteś online, jesteś szpiegowany przez wiele trackerów w różnych celach. Trackery prowadzą rejestr historii wyszukiwania i śledzą wszystkie działania użytkownika online za pomocą różnych środków. Daje im to jasny obraz tego, kim jesteś i jakie są twoje zainteresowania, co stanowi naruszenie polityki prywatności online i czyni cię własnością publiczną. W większości przypadków śledzenie to służy wyłącznie celom reklamowym i umożliwia reklamodawcom wyświetlanie reklam zgodnie z gustem i zainteresowaniami użytkownika. Czasami jednak informacje te są wykorzystywane przez cyberprzestępców do przeprowadzania nieautoryzowanych i nielegalnych działań zagrażających twojemu istnieniu online.

Co-funded by the
Erasmus+ Programme
of the European Union

Dane osobowe

Przed podaniem swoich danych osobowych należy przeanalizować, kto o nie prosi? Do czego potrzebne są te informacje?

Informacje, które będziesz musiał podać, na przykład w celu zawarcia umowy rachunku bankowego, nie są takie same jak w przypadku subskrypcji witryny zakupów online. W pierwszym przypadku wymagane informacje będą znacznie obszerniejsze, ale w drugim wystarczy imię, nazwisko, adres dostawy, dane rozliczeniowe i metoda płatności.

Jeśli ktoś prosi o podanie danych osobowych, należy poinformować o celu, w jakim będą one wykorzystywane, a także o sposobie ich przetwarzania oraz o tym, jak długo będą przechowywane.

Warto wiedzieć, jak korzystać ze swoich praw (dostęp, sprostowanie, sprzeciw, ograniczenie przetwarzania i przenoszenie).

Co-funded by the
Erasmus+ Programme
of the European Union

Phishing

Phishing to kradzież tożsamości usługi lub firmy w celu oszukania ludzi. Na przykład możesz otrzymać wiadomość e-mail z prośbą o aktualizację danych bankowych, ponieważ Twoja karta kredytowa wkrótce straci ważność. W tej wiadomości e-mail znajduje się link umożliwiający dostęp do tej usługi. Po jego otwarciu pojawia się strona internetowa będąca kopią oryginału, użytkownik aktualizuje dane swojego konta bankowego i w tym momencie pada ofiarą oszustwa.

Co-funded by the
Erasmus+ Programme
of the European Union

Phishing

Wskazówki, jak uniknąć bycia ofiarą

1. Należy uważać na wiadomości e-mail, które wydają się być wiadomościami od podmiotów bankowych lub znanych usług:

a. Problemy techniczne podmiotu

b. Problemy z bezpieczeństwem konta użytkownika.

c. Zalecenia dotyczące bezpieczeństwa w celu uniknięcia oszustw.

d. Zmiany w polityce bezpieczeństwa jednostki

e. Promocja nowych produktów

f. Kupony rabatowe, nagrody lub upominki

g. Nieuchronne zaprzestanie świadczenia usługi lub jej dezaktywacja.

Co-funded by the
Erasmus+ Programme
of the European Union

Phishing

2. Bądź podejrzliwy, jeśli w tekście występują błędy gramatyczne.

3. Otrzymywanie anonimowych wiadomości zaadresowanych do "Szanowny kliencie" lub "Powiadomienie użytkownika" jest sygnałem, który powinien Cię ostrzec.

4. Jeśli wiadomość zmusza do podjęcia decyzji w ciągu kilku godzin, jest to zły znak. Bezpośrednio kontrastuje to z tym, czy pilność jest rzeczywista, czy nie, z obsługą za pośrednictwem innych kanałów.

5. Sprawdź, czy tekst linku jest zgodny z adresem, na który wskazuje.

6. Renomowana usługa będzie używać własnych domen dla firmowych adresów e-mail. Jeśli otrzymujesz wiadomości ze skrzynki pocztowej typu @gmail.com lub @hotmail.com, nie jest to dobry znak.

Co-funded by the
Erasmus+ Programme
of the European Union

Phishing

Co należy zrobić w przypadku wykrycia phishingu?

1. Pod żadnym pozorem nie odpowiadaj na te wiadomości e-mail. Jeśli masz wątpliwości, zwróć się bezpośrednio do firmy lub usługi, którą reprezentuje.

2. Nie korzystaj z linków podanych w wiadomości ani nie pobieraj żadnych załączonych dokumentów.

3. Usuń wiadomość i ostrzeż kontakty o oszustwie.

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Co wiesz o niewłaściwym zarządzaniu informacjami?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

W Internecie istnieje wiele witryn, które wymagają podania danych osobowych użytkownika w celu uzyskania dostępu do swoich usług. Witryny te często przechowują pliki cookie i zapisują dane osobowe użytkownika, a następnie wykorzystują je do różnych celów. W większości przypadków informacje te nie są szyfrowane i każdy może uzyskać do nich dostęp. Takie niewłaściwe obchodzenie się z danymi osobowymi może prowadzić do poważnych konsekwencji. Współczesny trend bankowości elektronicznej i portali e-biznesowych zwielokrotnił ryzyko związane z prywatnością online. Udostępniając swoje dane bankowe i ważne pliki w Internecie, torujesz drogę włamywaczom i narażasz się na ataki cyberprzestępców.

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Dwie prawdy i jedno kłamstwo

Materiały

Telefony/tablety/laptopy z dostępem do Internetu, projektor, kartki papieru, długopisy, kartony

Kierunki

Gra Dwie prawdy i jedno kłamstwo. Uczestnicy otrzymują trzy stwierdzenia. Dwa z nich będą prawdziwe, a jedno będzie kłamstwem. Uczestnicy muszą zidentyfikować kłamstwo.

Dodatek

Uczestnicy otrzymują trzy stwierdzenia. Dwa z nich będą prawdziwe, a jedno będzie kłamstwem. Uczestnicy muszą zidentyfikować kłamstwo. Wszystkie stwierdzenia będą związane z tematyką internetową.

Zakupy online:

1. Karta kredytowa to jeden z najniebezpieczniejszych sposobów płacenia za towary online
2. Nigdy nie należy wprowadzać danych płatności na stronie, chyba że po HTTP znajduje się litera S.
3. Jeśli nie masz karty kredytowej lub debetowej, PayPal jest dobrą alternatywą do płacenia za towary online

Złośliwe oprogramowanie:

1. Złośliwe oprogramowanie to rodzaj wirusa komputerowego
2. Robak komputerowy często wykorzystuje komputery z przestarzałym oprogramowaniem
3. Ważnym krokiem w celu ochrony przed oprogramowaniem ransomware jest regularne tworzenie kopii zapasowych

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Dwie prawdy i jedno kłamstwo

Phishing:

1. Jeśli wiadomość e-mail zwraca się do użytkownika jako "klient", należy zachować szczególną ostrożność
2. Oszustwo phishingowe, które zna dane osobowe istotne dla odbiorcy, nazywane jest atakiem typu spear-phishing
3. Kliknięcie linku w wiadomości e-mail jest w porządku, jeśli wiadomość pochodzi z banku, w którym masz konto

Prywatność w mediach społecznościowych:

1. Jedynym zalecanym domyślnym poziomem prywatności są TYLKO znajomi i rodzina.
2. Instalowanie aplikacji społecznościowych (Facebook, Instagram, Twitter...) może dać zupełnie obcym osobom dostęp do pewnych informacji na Twój temat.
3. Jeśli zablokuję kogoś na Facebooku lub Twitterze, ta osoba nie będzie mogła zobaczyć niczego, co robię lub publikuję na moim koncie

Oszustwo na Facebooku:

1. Dodanie nieznajomego na Facebooku daje mu dostęp do mojego komputera
2. Dodanie nieznajomego na Facebooku może narazić moich znajomych na niebezpieczeństwo
3. Dodanie nieznajomego na Facebooku może prowadzić do kradzieży tożsamości

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Dwie prawdy i jedno kłamstwo

Oszustwa e-mailowe:

1. Oszustwa związane z opłatami zaliczkowymi polegają na nakłonieniu ofiary do wysłania pieniędzy w zamian za obietnicę znacznie większego zwrotu
2. Otwarcie załącznika wiadomości e-mail zawierającego dokument programu Word może być niebezpieczne
3. Najlepszym sposobem postępowania w przypadku otrzymania wiadomości e-mail z oszustwem typu "nigeryjski książę" jest odpisanie i powiedzenie, aby przestali do mnie wysyłać e-maile.

Ransomware

1. Jeśli oprogramowanie ransomware zainfekuje mój komputer, niezawodny i renomowany program antywirusowy może je usunąć.
2. Antywirus może odwrócić skutki działania oprogramowania ransomware
3. Ransomware to jedno z najbardziej rozpowszechnionych zagrożeń internetowych w 2017 i 2018 r.

Po podaniu tych przykładów uczestnicy będą musieli wymyślić co najmniej jeszcze jeden. Następnie spróbują dowiedzieć się, które stwierdzenie jest nieprawidłowe.

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Dwie prawdy i jedno kłamstwo

Odpowiedzi:

1

3

3

1

1

3

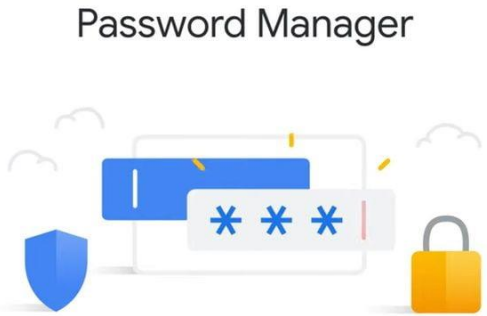
2

Co-funded by the
Erasmus+ Programme
of the European Union

Menedżery haseł

Posiadanie darmowej wersji świetnego menedżera haseł

jest zawsze lepsza niż jej brak.



Co-funded by the
Erasmus+ Programme
of the European Union

Menedżery haseł

1Password: świetna opcja dla całej rodziny ➞ https://cnews.link/get-1password_7/

==========

Wady bezpłatnego planu:

Sprawdza, czy hasła nie zostały złamane.

Wsparcie e-mail 24/7

Nieograniczona liczba użytkowników dla jednego konta

Opcja lokalnej pamięci masowej

Ograniczenia planu bezpłatnego:

Brak obsługi czatu na żywo

Brak aktualizacji hasła jednym kliknięciem

Co-funded by the
Erasmus+ Programme
of the European Union

Menedżery haseł

NordPass: najbardziej wszechstronny menedżer haseł ➞ https://cnews.link/get-nordpass_46/

==========

Zalety bezpłatnego planu:

Szyfrowanie nowej generacji

Nieograniczone przechowywanie haseł w sejfie

Uwierzytelnianie wieloskładnikowe

Łatwe transfery do skarbca

Obsługa klienta przez czat na żywo

Ograniczenia planu bezpłatnego:

Większość funkcji znajduje się za paywallem.

❌ Brak dodatków dla większej liczby przeglądarek

Co-funded by the
Erasmus+ Programme
of the European Union

Menedżery haseł

Dashlane: bezpieczne i usprawnione doświadczenie ➞ https://cnews.link/get-dashlane_39/

==========

Bezpłatny plan:

Współdzielenie hasła z 5 użytkownikami

Doskonała reputacja

Obsługa 2FA

Przechowywanie do 50 haseł

Ograniczenia planu bezpłatnego:

Maksymalna ilość przechowywanych haseł wynosi 50.

Brakuje wersji na iOS

Ogranicza użytkownika do jednego urządzenia

Co-funded by the
Erasmus+ Programme
of the European Union

Menedżery haseł

Keeper: wyjątkowe narzędzie do zarządzania hasłami ➞ https://cnews.link/get-keeper_10/

==========

Wady bezpłatnego planu:

Świetna kompatybilność

Wiele opcji 2FA

Aplikacja do prywatnych wiadomości

Ograniczenia planu bezpłatnego:

Niewiele opcji eksportu

Co-funded by the
Erasmus+ Programme
of the European Union

Menedżery haseł

RoboForm ➞ https://cnews.link/get-roboform_10/

==========

Wady bezpłatnego planu:

Nieograniczone przechowywanie haseł w sejfie

Wygodna aktualizacja słabszych haseł

Udostępnianie hasła przez e-mail

Monitorowanie dark web

Ograniczenia planu bezpłatnego:

Mógłby być bardziej przyjazny dla użytkownika

Czat na żywo tylko dla płatnych użytkowników

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czy możesz mi powiedzieć, czym jest kradzież tożsamości i w jaki sposób jest przeprowadzana? (phishing, złośliwe oprogramowanie, pharming, porzucone komputery i telefony...)

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Kradzież tożsamości i oszustwo tożsamości to terminy używane w odniesieniu do wszystkich rodzajów przestępstw, w których ktoś bezprawnie uzyskuje i wykorzystuje dane osobowe innej osoby w sposób, który wiąże się z oszustwem lub podstępem, zazwyczaj w celu uzyskania korzyści ekonomicznych.

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Z kim rozmawiasz?

Materiały

Telefony/tablety/laptopy z dostępem do Internetu, projektor, kartki papieru, długopisy, kartony

Kierunki

Ta gra ma symulować sytuację, w której rozmawiasz z kimś przez Internet i tak naprawdę nie wiesz, kto jest po drugiej stronie ekranu, czy mówi prawdę, czy nie, czy też udaje kogoś innego w ukrytym celu.

Każdy uczestnik ma przypisaną postać, a inni muszą dowiedzieć się, kim są. Ale niektóre z nich nie będą zgodne z prawdą. Ci, którzy nie mają postaci, w parach lub grupach (w zależności od uczestników) muszą odgadnąć za pomocą pytań, kim jest osoba, z którą rozmawiają (ta, która ma przypisaną rolę). Gra jest przeznaczona dla 15-osobowej grupy, w której 5 osób ma postać, a 10 w parach będzie próbowało dowiedzieć się, kim jest postać pozostałych 5 osób i czy jest prawdziwa, czy nie. Gra będzie rozgrywana w dwóch grupach po 15 uczestników.

Osoby z przypisanymi postaciami muszą odpowiadać na pytania tak, jakby były tymi postaciami. Pary będą wiedzieć, że możliwe jest, że niektóre postacie nie są tymi, za które się podają. Pięć par będzie zadawać sobie nawzajem pytania przez kilka minut i zmieniać się. Po zakończeniu rozmowy każda para musi powiedzieć, kim ich zdaniem jest każda postać i czy naprawdę jest tym, za kogo się podaje.

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Z kim rozmawiasz?

Postać 1:

20-letni chłopak. Lubi piłkę nożną, wychodzić z przyjaciółmi i chodzić na koncerty.

Postać 2:

25-letnia dziewczyna. Gra w drużynie rugby i lubi sporty górskie. Lubi zwierzęta i ma psa.

Postać 3: (Fałszywa postać)

Odpowiedzi jako: 18-letnia dziewczyna. Uczestniczka studiów biologicznych. Lubi przyrodę i rośliny. Jest fanką Rosalii.

Właściwie to jest: 39-letni mężczyzna.

Postać 4: (Fałszywa postać)

Odpowiedzi jako: 23-letni chłopak. Lubi muzykę rockową i surfing. Zwykle gra w gry wideo.

Właściwie to jest: 47-letni mężczyzna.

Postać 5:

27-letni chłopak. Gra w tenisa stołowego. Lubi zwierzęta i ma dwa koty. Pracuje jako grafik.

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Z kim rozmawiasz?

Co się dzieje?

Ta gra ma symulować sytuację, w której rozmawiasz z kimś przez Internet i tak naprawdę nie wiesz, kto jest po drugiej stronie ekranu, czy mówi prawdę, czy nie, czy też udaje kogoś innego w ukrytym celu.

Każdy uczestnik ma przypisaną postać, a inni muszą dowiedzieć się, kim są. Ale niektóre z nich nie będą zgodne z prawdą.

Osoby z przypisanymi postaciami muszą odpowiadać na pytania tak, jakby były tymi postaciami.

Co-funded by the
Erasmus+ Programme
of the European Union

Scenariusz 2
Technologia i IT (np. materiały, procesy, organizacja produkcji, IT)

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
HORIZONT X PROCONSULT

Co-funded by the
Erasmus+ Programme
of the European Union

Problemy z zakupami online i przelewami pieniężnymi

BRAIN
WSEI University
LUBLIN
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
HORIZONT X PROCONSULT

Co-funded by the
Erasmus+ Programme
of the European Union

Ice Breaker

Grupa tworzy koło. Uczestnicy rzucają do siebie piłkę. Każdy podaje skojarzenie z poprzednim słowem wypowiedzianym przez osobę, od której otrzymał piłkę. Ćwiczenie jest powtarzane.

Co się dzieje?

Lodołamacze to zabawne ćwiczenia, które pomagają ludziom poznać się nawzajem. Instruktorzy mogą wykorzystać je do zapoznania uczestników z treścią kursu i oczekiwaniami. Lodołamacze mogą być również zaprojektowane w celu rozgrzania przestrzeni do nauki online i zorientowania uczestników w środowisku online.

Co-funded by the
Erasmus+ Programme
of the European Union

Płatności mobilne

Portfele cyfrowe to nośnik do przechowywania wielu fizycznych kart kredytowych lub debetowych.

Aplikacja bankowa, która może być używana do celów uwierzytelniania wymaganych podczas dokonywania transakcji lub uzyskiwania dostępu do usług bankowych. Zazwyczaj każdy bank posiada własną aplikację.

Co-funded by the
Erasmus+ Programme
of the European Union

Korzyści z płatności mobilnych

Touch ID w postaci skanowania odcisków palców lub wprowadzania kodu PIN sprawia, że są one bezpieczniejsze niż fizyczne karty kredytowe lub debetowe,

Eliminacja fizycznego portfela

Ludzie nie mogą zobaczyć, jaką kartę posiadasz (niektóre karty są przeznaczone dla klientów z niskimi limitami zdolności kredytowej. Niektórzy ludzie czują wstyd pokazując je innym ludziom).

Działaj jako łatwiejszy zewnętrzny dostawca płatności podczas płacenia w witrynach handlu elektronicznego.

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czym są ciasteczka? Do czego służą?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Pliki cookie to małe fragmenty tekstu, które odwiedzane witryny wysyłają do przeglądarki. Pozwalają one witrynom internetowym zapamiętać informacje o wizycie użytkownika, co może ułatwić ponowne odwiedzanie witryn i uczynić je bardziej przydatnymi dla użytkownika. Są to pliki tymczasowe, które mogą trwać krócej lub dłużej. Możemy je konfigurować, używać narzędzi do ich blokowania, usuwać, kiedy tylko chcemy... Problem może pojawić się głównie wtedy, gdy gromadzą one dane osobowe bez powiadamiania użytkownika.

Co-funded by the
Erasmus+ Programme
of the European Union

Problemy z zakupami online, zakupami kartą i przelewami pieniężnymi.

Bezpieczne zakupy online

Materiały

Telefony/tablety/laptopy z dostępem do Internetu, projektor, kartki papieru, długopisy, kartony

Kierunki

Uczestnicy będą siedzieć w kręgu. Trener na flipcharcie napisze pytania prowadzące do uczestników, pomagając im wymyślić zasady bezpiecznych zakupów online (załącznik poniżej).

Dodatek

- korzystać ze znanej strony internetowej
- używać narzędzia do oceny bezpieczeństwa nowych stron internetowych
- Szukaj zamka
- Nie udostępniaj swoich wrażliwych danych każdemu
- Korzystanie z prywatnej sieci Wi-Fi
- Tworzenie silnych haseł
- Nie kupuj za pomocą karty w miejscach publicznych

Co-funded by the
Erasmus+ Programme
of the European Union

Portfele cyfrowe

- **Przykłady:**
- Apple Pay, Google Pay i Samsung Pay to prawdopodobnie trzy najpopularniejsze portfele cyfrowe, ale istnieje też kilka innych. Inne popularne portfele cyfrowe to PayPal i Venmo, z których oba są wyjątkowo społecznościowe, umożliwiając łatwe wysyłanie pieniędzy do sprzedawców detalicznych i znajomych.

Problemy z zakupami online, zakupami kartą i przelewami pieniężnymi.

Niebezpieczeństwa związane z używaniem pieniędzy w przestrzeni cyfrowej

Co-funded by the Erasmus+ Programme of the European Union

Materiały

Telefony/tablety/laptopy z dostępem do Internetu, projektor, kartki papieru, długopisy, kartony

Kierunki

Prowadzący zapisuje termin "Niebezpieczeństwa związane z używaniem pieniędzy w przestrzeni cyfrowej" na środku flipcharta. Rozdaj uczestnikom karteczki samoprzylepne Post-it (w różnych kolorach) i poproś ich o zapisanie swoich skojarzeń z tym terminem i przyklejenie ich do flipcharta. Przeczytaj zapisane skojarzenia, grupując je razem, jeśli to możliwe. Omów każde skojarzenie i spróbuj poznać zagrożenia online związane z pieniędzmi (załącznik poniżej).

Dodatek

Niebezpieczeństwa związane z używaniem pieniędzy w przestrzeni cyfrowej

1. Informacje o karcie mogą zostać skradzione (IBAN, CVC, data ważności).

Twoje dane osobowe mogą zostać skradzione (imię i nazwisko, kod identyfikacyjny, data urodzenia, numer telefonu, hasła).

Co-funded by the
Erasmus+ Programme
of the European Union

Czy portfele cyfrowe są bezpieczne?

Portfele cyfrowe są w rzeczywistości bezpieczniejsze niż karty fizyczne, ponieważ płatności mobilne są silnie szyfrowane i tokenizowane, co oznacza, że żaden z rzeczywistych numerów kart lub kont nie jest przechowywany w portfelu cyfrowym.

Portfele cyfrowe idą o krok dalej, dodając również tokenizację, która pobiera wrażliwe zaszyfrowane dane i zastępuje je niewrażliwym cyfrowym odpowiednikiem znanym jako token. Te unikalne tokeny są generowane losowo za każdym razem, gdy użytkownik dokonuje płatności i tylko bramka płatnicza sprzedawcy może dopasować ten token, aby zaakceptować płatność.

Informacje są bezpieczniejsze nie tylko dzięki tej technologii, ale także dzięki weryfikacji użytkownika. Ta dodatkowa warstwa zabezpieczeń jest zwykle wykonywana za pomocą odcisku palca, rozpoznawania twarzy lub kodu PIN.

Co-funded by the
Erasmus+ Programme
of the European Union

Apple i Google płacą podobnie

Oba systemy wykorzystują technologię NFC

Zarówno Google Pay, jak i Apple Pay mogą dokonywać zakupów online bezpośrednio z aplikacji lub strony internetowej, automatycznie obsługując cały proces płatności za pomocą wstępnie wypełnionych ustawień domyślnych i wymagając jedynie weryfikacji PIN lub Touch ID w celu sfinalizowania transakcji.

Oba są bezpieczniejsze niż fizyczne karty debetowe i kredytowe, ponieważ system nie ujawnia danych karty użytkownika sprzedawcy.

Co-funded by the
Erasmus+ Programme
of the European Union

Różnice w wynagrodzeniach Apple i Google

Apple Pay umożliwia uwierzytelnianie za pomocą Touch ID lub Face ID, ale jest kompatybilne tylko z nowymi gadżetami sprzętowymi.

Z drugiej strony Google wybiera bardziej tradycyjny system uwierzytelniania oparty na kodzie PIN. Pozwala to na pracę na starszym sprzęcie.

Do google pay można dodać dowolną kartę kredytową lub debetową. W apple pay możesz dodać tylko karty kredytowe lub debetowe, które firma Apple ma w kontaktach z bankami wydającymi fizyczne karty.

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czy wiesz, czym są dane w chmurze?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Przechowywanie danych w chmurze to model przetwarzania w chmurze, który przechowuje dane w Internecie za pośrednictwem dostawcy usług przetwarzania w chmurze, który zarządza i obsługuje przechowywanie danych jako usługę. Jest ona dostarczana na żądanie z wydajnością i kosztami just-in-time oraz eliminuje konieczność zakupu własnej infrastruktury do przechowywania danych i zarządzania nią.

Co-funded by the
Erasmus+ Programme
of the European Union

Google Pay

Bezpieczeństwo Google? Jak to działa?

1. Dane karty użytkownika są podawane tylko raz, podczas początkowej konfiguracji na serwerach Google. (Google przechowuje dane karty użytkownika na swoich serwerach)

2. Google zapisuje dane karty na swoich serwerach.

3. Karta wirtualna jest wydawana na urządzeniu z szyfrowaniem poufnych danych.

4. Podczas płatności sprzedawca nigdy nie widzi prawdziwych danych karty, które są chronione przez serwery Google.

Co-funded by the
Erasmus+ Programme
of the European Union

Bezpieczeństwo Apple? Jak to działa?

Pay

- Apple używa systemu tokenizacji.
  Kroki;
- Po podaniu danych karty urządzenie kontaktuje się bezpośrednio z bankiem, który ją wydał. (Apple nie przechowuje danych karty)
- Po potwierdzeniu karty bank otrzymuje specyficzny dla urządzenia i karty (powiązany) token o nazwie Device Account Number (DAN), który jest przechowywany na bezpiecznym chipie w urządzeniu.
- DAN strukturalnie przypomina numer karty kredytowej i jest przekazywany sprzedawcy podczas dokonywania płatności przed autoryzacją przez bank.
- Szczegółowe wyjaśnienie Apple Pay:
  https://www.youtube.com/watch?v=mt5FEvoEHEk

Co-funded by the
Erasmus+ Programme
of the European Union

Portfele kryptowalutowe

Posiadanie bezpiecznego portfela kryptowalutowego działa podobnie jak zwykły portfel, z wyjątkiem tego, że waluty i zawartość portfela mogą zostać zhakowane za pomocą środków cyfrowych. Dodatkowo, posiadanie portfela pozwala użytkownikom na wykonywanie różnych transakcji przy jednoczesnym monitorowaniu salda.

Niektóre banki internetowe, takie jak Revolut, Wirex, Cryptopay itp. umożliwiają bezpłatne wypłacanie kryptowalut z bankomatu w euro/dolarach do określonego limitu.

Revolut

wirex

CRYPTOPAY

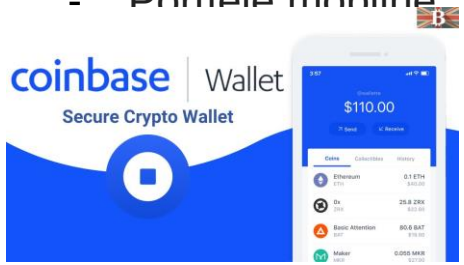
Co-funded by the
Erasmus+ Programme
of the European Union

Rodzaje portfeli kryptowalutowych

Portfele programowe

Portfele programowe są gorącymi portfelami, ponieważ często są połączone z Internetem. Są to portfele działające na określonym programie, który umożliwia łatwy dostęp. Niektóre przykłady portfeli programowych obejmują:

- Portfele na komputery stacjonarne
- Portfele mobilne



Portfele sprzętowe

Portfele sprzętowe różnią się od portfeli programowych tym, że przechowują klucze prywatne użytkownika w urządzeniu sprzętowym, takim jak pendrive. Ich głównym celem jest przechowywanie danych offline, aby uniknąć naruszenia prywatności. Ich głównym celem jest przechowywanie danych użytkownika w trybie offline, aby uniknąć naruszenia prywatności.

Portfele papierowe

Tego typu portfele zawierają specjalne oprogramowanie, które może być używane do generowania kluczy i ich drukowania. Ich inne funkcje obejmują przesyłanie środków na adres i przenoszenie aktywów do portfela stacjonarnego. Aby zrobić to drugie, użytkownicy będą musieli ręcznie wprowadzić swoje klucze lub zeskanować kod zawarty w portfelu.

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
HORIZONT X PROCONSULT

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czy ktoś może mi powiedzieć, czym jest cyberbezpieczeństwo?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Cyberbezpieczeństwo to praktyka ochrony systemów, sieci i programów przed atakami cyfrowymi. Te cyberataki mają zwykle na celu uzyskanie dostępu, zmianę lub zniszczenie poufnych informacji, wyłudzenie pieniędzy od użytkowników lub przerwanie normalnych procesów biznesowych.

Co-funded by the
Erasmus+ Programme
of the European Union

Zalety różnych rodzajów portfeli kryptowalutowych

Popularne portfele online/oprogramowanie

- Cele wydatków;
- Nie chcę płacić za portfel.

Portfele typu cold/offline/Hardware

- Cele inwestycyjne;
- Jeśli przechowujesz więcej kryptowalut, to ich używasz.

Co-funded by the
Erasmus+ Programme
of the European Union

Problemy z zakupami online, zakupami kartą i przelewami pieniężnymi.

Oszustwa w zakupach online - wideo

Materiały

Telefony/tablety/laptopy z dostępem do Internetu, projektor, kartki papieru, długopisy, kartony

Kierunki

ELEMENTY WIARYGODNOŚCI STRONY INTERNETOWEJ

Jak rozpoznać i uniknąć oszukańczej strony internetowej (angielski):

https://www.youtube.com/watch?v=3oEI0FCnI_Y

Wskazówki dotyczące bezpiecznych zakupów online (w języku angielskim):

https://www.youtube.com/watch?v=cWcNQgPiqhc

Kroki:

1. Przed odtworzeniem powyższych filmów uczestnicy proszeni są o prześledzenie ich i zwrócenie uwagi, że nie wszystkie elementy są wiarygodne.
2. Po obejrzeniu filmów uczestnicy siedzący w kręgu proszeni są o zapisanie na flipcharcie elementów dotyczących sprawdzania wiarygodności strony internetowej.
3. Każdy tekst jest od razu omawiany przez piszącego uczestnika i trenera (załącznik poniżej).

Co-funded by the
Erasmus+ Programme
of the European Union

Problemy z zakupami online, zakupami kartą i przelewami pieniężnymi.

Oszustwa w zakupach online - wideo

Dodatek

Jak sprawdzić wiarygodność strony internetowej:
Płatne reklamy - niektórzy oszuści używają płatnych reklam Google, aby pojawić się na szczycie wyszukiwania w Google.
Pozytywne fałszywe recenzje użytkowników - fałszywe strony internetowe tworzą pozytywne recenzje, aby zwiększyć wiarygodność.
pozytywnie fałszywe opinie użytkowników.
Fałszywy adres URL - niektóre fałszywe witryny wykorzystują litery z różnych alfabetów, aby naśladować legalne witryny.
PadLock i HTTPS - pokazują, że dane na stronie są szyfrowane. (Osoby trzecie nie mogą zobaczyć twoich haseł, e-maili itp.)
Certyfikat - sprawdź datę wygaśnięcia certyfikatu witryny i kto go wydał.
Adres firmy, prawa autorskie i kontakty - adres firmy nie znajduje się na mapach Google lub znajduje się w dziwnym miejscu (las, pustynia itp.).
Prawa autorskie, statut działania/pracy - powinny być aktualne.
Fałszywe wiadomości e-mail - lepiej wpisywać linki z przeglądarki niż z wiadomości e-mail, ponieważ mogą one zawierać dane spyware do zbierania poufnych danych.

Co-funded by the
Erasmus+ Programme
of the European Union

Karta debetowa

Karty debetowe są wydawane **przez bank i działają jako połączenie karty bankomatowej i kredytowej**. Jednak w przeciwieństwie do karty kredytowej, karta debetowa łączy się bezpośrednio z kontem bankowym, wykorzystując pieniądze, które masz na depozycie, aby zapłacić za zakup lub dokonać wypłaty z bankomatu cyfrowo.

Co-funded by the
Erasmus+ Programme
of the European Union

Karty debetowe

Plusy

- Zapobieganie zadłużeniu
- Brak opłat rocznych
- Dobry dla mniejszych zakupów
- Łatwy do zdobycia

Wady

- Posiadają ograniczone fundusze
- Opłaty za debet w koncie
- Skomplikowane w przypadku dużych przedmiotów

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czy ktoś wie, jak utworzyć silne hasło?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Głównymi kluczami do stworzenia silnego hasła jest to, że powinno mieć co najmniej 12 znaków, łącząc duże i małe litery, cyfry i symbol. Konieczne jest również używanie różnych haseł dla każdej witryny i zmienianie ich od czasu do czasu.

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

Co-funded by the
Erasmus+ Programme
of the European Union

Karty kredytowe

Karty kredytowe oferują linię kredytową, którą można wykorzystać do dokonywania **zakupów, przelewów salda i/lub zaliczek gotówkowych,** wymagając spłaty kwoty pożyczki w przyszłości. Korzystając z karty kredytowej, będziesz musiał co miesiąc dokonywać co najmniej minimalnej płatności w terminie wymagalności salda.

Co-funded by the
Erasmus+ Programme
of the European Union

Karty kredytowe

Plusy

- Czas na zauważenie błędów
- Może budować kredyt
- Oferuj nagrody
- Posiadają wysokie limity

Wady

- Nie można stracić dużo pieniędzy
- Może zaszkodzić kredytowi
- Potencjał nadmiernych wydatków

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czym jest VPN?

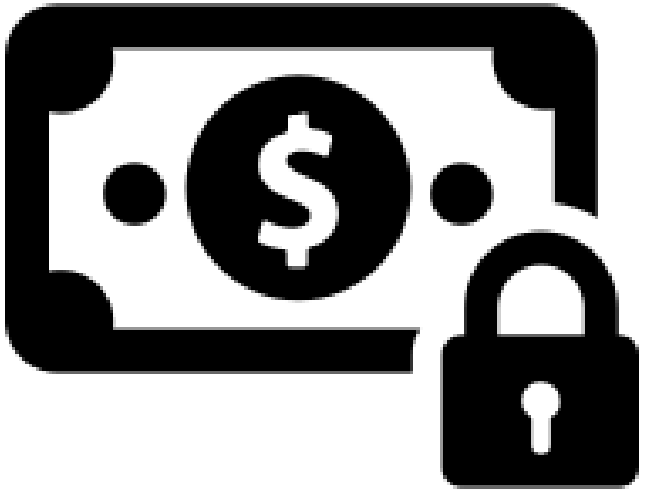
Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

VPN to skrót od "wirtualnej sieci prywatnej" - usługi, która pomaga zachować prywatność w Internecie. VPN ustanawia bezpieczne, szyfrowane połączenie między komputerem a Internetem, zapewniając prywatny tunel dla danych i komunikacji podczas korzystania z sieci publicznych

Co-funded by the
Erasmus+ Programme
of the European Union

Jak bezpiecznie korzystać z karty debetowej lub kredytowej w Internecie?



Zwróć uwagę na blokadę: Upewnij się, że robisz zakupy w bezpiecznej witrynie, zwłaszcza gdy przychodzi czas na wprowadzenie numeru karty. Szukaj ikony zamkniętej kłódki w przeglądarce i zwracaj uwagę na wszelkie pojawiające się ostrzeżenia dotyczące bezpieczeństwa.

Monitoruj swoje konto: Zawsze dobrze jest mieć oko na swoje pieniądze, a jest to szczególnie ważne, jeśli udostępniasz informacje o koncie online. Sprawdzaj swoje konta regularnie: minimum raz w miesiącu, choć lepiej częściej. Skonfiguruj też alerty na swoim koncie, aby wiedzieć, kiedy pieniądze zostaną wypłacone.

Korzystaj z bezpiecznych połączeń: Urządzenia mobilne i darmowe Wi-Fi ułatwiają wykonywanie zadań. Ale nigdy nie wiadomo, jak bezpieczny jest publiczny hotspot. Jeśli zamierzasz uzyskać dostęp do kont finansowych lub wprowadzić numery kart, zachowaj te zadania, gdy jesteś w domu lub pracy i wiesz, że Twój ruch jest bezpieczny.

Co-funded by the
Erasmus+ Programme
of the European Union

Korzystanie ze znanych stron internetowych

- Zacznij od zaufanej witryny. Wyniki wyszukiwania mogą zostać sfałszowane, by sprowadzić cię na manowce, zwłaszcza gdy przebrniesz przez kilka pierwszych stron linków. Jeśli znasz witrynę, istnieje mniejsze prawdopodobieństwo, że jest to oszustwo. Wszyscy wiemy, że Amazon.com oferuje wszystko pod słońcem; podobnie, prawie każdy duży punkt sprzedaży detalicznej ma sklep internetowy, od Target, przez Best Buy, po Home Depot. Uważaj na błędy ortograficzne lub witryny korzystające z innej domeny najwyższego poziomu (na przykład .net zamiast .com) - to najstarsze sztuczki w książce. Tak, sprzedaż na tych stronach może wyglądać kusząco, ale w ten sposób oszukują cię, byś podał swoje dane.

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czy wiesz, w jaki sposób użytkownicy są śledzeni w wyszukiwarkach (historia wyszukiwania, pliki cookie, adresy IP, historia kliknięć)?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Wyszukiwarka może śledzić użytkownika w różnych witrynach, jeśli odwiedzane witryny zawierają własne skrypty śledzące wyszukiwarki jako część strony. To, czego szukasz, pozostawia ślad informacji o tobie. Informacje te ujawniają, czym się interesujesz, co Cię ciekawi, a nawet co myślisz o tych rzeczach.

Co-funded by the
Erasmus+ Programme
of the European Union

Szukaj blokady

- Nigdy nie kupuj niczego online za pomocą karty kredytowej w witrynie, która nie ma zainstalowanego szyfrowania SSL (secure sockets layer) - przynajmniej.
- Będziesz wiedział, czy witryna ma SSL, ponieważ adres URL witryny będzie zaczynał się od HTTPS - zamiast tylko HTTP. Pojawi się ikona zamkniętej kłódki, zwykle po lewej stronie adresu URL na pasku adresu lub na pasku stanu poniżej; zależy to od przeglądarki.
- HTTPS jest obecnie standardem nawet w witrynach niezwiązanych ze sklepami, na tyle, że Google Chrome oznacza każdą stronę bez dodatkowego S jako "niezabezpieczoną". Tak więc strona bez niego powinna wyróżniać się jeszcze bardziej.

Co-funded by the
Erasmus+ Programme
of the European Union

Media społecznościowe - bezpieczne zarządzanie wizerunkiem i informacjami online
Nasze bezpieczeństwo online i ochrona naszej prywatności

Materiały

Laptop z dostępem do Internetu dla prezentera, rzutnik, długopisy, markery, flipchart, karteczki samoprzylepne, kartki A4, piłka tenisowa.

Kierunki

Prowadzący dzieli uczestników na grupy 4-5 osobowe i prosi o zastanowienie się i zapisanie na kartkach odpowiedzi na pytanie: co możemy zrobić, aby zadbać o nasze bezpieczeństwo w sieci i chronić naszą prywatność? Następnie prosi przedstawicieli grup o przeczytanie odpowiedzi i zapisanie ich na tablicy/flipcharcie. Po zapisaniu wszystkich odpowiedzi prowadzący prosi uczestników o wybranie zasady, która wydaje im się najważniejsza. Ochotnicy mówią pozostałym uczestnikom, dlaczego ją wybrali. Patrz poniżej:

Ponadto: Podsumowanie zajęć przez prowadzącego, dyskusja na temat wpływu mediów społecznościowych na nas, możliwości i zagrożeń związanych z korzystaniem z mediów społecznościowych w niewłaściwy sposób, co możemy zrobić, aby zwiększyć nasze bezpieczeństwo. Wspólne oglądanie całości lub fragmentów filmu na You Tube "Prawda o mediach społecznościowych"
https://www.youtube.com/watch?v=DU3655oQexw

Co-funded by the
Erasmus+ Programme
of the European Union

Media społecznościowe - bezpieczne zarządzanie wizerunkiem i informacjami online
Nasze bezpieczeństwo online i ochrona naszej prywatności

Dodatek

- Jeśli nie masz pewności, z kim rozmawiasz, nie podawaj żadnych informacji o sobie.
- Nie ujawniaj swoich haseł innym osobom. Ułóż takie, które będzie trudne do odgadnięcia (nie może to być Twoja data urodzenia ani imię!). Hasło powinno zawierać nie mniej niż 8 znaków, w tym cyfry i wielkie litery. Używaj różnych haseł w różnych usługach.
- Nie zezwalaj przeglądarce na zapamiętywanie haseł do poczty e-mail i usług, z których korzystasz. Wyloguj się, gdy skończysz.
- Jeśli korzystasz z portali społecznościowych, upewnij się, że masz odpowiednie ustawienia prywatności. Im mniej informacji udostępniasz osobom postronnym, tym lepiej.
- Na forach dyskusyjnych lub blogach używaj pseudonimu, a nie swojego imienia i nazwiska. Unikaj publikowania informacji o sobie w Internecie.
- Nie korzystaj z możliwości automatycznego "oznaczania się" w miejscu, w którym się znajdujesz.
- Zwracaj uwagę na komunikaty pojawiające się podczas pobierania gier i aplikacji na telefony komórkowe i smartfony. Można się z nich dowiedzieć, do jakich danych żąda dostępu pobierana usługa. Uważaj na to, na co się zgadzasz.
- Podaj tylko dane niezbędne do utworzenia konta.
- Zamiast śledzenia na Facebooku, używaj newsletterów i kanałów RSS.

Co-funded by the
Erasmus+ Programme
of the European Union

Nie dziel się nadmiernie

- Żaden sprzedawca internetowy nie potrzebuje numeru ubezpieczenia społecznego ani daty urodzenia do prowadzenia działalności.
- Jeśli jednak oszuści zdobędą je i numer karty kredytowej, mogą wyrządzić wiele szkód. Im więcej oszuści wiedzą, tym łatwiej jest im ukraść Twoją tożsamość.
- Jeśli to możliwe, domyślnie podawaj jak najmniej danych osobowych. Duże witryny są cały czas atakowane.

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na pytanie...

Czy znasz jakieś sztuczki zapobiegające śledzeniu twoich informacji?

Co-funded by the
Erasmus+ Programme
of the European Union

Czas na odpowiedź...

Zmień ustawienia, aby zablokować trackery, użyj trybu incognito, użyj VPN, użyj prywatnych przeglądarek. Search Encrypt wykorzystuje szyfrowanie do ukrywania historii wyszukiwania przed innymi osobami, które mogą korzystać z urządzenia po wyszukiwaniu.

Co-funded by the
Erasmus+ Programme
of the European Union

Problemy z zakupami online, zakupami kartą i przelewami pieniężnymi.

Bezpieczne korzystanie z kart kredytowych i debetowych

Materiały

Telefony/tablety/laptopy z dostępem do Internetu, projektor, kartki papieru, długopisy, kartony

Kierunki

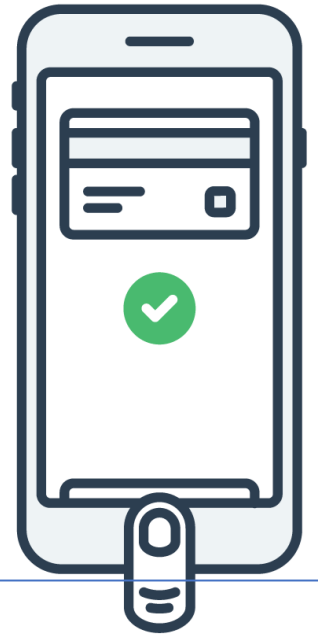
Uczestnicy będą siedzieć w kręgu. Trener na flipcharcie napisze pytania prowadzące do uczestników, pomagając im wymyślić zasady bezpiecznego korzystania z kart kredytowych i debetowych (załącznik poniżej).

Dodatek

- Lepsze wykorzystanie aplikacji do płatności mobilnych
- Korzystaj z zabezpieczeń zapewnianych przez wydawcę karty.
- W przypadku utraty karty należy niezwłocznie poinformować o tym bank
- Nie pokazuj swojej karty publicznie.

Co-funded by the
Erasmus+ Programme
of the European Union

Pomiń kartę, użyj telefonu



Płacenie za przedmioty za pomocą smartfona jest obecnie standardem w sklepach stacjonarnych i jest nawet bezpieczniejsze niż korzystanie z karty kredytowej.

Korzystanie z aplikacji do płatności mobilnych, takich jak Apple Pay, generuje jednorazowy kod uwierzytelniający do zakupu, którego nikt inny nie może ukraść i wykorzystać.

Ponadto unikasz skimmerów kart - nie musisz nawet zabierać ze sobą karty kredytowej, jeśli odwiedzasz tylko miejsca, które akceptują płatności telefoniczne.

Jakie to ma znaczenie, jeśli robisz zakupy online? Wiele aplikacji telefonicznych akceptuje teraz płatności za pomocą Apple Pay i Google Pay. Potrzebujesz tylko odcisku palca, twarzy lub kodu dostępu, aby zrobić to natychmiast.

Co-funded by the
Erasmus+ Programme
of the European Union

Tworzenie silnych haseł

- Upewnienie się, że używasz haseł niemożliwych do złamania. Nigdy nie jest to ważniejsze niż podczas bankowości i zakupów online. Nasze stare wskazówki dotyczące tworzenia unikalnego hasła mogą się przydać w tym okresie roku, kiedy zakupy prawdopodobnie oznaczają tworzenie nowych kont w witrynach handlu elektronicznego.
- Nawet idealne hasło nie jest idealne. Mądrzejszym posunięciem jest skorzystanie z menedżera haseł, który stworzy dla Ciebie hasła nie do złamania. Będzie on je śledził i wprowadzał, więc nie będziesz musiał o tym myśleć.

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Nigdy przenigdy...

Co-funded by the Erasmus+ Programme of the European Union

Materiały

Telefony/tablety/laptopy z dostępem do Internetu, projektor, kartki papieru, długopisy, kartony

Kierunki

- Wszyscy uczestnicy stają w kole. Wypowiadane są stwierdzenia zaczynające się od "Nigdy...", a uczestnicy, którzy je wypowiedzieli, muszą przesunąć się o jeden krok do przodu. Następnie wracają na swoje miejsca. Poniżej znajduje się kilka przykładów, ale uczestnicy mogą również wypowiedzieć dowolne stwierdzenie.
- Nigdy wcześniej nie robiłem zakupów online
- Nigdy nie zostałem oszukany w Internecie.
- Nigdy nie rozmawiałem z kimś online, nie znając go/jej
- Nigdy nie zapomniałem swoich haseł
- Nigdy nie otrzymałem wiadomości spam
- Nigdy nie zostałem zaatakowany przez złośliwe oprogramowanie
- Nigdy wcześniej nie otrzymałem wiadomości e-mail z prośbą o podanie wszystkich moich danych osobowych
- Nigdy nie próbowałem poznać czyjegoś hasła
- Nigdy nie podejrzewałem, że ktoś włamał się na moje konto.
- Nigdy nie zdarzyło mi się znaleźć w telefonie reklamy czegoś, czego właśnie szukałem.
- Nigdy nie podejrzewałem, że jestem szpiegowany przez Internet
- Nigdy nikogo nie prześladowałem
- Nigdy nie doświadczyłem cyberprzemocy

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Nigdy przenigdy...

Co-funded by the Erasmus+ Programme of the European Union

- Nigdy nikogo nie cyberprzemocą
- Nigdy nie wchodziłem na podejrzane strony
- Nigdy nie zdarzyło mi się pobrać wirusa podczas próby pobrania czegoś innego
- Nigdy wcześniej nie musiałem zmieniać wszystkich haseł
- Nigdy wcześniej nie musiałem zmieniać karty kredytowej z powodu wycieku jej danych
- Nigdy nie udawałem kogoś innego w Internecie
- Nigdy nie zdarzyło mi się zignorować zasad przechowywania bezpiecznego hasła.
- Nigdy nie brałem udziału w fałszywej loterii internetowej
- Nigdy nie zdarzyło mi się stracić całej pracy lub czegokolwiek ważnego, ponieważ nie miałem kopii zapasowej
- Nigdy wcześniej nie kliknąłem na baner z informacją, że wygrałem nagrodę
- Nigdy nie surfowałem po głębokiej sieci
- Nigdy nie udostępniałem prywatnych informacji w mediach społecznościowych
- Nigdy nie udostępniałem w internecie kompromitujących zdjęć
- Nigdy nie publikowałem obraźliwych komentarzy w internecie
- Nigdy nie otrzymałem obraźliwych komentarzy w Internecie
- Nigdy nie próbowałem poznać czyichś prywatnych informacji
- Nigdy nie korzystałem z uwierzytelniania dwuetapowego
- Nigdy nie korzystałem z VPN
- Nigdy nie czułem się niebezpiecznie w Internecie

Co-funded by the
Erasmus+ Programme
of the European Union

Wyciek danych osobowych, tworzenie silnych haseł, organizowanie haseł
Gra: Nigdy przenigdy...

Co się dzieje?

Gra Nigdy przenigdy. O tematach internetowych.
Wszyscy uczestnicy stają w kole. Wypowiadane są stwierdzenia zaczynające się od "Nigdy nie zdarzyło mi się...", a uczestnicy, którzy je wypowiedzieli, muszą przesunąć się o jeden krok do przodu. Następnie wracają na swoje miejsca. Podano kilka przykładów, ale uczestnicy mogą również wypowiedzieć dowolne stwierdzenie, które przyjdzie im do głowy.

Prywatyzacja sieci Wi-Fi

Co-funded by the Erasmus+ Programme of the European Union

- Jeśli robisz zakupy za pośrednictwem publicznego hotspotu, trzymaj się znanych sieci, nawet jeśli są one bezpłatne, takie jak te, które można znaleźć w Starbucks lub sklepach Barnes & Noble.
- Każdemu z dostawców w naszym zestawieniu najszybszych darmowych krajowych sieci Wi-Fi można ogólnie zaufać, ale prawdopodobnie powinieneś także korzystać z wirtualnej sieci prywatnej (VPN), aby być bezpiecznym (oto dlaczego).

Co-funded by the
Erasmus+ Programme
of the European Union

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.

Test CRAAP - prezentacja

Materiały

telefony/tablety/laptopy z dostępem do Internetu, rzutnik multimedialny, długopisy, markery, flipchart, karteczki samoprzylepne, arkusze papieru A4

Kierunki

Prezentacja narzędzia weryfikacji informacji (test CRAAP), do czego służy i jak z niego korzystać (załącznik poniżej) wraz z prezentacją.

Dodatek

Test CRAAP to test obiektywnej wiarygodności źródeł informacji w różnych dyscyplinach naukowych. CRAAP to akronim oznaczający aktualność, istotność, autorytet, dokładność i cel. Test CRAAP został zaprojektowany, aby pomóc nauczycielom i uczestnikom określić, czy ich źródłom można zaufać. Korzystając z testu podczas oceny źródeł, badacz może zmniejszyć prawdopodobieństwo wykorzystania niewiarygodnych informacji. Test CRAAP, opracowany przez Sarah Blakeslee i jej zespół bibliotekarzy z California State University, Chico (CSU Chico), jest używany głównie przez bibliotekarzy szkolnictwa wyższego. Jest to jedno z wielu podejść do krytyki źródeł.

Co-funded by the
Erasmus+ Programme
of the European Union

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.

Test CRAAP - prezentacja

Może być kuszące, aby użyć w swoim artykule dowolnego źródła, które wydaje się zgadzać z twoją tezą, ale pamiętaj, że nie wszystkie informacje są dobrymi informacjami, szczególnie w środowisku online. Opracowany przez bibliotekarzy z California State University-Chico test CRAAP to przydatna lista kontrolna do wykorzystania podczas oceny zasobów internetowych (lub JAKICHKOLWIEK zasobów). Test zawiera listę pytań, które należy sobie zadać, decydując, czy zasób jest wystarczająco wiarygodny i godny zaufania, aby można go było wykorzystać w pracy badawczej.
Test CRAAP jest akronimem dla: Currency (aktualność), Relevance (znaczenie), Authority (autorytet), Accuracy (dokładność) i Purpose (cel). Nie jest łatwo określić, czy źródło jest godne zaufania i może być wykorzystywane jako narzędzie badawcze. Test pozwala zaoszczędzić czas i energię potrzebne do oceny treści dostępnych w Internecie.

Co-funded by the
Erasmus+ Programme
of the European Union

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.

Test CRAAP - prezentacja

Zasoby muszą przejść przez pięć etapów weryfikacji.
Aktualność - aktualność informacji
Czas publikacji lub zamieszczenia informacji, czy informacje zostały zaktualizowane lub poprawione oraz czy link działa, czy nie.
Istotność - istotność informacji
Sprawdza, czy informacje są związane z tematem, czy zasób jest odpowiedni i czy można go wykorzystać w pracy akademickiej.
Władza
Buduje zaufanie, podając szczegółowe informacje o autorze, wydawcy przed zaufaniem do informacji i strony internetowej.
Dokładność
Zwróć uwagę na dokładność treści. Informacje muszą być oparte na dowodach przedstawionych odbiorcom. Należy sprawdzić ton języka, błędy gramatyczne i inne błędy typograficzne.
Cel informacji
Określ cele informacji: informowanie, nauczanie, sprzedaż, rozrywka lub przekonywanie.

Co-funded by the
Erasmus+ Programme
of the European Union

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.

Test CRAAP - Quiz

Materiały

telefony/tablety/laptopy z dostępem do Internetu, rzutnik multimedialny, długopisy, markery, flipchart, karteczki samoprzylepne, arkusze papieru A4

Kierunki

Podziel grupę na zespoły składające się z około 4 osób. Poproś każdy zespół o znalezienie artykułu na jeden wybrany przez siebie temat. Wybierz temat, który pasuje do grupy (załącznik poniżej). Rozdaj wydrukowane testy craap (załącznik poniżej) i rozdaj każdej osobie. Poproś uczestników, aby przeczytali artykuł, a następnie przeanalizowali cały tekst w świetle pytań zawartych w teście. Po prawej stronie mają miejsce na przemyślenia/wnioski/odpowiedzi. Na podstawie testu określą, jak wiarygodny jest artykuł. Nie ma skali ocen ani liczby punktów.

Ludzie pracują "online" na otrzymanym materiale, co oznacza, że mogą przeprowadzić dogłębną analizę materiału - poznać cały artykuł, przyjrzeć się bardziej szczegółowo jego źródłu, zweryfikować użyte dane, dowiedzieć się czegoś o autorze itp. Ważne jest, aby sprawdzili, korzystając z kryteriów podanych w teście craap, czy materiał jest wiarygodny, które elementy wskazują na wiarygodność, a które ją podważają. Uczestnicy mogą również zapisywać swoje przemyślenia, co ułatwi dyskusję. Poproś każdą grupę o krótkie przedstawienie wyników swojej analizy.

Co-funded by the
Erasmus+ Programme
of the European Union

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.

Test CRAAP - Quiz

Dodatek

Tematy dla grup:
Klimat
Koronawirus
Uchodźcy
Szczepionki
Gwiazdy
Sport
Unia Europejska

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.

Test CRAAP - Quiz

		Uwagi / odpowiedzi
Waluta terminowość informacja	Kiedy informacje zostały opublikowane?	
	Czy informacje (jeśli nie są nowe) zostały zaktualizowane?	
	Czy sprawa, dla której przeglądasz te informacje, wymaga nowszych, aktualnych danych, czy też możesz polegać na starszych materiałach?	
	Czy linki (jeśli są) zamieszczone w informacjach działają?	
Znaczenie istotność informacji w odniesieniu do potrzeby	Czy informacje w ogóle odnoszą się do tematu, który poruszasz lub odpowiadają na ważne dla Ciebie pytanie?	
	Dla kogo przygotowano te informacje? Dla jakiej grupy docelowej?	
	Czy informacje są na odpowiednim poziomie dla Twoich potrzeb? Czy są zbyt podstawowe i ogólne, czy zbyt zaawansowane i szczegółowe?	
	Czy sprawdziłeś inne źródła informacji, zanim zdecydowałeś się skorzystać tylko z tego?	

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.

Co-funded by the Erasmus+ Programme of the European Union

Test CRAAP - Quiz

Władza pochodzenie informacji	**Kto jest autorem, wydawcą, źródłem lub sponsorem informacji?**	
	Jakie są referencje autora informacji? Z jaką organizacją, podmiotem, instytucją jest powiązany?	
	Czy autor ma kwalifikacje do pisania na ten temat?	
	Czy obok informacji można znaleźć dane kontaktowe, np. nazwę wydawcy, adres e-mail itp.	
	Czy adres strony internetowej, na której pojawiły się informacje, mówi coś o autorze lub nadawcy (np. adres URL kończy się na .com, .edu, .gov)?	
Dokładność rzetelność, prawdziwość i dokładność informacji	Skąd pochodzą te informacje?	
	Czy podane informacje są poparte dowodami?	
	Czy informacje zostały zrecenzowane lub zacytowane (dotyczy głównie artykułów naukowych)?	
	Czy jesteś w stanie potwierdzić przynajmniej część informacji podanych w innym źródle lub wykorzystując swoją wiedzę?	
	Czy język lub wymowa wszystkich informacji wskazuje na bezstronność i jest pozbawiona zabarwienia emocjonalnego?	
	Czy występują błędy ortograficzne, gramatyczne lub stylistyczne?	

Fake news - czyli przeszukiwanie internetu, weryfikowanie informacji podawanych przez media.

Test CRAAP - Quiz

Cel, informacje, powód ich utworzenia	W jakim celu zostały stworzone informacje? Edukować, informować, bawić, przekonywać?
	Czy autor lub osoba finansująca tworzenie informacji jasno określiła ich cel?
	Czy informacja jest cytatem lub opisem faktów, czy przedstawia opinię, czy też ma charakter propagandowy?
	Czy punkt widzenia przedstawiony w informacjach sprawia wrażenie bezstronności i obiektywizmu?
	Czy dostrzegasz w informacjach elementy wskazujące na stronniczość, zajmowanie określonego stanowiska w kwestiach związanych z polityką, religią, światopoglądem lub np. przedstawianie perspektywy tylko jednej instytucji lub osoby?