Scenariusz zajęć dla trenerów pracujących z osobami dorosłymi

Bezpieczeństwo w sieci

autorka: Katarzyna Górkiewicz
czas trwania: 3 godziny (180 minut)
liczebność grupy: 8–20 osób

W trakcie warsztatu uczestnicy:

- zdobędą wiedzę dotyczącą bezpiecznych zachowań w sieci,
- poznają podstawowe zasady bezpieczeństwa w internecie i dowiedzą się, jak je stosować,
- przeanalizują własne zachowania w sieci,
- zaplanują zmiany w swoich działaniach i nawykach.

Materiały/sprzęt:

- karta pracy nr 1 (wydrukowana dla każdego uczestnika),
- karta pracy nr 2 (wydrukowana i pocięta w 4 kompletach),
- karta pracy nr 3 (wydrukowana jako całość i podzielona na 4 oddzielne grupy),
- duże arkusze papieru, np. papier do flip charta,
- kartki papieru A4 (kilka sztuk),
- 4 zestawy kredek lub kolorowych flamastrów,
- taśma malarska (lub coś innego do przywieszania kartek z rezultatami pracy uczestników),
- kolorowe post-ity (jak największe, tak żeby wygodnie zapisać na nich kilka zdań),
- komputery/laptopy/telefony komórkowe z dostępem do sieci, min. jeden na dwoje uczestników,
- komputer z podłączonym rzutnikiem dla prowadzącego,
- opcjonalnie: wirtualna tablica Padlet przygotowana wg. instrukcji w scenariuszu,
- infografika *Jak dbać o swoje bezpieczeństwo w sieci?*

Kilka słów dla prowadzącego

Temat bezpieczeństwa korzystania z internetu stał się w ostatnim czasie bardzo głośny. Często, poprzez przekazy medialne, docierają do nas informacje o niebezpieczeństwach, jakie mogą grozić użytkownikom sieci. Rzeczywiście, lekkomyślne korzystanie z internetu może skończyć się kłopotami. Ważne jednak, by informacje o ryzyku nie zniechęcały nas do używania wielu narzędzi, które mogą nam przecież ułatwić życie, dostarczyć wiedzy i rozrywki.
W dzisiejszym świecie funkcjonujemy jednocześnie online i offline. Trudno wyobrazić sobie uczestniczenie w życiu społecznym czy kulturalnym bez dostępu do internetu. Aby bezpiecznie, odpowiedzialnie i na swoich warunkach poruszać się w internecie, warto nieustannie, w każdym wieku, poszerzać swoją wiedzę i stale ćwiczyć umiejętności bezpiecznego korzystania z internetu.

Przebieg zajęć:

1 / INTEGRACJA – 30 min

Przywitaj uczestników i uczestniczki i zapoznaj ich z planem i celami warsztatu. Zwróć uwagę na ramy czasowe, zaplanujcie długość i moment przerwy, a także ustalcie, w jakiej formie będziecie się do siebie zwracać.
Powiedz kilka słów o sobie i o swoich doświadczeniach związanych z bezpieczeństwem w sieci.
Poproś uczestników, żeby także się przedstawili i opowiedzieli o sobie, omawiając hasło: *Ja i bezpieczeństwo w sieci.*
Możesz przeprowadzić tę rozmowę z użyciem narzędzia Padlet. Jest to rodzaj wirtualnej tablicy, na której ty i każda osoba, której ją udostępnisz, możecie dzielić się np. zdjęciami czy informacjami. Narzędzie jest bardzo proste i intuicyjne w obsłudze, więc przygotowanie tego ćwiczenia zajmie ci tylko chwilę. W tym celu wcześniej załóż konto na https://pl.padlet.com/auth/signup i przygotuj tablicę z zagadnieniem: *Ja i bezpieczeństwo w sieci*. W prawym górnym rogu znajdziesz opcje udostępniania swojej tablicy. Możesz wygenerować link lub kod QR, które udostępnisz uczestnikom, wyświetlając je w prezentacji lub drukując w materiałach dla nich.
Zachęć uczestników do znalezienia zdjęcia, które najlepiej dla nich obrazuje to zagadnienie. Mogą wyszukać i zapisać na swoich komputerach (telefonach, tabletach) zdjęcia w serwisie https://www.flickr.com lub po prostu w grafikach https://www.google.pl/. Wybrane zdjęcia uczestnicy dodają do tablicy Padlet, którą wyświetl na ekranie za pomocą rzutnika. Kiedy wszystkie zdjęcia znajdą się na tablicy, poproś uczestników, aby po kolei omówili swoje zdjęcia i to, dlaczego wybrali je jako ilustrację hasła: *Ja i bezpieczeństwo w sieci.*

Podziękuj wszystkim i przejdź do kolejnego etapu warsztatów.

2 / TEST BEZPIECZEŃSTWA W SIECI – 20 min

Rozdaj wydrukowane wcześniej karty z testem pozwalającym ocenić nawyki i umiejętności użytkowników internetu pod kątem bezpieczeństwa (karta pracy nr 1), zachęć uczestników do wypełnienia go oraz podliczenia uzyskanych punktów. Następnie omówcie na forum wszystkie pytania. Zachęć uczestników, żeby podzielili się swoimi doświadczeniami w kwestiach poruszanych w teście. Zapytaj, czy byli zaskoczeni którymś z zagadnień. Czy uważają, że wynik, który uzyskali w teście, odzwierciedla ich poziom zaawansowania w dbaniu o bezpieczeństwo w sieci?

3 / TRUDNE TERMINY – zdobywamy wiedzę – 20 min

Podziel uczestników na 4 grupy. Każdej grupie daj do ułożenia rozsypankę Trudne terminy (karta pracy nr 2). Daj uczestnikom tyle czasu, ile będą potrzebowali, żeby wykonać zadanie. Jeśli będą znali któregoś terminu, zachęć ich do skorzystania z internetu i poszerzenia swojej wiedzy. Następnie omówcie na forum wszystkie definicje, sprawdzając, czy każda z grup prawidłowo rozwiązała zadanie. Zapytaj uczestników, czy znali te terminy i czy w swoich doświadczeniach w sieci spotkali się z sytuacjami opisanymi w definicjach. Jeśli któreś z zagadnień będzie wymagało dodatkowego wyjaśnienia, omówcie je wspólnie z grupą. W przypadku takich terminów jak połączenie HTTPS czy tryb incognito warto zaprezentować je grupie na dużym ekranie za pomocą rzutnika i zachęcić, żeby zobaczyli w swoich przeglądarkach, jak sprawdzić, czy maja odpowiednie ustawienia gwarantujące im bezpieczeństwo.

przerwa: 5–10 min

4 / PERSONY: JAK KORZYSTAJĄ Z SIECI I JAKI BĘDZIE NAJLEPSZY DLA NICH KODEKS BEZPIECZEŃSTWA? – 70 min

To ćwiczenie zostało opracowane z wykorzystaniem elementów metody DesignThinking, która polega na tworzeniu innowacyjnych, kreatywnych rozwiązań w oparciu o poznanie i zrozumienie potrzeb odbiorców, czyli osób, dla których te rozwiązania przygotowujemy. Zanim uczestnicy stworzą plany zmian własnych zachowań w sieci, wspólnie przyjrzą się personom, czyli wyobrażonym osobom i ich nawykom.
W karcie pracy nr 3 znajdziesz opis czterech różnych person. Rozdaj każdej z grup po jednym opisie i zachęć do uzupełnienia informacji na ich temat wg przygotowanych pytań. Następnie zachęć uczestników do stworzenia plakatu ilustrującego ich personę.
Na tę część zadania przeznacz 25 min.

Następnie poproś każdą z grup o zaprezentowanie jej persony na forum. Przeznacz na tę część zadania 15 minut.

Poproś każdą z grup o opracowanie kodeksu 10 zasad/dobrych rad bezpieczeństwa w sieci dla jej persony. W tym celu rozdaj uczestnikom czyste kartki. Zachęć uczestników, żeby wrócili pamięcią do wcześniejszych ćwiczeń i zdobytej w nich wiedzy – testu bezpieczeństwa w sieci i trudnych terminów. Przeznacz na tę część zadania 15 minut.

Na koniec poproś każdą z grup o odczytanie jej wersji kodeksu, a następnie powieście je wszystkie w widocznym miejscu. Zachęć uczestników do podzielenia się refleksjami: Na ile te kodeksy są uniwersalne? Czy odnajdują siebie wśród ich odbiorców? Czy widzą zasady, które powinni wdrożyć przy korzystaniu z internetu?
Przeznacz na tę część zadania 15 minut.

5 / PODSUMOWANIE I WŁASNE WNIOSKI UCZESTNIKÓW – 15 min

Z omówienia kodeksów z poprzedniego ćwiczenia przejdź płynnie do podsumowania i własnych wniosków uczestników. W tym celu rozdaj wszystkim po kilka karteczek post-it i poproś, żeby zanotowali na nich rzeczy, które po dzisiejszym warsztacie planują zmienić/wdrożyć w swoich nawykach korzystania z sieci. Mogą w tym celu posiłkować się wypracowanymi kodeksami oraz pozostałymi materiałami. Niech każdą z tych rzeczy zapiszą osobno. Zachęć uczestników do podzielenia się swoimi postanowieniami. Niech przyczepią je do dużego arkusza widocznego dla wszystkich, a każda kolejna osoba, która widzi, że podobne/takie same postanowienia ktoś już zadeklarował, niech przyczepi je obok. Dzięki temu uda się wam zmapować wspólne obszary, w których uczestnicy zamierzają wprowadzić zmiany swoich nawyków. Wymieńcie spostrzeżenia na temat tych postanowień.
Na koniec podziękuj uczestnikom i zachęć do poszerzania swojej wiedzy w zakresie bezpieczeństwa w sieci i ćwiczenia dobrych nawyków oraz zaprezentuj lub rozdaj wcześniej wydrukowana infografikę Jak dbać o swoje bezpieczeństwo w sieci?

towarzystwo inicjatyw twórczych

Transitions

Polsko-Amerykańska Fundacja Wolności

/ scenariusz powstał z wykorzystaniem materiałów dostępnych w serwisie edukacjamedialna.org.pl /

Karta pracy nr 1

Test bezpieczeństwa w sieci

Rozwiąż test, odpowiadając szczerze na poniższe pytania i zaznaczając odpowiedzi najbardziej pasujące do twoich nawyków.

1. **Moje hasła do kont i profili (w komputerze, poczcie e-mail, serwisach społecznościowych, sklepach internetowych):**
   a/ są krótkie i proste, żeby łatwo mi było je zapamiętać (np. takie same jak login, data urodzenia, drugie imię, imię zwierzęcia, prosta kombinacja cyfr, pojedyncze słowo ze słownika, to samo hasło różniące się cyfrą na końcu), używam tego samego hasła do wielu kont, pozwalam je zapamiętać przeglądarce internetowej, mam też je zapisane przy komputerze i na kartce, którą noszę przy sobie,
   b/ są średniej długości i średnio skomplikowane, używam kilku haseł do wielu kont,
   c/ są długie i jak najbardziej skomplikowane, składają się z małych i dużych liter, a także cyfr i znaków niealfanumerycznych (co nie zawsze jest możliwe) albo długiej frazy (nawet jeśli jest łatwa do zapamiętania), używam innego hasła do każdego konta, pilnuję zwłaszcza, by hasła do ważnych kont (bank, e-mail) były wyjątkowe i skomplikowane, znane tylko mnie.

2. **Podaję swoje prawdziwe dane:**
   a/ zawsze, gdy strona internetowa o to pyta (np. biorąc udział w konkursach, badaniach czy quizach),
   b/ czasem, np. rejestrując się w różnych serwisach nawet jednorazowo,
   c/ tylko gdy jest to konieczne (np. robiąc zakupy).

3. **Gdy widzę bannery reklamowe lub linki, które zachęcają do skorzystania z promocji, oferty specjalnej, konkursu czy odbioru nagrody, którą się wygrało:**
   a/ klikam w najciekawsze, jeśli mnie dotyczą,
   b/ czasem klikam, ale czasami wydaje mi się to niebezpieczne,
   c/ ignoruję je, chyba że widzę, że reklama jest związana z zaufaną instytucją.

4. **Kiedy loguję się w miejscu publicznym na któreś ze swoich kont, zwracam uwagę na bezpieczne połączenie (np. https, czy certyfikat jest bezpieczny) i czy nikt niepowołany nie patrzy na klawiaturę:**
   a/ nigdy,
   b/ czasem,
   c/ zawsze.

5. **Gdy ktoś przesyła mi link czy załącznik e-mailem lub za pośrednictwe komunikatorów, np. WhatsApp, czy Messenger, otwieram go:**
   a/ zawsze i od każdego,

b/ czasem, ale tylko wtedy, gdy mnie dotyczy,
c/ tylko gdy przesyła go znajoma osoba i gdy wygląda wiarygodnie (np. temat wskazuje, że to rzeczywiście do mnie), jeśli mam wątpliwość, upewniam się, że przesyłający świadomie mi go wysłał.

6. Publikuję swoje zdjęcia w internecie
a/ wszystkie, którymi mam ochotę się podzielić,
b/ najciekawsze, które mnie pozytywnie pokazują, nie analizuję potencjalnych konsekwencji ich publikacji,
c/ ze świadomością, że odtąd każdy będzie mógł je zobaczyć (mimo ustawień prywatności, ktoś niepowołany może dostać do nich dostęp), w tym rodzina, znajomi, potencjalni pracodawcy.

7. Publikuję zdjęcia dotyczące innych osób:
a/ wszystkie, którymi mam ochotę się podzielić,
b/ najciekawsze, które pozytywnie pokazują te osoby, ale nie pytam ich o zgodę i nie analizuję potencjalnych konsekwencji ich publikacji,
c/ tylko za zgodą osób, które są na zdjęciach (lub ich prawnych opiekunów), ze świadomością, że odtąd każdy będzie mógł je zobaczyć (mimo ustawień prywatności, ktoś niepowołany może dostać do nich dostęp), w tym rodzina, znajomi, potencjalni pracodawcy.

8. Co widzą w moich profilach w serwisach społecznościowych moi znajomi a co nieznajomi?
a/ nie wiem / każdy widzi wszystko (np. e-mail, telefon, adres zamieszkania, wszystkie moje zdjęcia),
b/ część danych (jak e-mail, telefon, adres zamieszkania czy zdjęcia) jest widoczna dla nieznajomych,
c/ ustawiam różne dostępy dla różnych grup znajomych, członkowie każdej widzą co innego, nieznajomi widzą tylko nazwisko i zdjęcie.

9. Do grona znajomych w serwisach społecznościowych zapraszam:
a/ każdego, kto zapyta, nawet jeśli nic o nim nie wiem,
b/ różnie, zdarza się, że przyjmuję nieznajomych, a potem ich weryfikuję,
c/ tylko znajomych, ew. osoby ostatnio poznane, które są w gronie znajomych moich znajomych

10. Kiedy wyszukuję informacji w sieci:
a/ wpisuję interesujące mnie hasło w wyszukiwarkę i zapoznaję się z pierwszymi wynikami,
b/ szukam nie tylko poprzez wyszukiwarkę, ale i w Wikipedii i w różnych serwisach,
c/ szukam, korzystając z zaawansowanych narzędzi w wyszukiwarce (np. ustawienia daty, czy wyszukiwania zaawansowanego), korzystam z Wikipedii i wiarygodnych serwisów specjalistycznych; każdą istotną informację weryfikuję w co najmniej dwóch różnych źródłach.

WYNIK:

Przelicz swoje odpowiedzi na punkty:
a/ 0 punktów
b/ 1 punkt
c/ 2 punkty

0 – 7 punktów

Twoje zachowania i nawyki w sieci niestety nie są odpowiedzialne i bezpieczne dla ciebie i twoich bliskich. Nie chronisz odpowiednio swoich danych, prywatności i wizerunku. Nie weryfikujesz treści i informacji, jakie znajdujesz w sieci, lub otrzymujesz za pomocą poczty e-mail czy komunikatorów. Mamy nadzieję, że nie spotkały cię przez to kłopoty. Jeśli poszerzysz swoją wiedzę i popracujesz nad zmianą nawyków, z pewnością będziesz bezpieczniejszy/bezpieczniejsza w sieci!

8 – 14 punktów

Wiesz, że korzystając z internetu należy zachować rozsądek i dbać o bezpieczeństwo. Niestety często nie wiesz, jak to zrobić. Czasem udaje ci się wyłapać niebezpieczne reklamy, wiadomości, banery, czy linki. Czasem jednak zapominasz się i serfujesz po sieci bez odpowiedniego namysłu i ostrożności. Jeśli poszerzysz swoją wiedzę i popracujesz nad lepszymi nawykami, z pewnością będziesz bezpieczniejszy/bezpieczniejsza w sieci!

15 – 20 punktów

Bardzo odpowiedzialnie i rozsądnie korzystasz z internetu. Masz dużą wiedzę i wypracowane dobre nawyki. Dbasz o prywatność swoją i swoich bliskich w sieci, pilnujesz bezpieczeństwa swoich danych, stosujesz zasadę ograniczonego zaufania wobec wszystkich treści, jakie znajdujesz w sieci. Wiesz, jak weryfikować informacje. Pamiętaj, że internet nieustannie się zmienia i rozwija, dlatego warto trzymać rękę na pulsie i nie ustawać w rozwijaniu wiedzy, tak by zawsze być bezpiecznym/bezpieczną w sieci

Karta pracy nr 2

Trudne terminy – zdobywamy wiedzę

spam
Wysyłane automatycznie informacje, drogą mailową lub np. poprzez komunikatory czy SMS-y, których wcale nie chcemy otrzymać. Zwykle zawierają reklamy lub mają nas nakłonić do określonych działań.

phishing
Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) albo nakłonienia ofiary do określonych działań.

maskowanie adresu nadawcy wiadomości
Ukrycie faktycznego adresu e-mail pod inną nazwą użytkownika. Może być używana w celach porządkowych (np. nadawca o adresie jankowalski@firma.pl może być wyświetlany po prostu jako „Jan Kowalski"), często jednak wykorzystywana przez hakerów (ukrycie adresu za nazwą banku, sieci komórkowej lub innego usługodawcy bądź instytucji, np. „Urząd Skarbowy w Pszczynie").

dane wrażliwe
Kategoria danych osobowych wymagająca szczególnej ochrony. Ogólne rozporządzenie o ochronie danych (RODO) wskazuje następujące dane podlegające ochronie: pochodzenie rasowe i etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej), dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej.

połączenie HTTPS
Połączenie przeglądarki ze stroną internetową za pomocą odpowiedniego protokołu zapewniające szyfrowanie komunikacji, a tym samym znacznie utrudniające dostęp do treści osobom innym niż nadawca i odbiorca. Szyfrowanie niezbędne jest w bankowości elektronicznej i w innych sytuacjach, w których podajesz swoje prawdziwe dane. Korzystanie z połączenia https:// zaleca się każdorazowo przy logowaniu.

stalking
Termin określający takie zachowania jak śledzenie ofiary, osaczanie jej (np. poprzez ciągłe wizyty, telefony, SMS-y, pocztę elektroniczną, podarunki) i ciągłe, powtarzające się nagabywanie. W Polsce od 2011 r. uznawane jest za przestępstwo i zagrożone karą pozbawienia wolności do lat 3 lub – w przypadku doprowadzenia ofiary do próby samobójczej – do 10 lat.

cyberbullying
(inaczej: agresja elektroniczna), stosowanie przemocy poprzez: prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób przy pomocy narzędzi elektronicznych, np. SMS-y, e-maile, witryny internetowe, fora

dyskusyjne. Jest rodzajem stalkingu, realizowanego w internecie. Osobę dopuszczającą się takich czynów określa się stalkerem.

szyfrowanie wiadomości

Korzystanie ze specjalnego oprogramowania zabezpieczającego treści komunikacji e-mailowej, SMS-owej lub poprzez komunikatory internetowe (Messenger, WhatsUpp), tak by odczytać ją mogli tylko nadawca i adresaci.

tryb incognito

Sposób działania przeglądarki internetowej, który zapewnia wykasowanie wszystkich danych zapisanych podczas przeglądania (historii, ciasteczek) po zamknięciu przeglądarki (lub po wyłączeniu trybu prywatnego).

cyfrowy ślad

Informacje na temat aktywności każdej z osób korzystających z sieci, magazynowane na serwerach dostawców internetu i przez właścicieli stron. Tworzą go m.in. zdjęcia, informacje o kupionych produktach, nicki, wpisy na blogach, ale również dane, które zostawiamy w sieci mimowolnie, np. adres IP czy informacja o systemie operacyjnym, z którego korzystamy.

profilowanie

Oparty na określonych algorytmach mechanizm, który służy kategoryzowaniu ludzi według ich cech, zachowań, preferencji. Jest stosowany m.in. w marketingu internetowym w celu prezentowania reklam jak najściślej dopasowanych do potrzeb określonych użytkowników sieci, w branży bankowej i ubezpieczeniowej w celu oceny klienta, a także przez państwo w celu zwiększenia bezpieczeństwa (np. No Fly List w USA).

bańka filtrująca

Termin określający personalizowanie treści, które widzimy w sieci (np. podczas wyszukiwania w wyszukiwarce albo widoczne w serwisach społecznościowych). Polega ono na dopasowywaniu treści za pomocą określonych algorytmów w taki sposób, aby jak najbardziej odpowiadały naszym zainteresowaniom. Ustalane jest to na podstawie naszego wcześniejszego wyszukiwania, historii przeglądania stron www na komputerze i urządzeniu mobilnym, treści maili czy geolokalizacji.

spyware

Oprogramowanie pozwalające na zbieranie danych na temat konkretnego użytkownika lub organizacji bez ich świadomości. Ofiara może nawet nie podejrzewać, że na jej komputerze znajduje się spyware. Z reguły celem tego szkodnika jest:

- śledzenie działań wykonywanych na komputerze przez użytkownika,
- gromadzenie informacji na temat zawartości dysków twardych, co często oznacza skanowanie niektórych folderów i rejestru systemu w celu utworzenia listy oprogramowania zainstalowanego na komputerze,
- zbieranie informacji o jakości połączenia, sposobie podłączenia, prędkości modemu itp.

fake news

Informacje, które podają nieprawdziwe, częściowo nieprawdziwe lub przeinaczone fakty. Promują konkretne poglądy polityczne i udają, że są rzetelne. Dominują w nich zdjęcia, a tekst jest często krótki i bardzo ogólny. Mają silnie emocjonalnie nacechowany przekaz. Często udają przekaz z pierwszej ręki, wykorzystują ogólnie znane prawdy i przekonania.

Wydrukuj i wytnij

Wysyłane automatycznie informacje, drogą mailową lub np. poprzez komunikatory czy SMS-y, których wcale nie chcemy otrzymać. Zwykle zawierają reklamy lub mają nas nakłonić do określonych działań.

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) albo nakłonienia ofiary do określonych działań.

Ukrycie faktycznego adresu e-mail pod inną nazwą użytkownika.
Może być używana w celach porządkowych (np. nadawca o adresie jankowalski@firma.pl może być wyświetlany po prostu jako „Jan Kowalski"), często jednak wykorzystywana przez hakerów (ukrycie adresu za nazwą banku, sieci komórkowej lub innego usługodawcy bądź instytucji, np. „Urząd Skarbowy w Pszczynie").

Kategoria danych osobowych wymagająca szczególnej ochrony. Ogólne rozporządzenie o ochronie danych (RODO) wskazuje następujące dane podlegające ochronie: pochodzenie rasowe i etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej), dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej.

Połączenie przeglądarki ze stroną internetową za pomocą odpowiedniego protokołu zapewniające szyfrowanie komunikacji, a tym samym znacznie utrudniające dostęp do treści osobom innym niż nadawca i odbiorca. Szyfrowanie niezbędne jest w bankowości elektronicznej i w innych sytuacjach, w których podajesz swoje prawdziwe dane. Korzystanie z połączenia https:// zaleca się każdorazowo przy logowaniu.

Termin określający takie zachowania jak śledzenie ofiary, osaczanie jej (np. poprzez ciągłe wizyty, telefony, SMS-y, pocztę elektroniczną, podarunki) i ciągłe, powtarzające się nagabywanie. W Polsce od 2011 r. uznawane jest za przestępstwo i zagrożone karą pozbawienia wolności do lat 3 lub – w przypadku doprowadzenia ofiary do próby samobójczej – do 10 lat.

Inaczej: agresja elektroniczna, stosowanie przemocy poprzez: prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób przy pomocy narzędzi elektronicznych, np. SMS-y, e-maile, witryny internetowe, fora dyskusyjne. Jest rodzajem stalkingu, realizowanego w internecie. Osobę dopuszczającą się takich czynów określa się stalkerem.

Korzystanie ze specjalnego oprogramowania zabezpieczającego treści komunikacji e-mailowej, SMS-owej lub poprzez komunikatory internetowe (Messenger, WhatsUpp), tak by odczytać ją mogli tylko nadawca i adresaci.

Sposób działania przeglądarki internetowej, który zapewnia wykasowanie wszystkich danych zapisanych podczas przeglądania (historii, ciasteczek) po zamknięciu przeglądarki (lub po wyłączeniu trybu prywatnego).

Informacje na temat aktywności każdej z osób korzystających z sieci, magazynowane na serwerach dostawców internetu i przez właścicieli stron. Tworzą go m.in. zdjęcia, informacje o kupionych produktach, nicki, wpisy na blogach, ale również dane, które zostawiamy w sieci mimowolnie, np. adres IP czy informacja o systemie operacyjnym, z którego korzystamy.

Oparty na określonych algorytmach mechanizm, który służy kategoryzowaniu ludzi według ich cech, zachowań, preferencji. Jest stosowany m.in. w marketingu internetowym w celu prezentowania reklam jak najściślej dopasowanych do potrzeb określonych użytkowników sieci, w branży bankowej i ubezpieczeniowej w celu oceny klienta, a także przez państwo w celu zwiększenia bezpieczeństwa (np. No Fly List w USA).

Termin określający personalizowanie treści, które widzimy w sieci (np. podczas wyszukiwania w wyszukiwarce albo widoczne w serwisach społecznościowych). Polega ono na dopasowywaniu treści za pomocą określonych algorytmów w taki sposób, aby jak najbardziej odpowiadały naszym zainteresowaniom. Ustalane jest to na podstawie naszego wcześniejszego wyszukiwania, historii przeglądania stron www na komputerze i urządzeniu mobilnym, treści maili czy geolokalizacji.

Oprogramowanie pozwalające na zbieranie danych na temat konkretnego użytkownika lub organizacji bez ich świadomości. Ofiara może nawet nie podejrzewać, że na jej komputerze znajduje się spyware. Z reguły celem tego szkodnika jest:

- śledzenie działań wykonywanych na komputerze przez użytkownika,
- gromadzenie informacji na temat zawartości dysków twardych, co często oznacza skanowanie niektórych folderów i rejestru systemu w celu utworzenia listy oprogramowania zainstalowanego na komputerze,
- zbieranie informacji o jakości połączenia, sposobie podłączenia, prędkości modemu itp.

Informacje, które podają nieprawdziwe, częściowo nieprawdziwe lub przeinaczone fakty. Promują konkretne poglądy polityczne i udają, że są rzetelne. Dominują w nich zdjęcia, a tekst jest często krótki i bardzo ogólny. Mają silnie emocjonalnie nacechowany przekaz. Często udają przekaz z pierwszej ręki, wykorzystują ogólnie znane prawdy i przekonania.

SPAM

PHISHING

MASKOWANIE ADRESU NADAWCY WIADOMOŚCI

DANE WRAŻLIWE

POŁĄCZENIE HTTPS

STALKING

CYBERBULLYING

SZYFROWANIE WIADOMOŚCI

TRYB INCOGNITO

CYFROWY ŚLAD

PROFILOWANIE

BAŃKA FILTRUJĄCA

SPYWARE

FAKE NEWS

Karta pracy nr 3

Persona

Nicola (1)
Jest nastolatką, ma czwórkę rodzeństwa, mieszkają razem z rodzicami w bloku, w dwupokojowym mieszkaniu. Mama jest pielęgniarką, tata nocnym stróżem. W domu się nie przelewa. Nicola zalicza wszystkie przedmioty na poziomie minimalnym, ale jest duszą towarzystwa w klasie – większość rówieśników bardzo liczy się z jej zdaniem. Wstydzi się materialnego statusu swojej rodziny i próbuje go ukrywać. Uwielbia kosmetyki, mocno się maluje. Dba o swój wizerunek, choć ma sporo kompleksów. Uwielbia robić selfie, nie rozstaje się ze smartfonem, jest nieustannie w sieci – przede wszystkim na portalach społecznościowych.

Wasze zadanie polega na zbudowaniu jak najpełniejszego profilu opisanej wyżej osoby. Na otrzymanych arkuszach papieru stwórzcie plakat zawierający wszystkie informacje o waszej personie. To, co o niej wiecie, zapiszcie w formie haseł, słów kluczy, cytatów czy krótkich opisów. Odnosząc się do rzeczywistości waszej persony, używajcie konkretnych przykładów,.

Poniżej zestaw pytań, które pomogą zebrać i uporządkować wiedzę o waszej personie.

PODSTAWOWE INFORMACJE O TEJ OSOBIE

- Jak się nazywa?
- Rodzina (kto, ile osób, imiona, wiek)?
- Gdzie mieszka, uczy się, pracuje?
- Czym się interesuje?
- Jakie jedzenie lubi?
- Jak się ubiera?
- Jakiej muzyki słucha?
- Co ogląda w telewizji (kanały, programy)?

CHARAKTERYSTYKA

- Co ją cieszy, a co irytuje?
- Czy ktoś wywiera na nią presję (jedna osoba, grupa)?
- W czym jest dobra?
- Jakie osoby lubi, a jakich nie?
- Jaki ma stosunek do ludzi, do życia?
- Co mówią o niej bliscy, przyjaciele?
- Czy ulega trendom/modom (jeżeli tak, to jakim ostatnio)?
- Od czego rozpoczyna dzień?
- Jak kończy dzień?

CZAS WOLNY

- Jak spędza weekendy?
- W jaki sposób spędza czas wolny (z kim, gdzie)?
- Czy uprawia sport (jaki, jak często)?
- Dokąd jeździ, a dokąd chciałaby pojechać na wakacje?
- Gdzie i jak się bawi?
- Z jakich mediów korzysta?
- Jakie seriale, filmy, książki lubi?
- Jakie ma ulubione strony www?
- Ile czasu spędza w internecie?
- Jak korzysta z internetu i z nowych technologii?
- Z jakich narzędzi internetowych korzysta?
- Jakie są jej zachowania w cyberświecie?
- Jaką rolę w jej życiu odgrywają media społecznościowe?

Tomasz (2)

Tomasz mieszka w okazałym domu na przedmieściach dużego miasta. Ma żonę i dwójkę dzieci, z którymi uwielbia podróżować po świecie. Wspólnie odwiedzili już dwadzieścia pięć krajów. Pracuje na stanowisku kierowniczym w dużej korporacji. Praca pochłania dużą część jego życia, ale znajduje też czas na regularne treningi tenisa z przyjacielem. Każdy poranek zaczyna od biegania. Jego pasją są nowe technologie – ma mnóstwo gadżetów i sprzętów elektronicznych.

Wasze zadanie polega na zbudowaniu jak najpełniejszego profilu opisanej wyżej osoby. Na otrzymanych arkuszach papieru stwórzcie plakat zawierający wszystkie informacje o waszej personie. To, co o niej wiecie, zapiszcie w formie haseł, słów kluczy, cytatów czy krótkich opisów. Odnosząc się do rzeczywistości waszej persony, używajcie konkretnych przykładów,.

Poniżej zestaw pytań, które pomogą zebrać i uporządkować wiedzę o waszej personie.

PODSTAWOWE INFORMACJE O TEJ OSOBIE

- Jak się nazywa?
- Jaka jest jej rodzina (kto, ile osób, imiona, wiek)?
- Gdzie mieszka, uczy się, pracuje?
- Czym się interesuje?
- Jakie jedzenie lubi?
- Jak się ubiera?
- Jakiej muzyki słucha?
- Co ogląda w telewizji (kanały, programy)?

CHARAKTERYSTYKA

- Co ją cieszy, a co irytuje?
- Czy ktoś wywiera na nią presję (jedna osoba, grupa)?
- W czym jest dobra?
- Jakie osoby lubi, a jakich nie?
- Jaki ma stosunek do ludzi, do życia?
- Co mówią o niej bliscy, przyjaciele?
- Czy ulega trendom/modom (jeżeli tak, to jakim ostatnio)?
- Od czego rozpoczyna dzień?
- Jak kończy dzień?

CZAS WOLNY

- Jak spędza weekendy?
- W jaki sposób spędza czas wolny (z kim, gdzie)?
- Czy uprawia sport (jaki, jak często)?
- Dokąd jeździ, a dokąd chciałaby pojechać na wakacje?
- Gdzie i jak się bawi?
- Z jakich mediów korzysta?
- Jakie seriale, filmy, książki lubi?

- Jakie ma ulubione strony www?
- Ile czasu spędza w internecie?
- Jak korzysta z internetu i z nowych technologii?
- Z jakich narzędzi internetowych korzysta?
- Jakie są jej zachowania w cyberświecie?
- Jaką rolę w jej życiu odgrywają media społecznościowe?

Pani Konstancja (3)

Pani Konstancja ma 65 lat. Mieszka sama w pięknym, zabytkowym domu. Na ścianach wiszą czarno-białe zdjęcia jej dziadków na tle szlacheckiego dworku. Jej dzieci są już dorosłe i kilka lat temu wyprowadziły się z domu. W młodości chciała zostać pianistką i dziś z jej domu często dobiegają dźwięki rapsodii Liszta. Pracowała jako polonistka w elitarnym liceum, teraz jest już na emeryturze. Wciąż utrzymuje kontakty ze swoimi byłymi uczniami. Kocha stare polskie kino i poezję. Ma komputer i internet, ale wciąż trudno jej połapać się we wszystkich nowinkach technologicznych. Nie pamięta nigdy haseł, więc zapisuje je wszystkie w specjalnym notesiku, który zawsze ma przy sobie. Czasem prosi swoje dzieci, żeby pomogły jej w różnych komputerowych sprawach, one jednak nie mają cierpliwości tłumaczyć jej kolejny raz tego samego.

Wasze zadanie polega na zbudowaniu jak najpełniejszego profilu opisanej wyżej osoby. Na otrzymanych arkuszach papieru stwórzcie plakat zawierający wszystkie informacje o waszej personie. To, co o niej wiecie, zapiszcie w formie haseł, słów kluczy, cytatów czy krótkich opisów. Odnosząc się do rzeczywistości waszej persony, używajcie konkretnych przykładów,.

Poniżej zestaw pytań, które pomogą zebrać i uporządkować wiedzę o waszej personie.

PODSTAWOWE INFORMACJE

- Jak się nazywa?
- Jaka jest jej rodzina (kto, ile osób, imiona, wiek)?
- Gdzie mieszka, uczy się, pracuje?
- Czym się interesuje?
- Jakie jedzenie lubi?
- Jak się ubiera?
- Jakiej muzyki słucha?
- Co ogląda w telewizji (kanały, programy)?

CHARAKTERYSTYKA

- Co ją cieszy, a co irytuje?
- Czy ktoś wywiera na nią presję (jedna osoba, grupa)?
- W czym jest dobra?
- Jakie osoby lubi, a jakich nie?
- Jaki ma stosunek do ludzi, do życia?
- Co mówią o niej bliscy, przyjaciele?
- Czy ulega trendom/modom (jeżeli tak, to jakim ostatnio)?
- Od czego rozpoczyna dzień?
- Jak kończy dzień?

CZAS WOLNY

- Jak spędza weekendy?
- W jaki sposób spędza czas wolny (z kim, gdzie)?
- Czy uprawia sport (jaki, jak często)?
- Dokąd jeździ, a dokąd chciałaby pojechać na wakacje?
- Gdzie i jak się bawi?
- Z jakich mediów korzysta?
- Jakie seriale, filmy, książki lubi?
- Jakie ma ulubione strony www?
- Ile czasu spędza w internecie?
- Jak korzysta z internetu i z nowych technologii?
- Z jakich narzędzi internetowych korzysta?
- Jakie są jej zachowania w cyberświecie?
- Jaką rolę w jej życiu odgrywają media społecznościowe?

Pan Zbyszek (4)

Pan Zbyszek jest na emeryturze, wcześniej pracował w miejscowym zakładzie przetwórczym. Mieszka na wsi, gdzie od lat pełni funkcję sołtysa. Ma dwoje wnuków i często się nimi opiekuje. Mieszka z żoną, która pracuje na pół etatu, a wolny czas oboje spędzają w klubie seniora działającym przy wiejskiej świetlicy. Razem organizują w świetlicy różne aktywności dla mieszkańców ich miejscowości. Pan Zbyszek razem z dyrektorką miejscowej szkoły piszą wnioski o dofinansowanie projektów, które wymyślają dla lokalnej społeczności. Jest bardzo aktywny i nieustannie ma wrażenie, że dzień jest za krótki, żeby zdążyć ze wszystkim, co chciałby zrobić.

Wasze zadanie polega na zbudowaniu jak najpełniejszego profilu opisanej wyżej osoby. Na otrzymanych arkuszach papieru stwórzcie plakat zawierający wszystkie informacje o waszej personie. To, co o niej wiecie, zapiszcie w formie haseł, słów kluczy, cytatów czy krótkich opisów. Odnosząc się do rzeczywistości waszej persony, używajcie konkretnych przykładów.

Poniżej zestaw pytań, które pomogą zebrać i uporządkować wiedzę o waszej personie.

PODSTAWOWE INFORMACJE

- Jak się nazywa?
- Jaka jest jej rodzina (kto, ile osób, imiona, wiek)?
- Gdzie mieszka, uczy się, pracuje?
- Czym się interesuje?
- Jakie jedzenie lubi?
- Jak się ubiera?
- Jakiej muzyki słucha?
- Co ogląda w telewizji (kanały, programy)?

CHARAKTERYSTYKA

- Co ją cieszy, a co irytuje?
- Czy ktoś wywiera na nią presję (jedna osoba, grupa)?
- W czym jest dobra?
- Jakie osoby lubi, a jakich nie?
- Jaki ma stosunek do ludzi, do życia?
- Co mówią o niej bliscy, przyjaciele?
- Czy ulega trendom/modom (jeżeli tak, to jakim ostatnio)?
- Od czego rozpoczyna dzień?
- Jak kończy dzień?

CZAS WOLNY

- Jak spędza weekendy?
- W jaki sposób spędza czas wolny (z kim, gdzie)?
- Czy uprawia sport (jaki, jak często)?
- Dokąd jeździ, a dokąd chciałaby pojechać na wakacje?
- Gdzie i jak się bawi?
- Z jakich mediów korzysta?

- Jakie seriale, filmy, książki lubi?
- Jakie ma ulubione strony www?
- Ile czasu spędza w internecie?
- Jak korzysta z internetu i z nowych technologii?
- Z jakich narzędzi internetowych korzysta?
- Jakie są jej zachowania w cyberświecie?
- Jaką rolę w jej życiu odgrywają media społecznościowe?