**SCENARIUSZ 1**

**Tytuł warsztatu:**

|  |
| --- |
| Cyberbezpieczeństwo – poznaj zagrożenia i bądź bezpieczny/a w sieci |

**Opracowanie**: Małgorzata Bazan

**Odbiorcy:** bibliotekarze/rki z bibliotek naukowych, nauczyciele/ki akademiccy/ckie

**Liczebność grupy:** 15-20 osób

**Miejsce spotkania:** warsztaty mogą być przeprowadzone zdalnie lub stacjonarnie w sali z dostępem do komputera, internetu i rzutnika

**Czas trwania:** 120 min

**Cele ogólne:**

|  |
| --- |
| poznanie podstawowych zasad cyberbezpieczeństwa. |

**Metody:**

* prezentacja multimedialna,
* metody aktywne (plastry miodu, nasza aktywność w sieci, praca z personami, praca ze stronami internetowymi),
* dyskusja,
* mini-wykład,
* pokaz filmu.

**Formy pracy warsztatowej:**

* indywidualna,
* zespołowa,
* interaktywna.

**Materiały:**

* linki do istotnych informacji i narzędzi,
* załączniki.

**Narzędzia:**

* MS Teams, Jitsi, Zoom lub inne narzędzia pozwalające na aktywny udział wszystkich uczestników/czek w zajęciach zdalnych,
* narzędzia pozwalające na wzbogacenie zajęć: Jamboard, Mentimenter, Miro, Wisemapping,
* telefony komórkowe uczestników i uczestniczek/ów,
* flipchart, karteczki post-it, mazaki, flamastry, długopisy dostępne w sali podczas zajęć stacjonarnych.

**Przebieg warsztatu:**

Warsztat podzielony został na kilka tematów. W zależności od przebiegu warsztatu i czasu możesz wykorzystać wszystkie ćwiczenia, ale możesz także wybrać te, które wydają Ci się najbardziej interesujące.

1. **Ćwiczenie/aktywność**

**Tytuł: Wprowadzenie**

**Czas trwania: 5-7 min**

**Cele:**

* poznanie uczestników/czek,
* diagnoza zainteresowań i umiejętności uczestników/czek,
* integracja,
* przedstawienie programu szkolenia.

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **aplikacja, program, strona internetowa, cyberbezpieczeństwo, wykradanie danych, phishing, WiFi, wirus** |

**Opis:**

|  |
| --- |
| Zacznij od rundy zapoznawczej. Przedstaw się i powiedz, czym się zajmujesz, a także, jakie jest Twoje ulubione narzędzie/aplikacja. O to samo poproś pozostałe osoby.  Przedstaw ramowy plan warsztatów/program szkolenia. |

1. **Ćwiczenie/aktywność**

**Tytuł: Z czym kojarzy Ci się cyberbezpieczeństwo? – ćwiczenie z wykorzystaniem plastrów miodu. Rozmowa, dyskusja, refleksja.**

**Czas trwania: 10 min**

**Cele:**

* **wprowadzenie do tematu cyberbezpieczeństwa,**
* **diagnoza wiedzy uczestników/czek,**
* **zainteresowanie uczestniczek/ów tematem,**
* **zwrócenie uwagi na skalę zjawiska cyberbezpieczeństwa.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **haker, wykradanie danych, hejt, przemoc w sieci, kradzież z kont bankowych, kradzież tożsamości, ostrożność, bezpieczne hasła** |

**Opis aktywności:**

|  |
| --- |
| Rozpocznij ćwiczenie wstępne. Połóż przygotowane wcześniej plastry miodu (przykład znajdziesz w załączniku nr 1) na podłodze i poproś, aby uczestnicy/czki wpisali w nie wszystko, co kojarzy im się z zagadnieniem bezpieczeństwa w sieci, a następnie ułożyli mapę myśli lub mozaikę z pojedynczych plastrów. Jeżeli będziesz prowadzić zajęcia online, wykonaj to ćwiczenie, korzystając z bezpłatnego narzędzia, jakim jest Jamboard. Jest to najprostsza biała tablica, którą możesz udostępnić uczestnikom/czkom. Znajdziesz ją w narzędziach Google, gdy masz założone konto. Kiedy uruchomisz Jamboard, w panelu po lewej stronie ekranu znajdziesz przycisk „Notatka”. Są to wirtualne karteczki post-it. Poproś, aby wszystkie osoby wpisywały swoje skojarzenia na tych karteczkach, a później ułożyły z nich mapę myśli.  Po wykonanym ćwiczeniu odczytaj napisy w komórkach i krótko je omów. Zwróć uwagę, jak szeroki jest to temat i jak ważny dla współczesnego człowieka. Porozmawiaj z uczestnikami/czkami na temat skali problemu bezpieczeństwa w sieci (dotyczy wszystkich użytkowników/czek sieci). Jeżeli jesteś po lekturze trylogii Jakuba Szamałka pt.: *Ukryta sieć*, możesz zachęcić uczestników/czki do jej przeczytania, zwracając uwagę na pierwszą część (pt. *Cokolwiek wybierzesz*), która mówi o wykradaniu danych. |

1. **Ćwiczenie/aktywność: Nasza aktywność w sieci.**

**Czas trwania: 10 min**

**Cele:**

* **poznanie pojęcia: cyfrowy ślad,**
* **uświadomienie uczestniczkom/kom, że dbałość o bezpieczeństwo w sieci zaczyna się od własnych działań.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **cyfrowy ślad, dbałość o własne bezpieczeństwo w sieci** |

**Opis aktywności:**

|  |
| --- |
| Przeprowadź ćwiczenie nr 2, pt. *Nasza aktywność w sieci*. Poproś uczestników/czki o wypisanie na karteczkach post-it wszystkich aplikacji i stron internetowych, z których korzystają każdego dnia, zgodnie z zasadą: jedna karteczka – jedna aktywność (strona, aplikacja). Po wykonaniu zadania poproś, aby położyli karteczki na podłodze. W ten sposób stwórz obraz wszystkich działań uczestników/czek w internecie. Możesz powiedzieć, że jest to jak gdyby portret zbiorowy grupy. Omów poszczególne aplikacje i strony internetowe (np. powiedz: „Korzystacie z map Google. Jeżeli nie macie odpowiednich ustawień, pozostawiacie w sieci swoje dane geolokalizacyjne”. Albo: „Korzystacie z Facebooka, wrzucając do sieci swoje zdjęcia. Pozostawiacie w internecie informacje na temat swoich upodobań i preferencji”.), zwracając uwagę, że z punktu widzenia hakera wszystkie te aktywności to ślady pozostawione w internecie. Zakończcie ćwiczenie, mówiąc, że ochrona prywatności w sieci zaczyna się od własnych działań.  Ćwiczenie to możesz wykonać online, korzystając z poznanego już Jamboarda.  **Przed zajęciami możesz:**   * poznać inne narzędzia cyfrowe, z pomocą których wykonasz to ćwiczenie online, np.:   <https://miro.com/>, <https://en.linoit.com/>, <https://www.wisemapping.com/>. |

1. **Ćwiczenie/aktywność**

**Tytuł: Film i burza mózgów**

**Czas trwania: 25 min**

**Cele:**

* **poznanie działań wpływających na bezpieczeństwo w sieci.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **profile na portalach społecznościowych, ustawienia prywatności, publikacja zdjęć, oszczędne gospodarowanie danymi w sieci** |

**Opis aktywności:**

|  |
| --- |
| Odtwórz jeden z poniższych filmów:   * Norbert Rudaś, *Cyberprzemoc*:   <https://www.youtube.com/watch?v=XMcr2-Ke3I4> [dostęp: 1.10.2022].   * Rafał Jarząbek, *Uważaj, co udostępniasz. Social media stalker*:   <https://www.youtube.com/watch?v=CLRBYhd7e4Q> [dostęp: 1.10.2022].   * *Cyberbezpieczeństwo to nie tylko modne słowo.* Wywiad z Piotrem Koniecznym. Niebezpiecznik.pl:   <https://www.youtube.com/watch?v=jxTKGQoHjEw> [dostęp: 1.10.2022].  Po projekcji zapytaj uczestników/czki o wrażenia i refleksje związane z tym, co obejrzeli. Zainicjuj dyskusję na temat ochrony prywatności związanej z własnymi działaniami w sieci, z własną aktywnością. Wspólnie wypiszcie na flipcharcie wszystkie te zasady, które mogą nam pomóc chronić swoją prywatność w sieci.  Przykładowe zasady:   * korzystając z ustawień prywatności, „zamykamy” swoje profile w mediach społecznościowych tak, aby wyłącznie znajomi mieli dostęp do publikowanych przez nas informacji; * nie przyjmujemy do grona znajomych osób, których nie poznaliśmy w świecie pozawirtualnym; * nie publikujemy swoich intymnych zdjęć w internecie (np. w kostiumach kąpielowych); * nie oznaczamy nieustannie miejsc, w których przebywamy; * nie publikujemy tras naszych aktywności sportowych; * nie chwalimy się w sieci bogactwem; * nie publikujemy zdjęć z wyjazdów zagranicznych, na których obecnie przebywamy, gdy nasze mieszkanie pozostaje bez opieki.   **Przed zajęciami możesz:**   * pogłębić swoją wiedzę, poświęcając czas na obejrzenie jednego lub kilku dłuższych filmów związanych z cyberbezpieczeństwem, np.:    Dr Michał Jankowski Lorek, *Cyberbezpieczeństwo*:  <https://www.youtube.com/watch?v=evsJKRIK_nk> [dostęp 1.10.2022].  Piotr Konieczny, SECURE 2018, Niebezpiecznik.pl:  <https://www.youtube.com/watch?v=NsMw7hL5idw> [dostęp 1.10.2022].  Piotr Konieczny, *3 mity cybersecurity*, TEDxKatowice:  <https://www.youtube.com/watch?v=wDGAkp1sHM4> [dostęp 1.10.2022]. |

1. **Ćwiczenie/aktywność**

**Tytuł: Phishing. Czy łatwo kogoś zaatakować? Praca w parach/grupach/ indywidualna**

**Czas trwania: 20 min.**

**Cele:**

* **poznanie i zrozumienie zjawiska phishingu,**
* **uświadomienie, jak łatwo kogoś zaatakować w sieci, gdy nieroztropnie zostawia zbyt dużo informacji o sobie w sieci.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **phishing, kradzież danych, haker, kradzież pieniędzy, nierozsądne gospodarowanie danymi w sieci** |

**Opis aktywności:**

|  |
| --- |
| Wytłumacz uczestniczkom/kom, czym jest phishing i omów różne jego typy. Pokaż schemat ataku phishingowego, a następnie rozdaj wcześniej przygotowane persony (przykłady w załączniku nr 2).  Przeprowadź ćwiczenie nr 3. Poproś, aby uczestniczki/cy, pracując indywidualnie lub w grupach (decyzja należy do Ciebie), wyobrazili sobie, że są hakerami i na podstawie informacji z person atakują konkretne osoby. Ich zadanie polega na napisaniu maila skierowanego do wybranej osoby tak, aby wyłudzić od niej dane. Po upływie wyznaczonego czasu (ok. 5 min) poproś kilka osób (lub przedstawicieli/ek grup) o odczytanie swoich e-maili. Zapytaj, czy zadanie to było łatwe czy trudne. Zastanów się, w jaki sposób hakerzy zdobywają dane o użytkownikach sieci. Wróć do *Naszej aktywności w sieci* i obejrzanego filmu, mówiąc o tym, że sporo osób nie zwraca uwagi na oszczędne gospodarowanie swoimi danymi w sieci. Zaznacz, że ćwiczenie to służy jedynie uświadomieniu, iż nierozsądne gospodarowanie swoimi danymi w sieci, np. publikowanie zdjęć na niezabezpieczonych, otwartych kontach w mediach społecznościowych, prowadzi do narażenia na wykradanie danych. Ćwiczenie to nie jest natomiast zachętą do działań cyberprzestępczych.  **Przed zajęciami możesz:**   * zapoznać się z definicją i przykładami phishingu, np. na stronach:   <https://pl.wikipedia.org/wiki/Phishing> [dostęp 1.10.2022].  <https://kwestiabezpieczenstwa.pl/phishing/> [dostęp 1.10.2022].  <https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/> [dostęp 1.10.2022].  <https://niebezpiecznik.pl/post/jak-internetowi-zlodzieje-okradaja-bankowe-konta-polakow/> [dostęp 1.10.2022].   * przygotować, np. w formie prezentacji multimedialnej, kilka przykładów phishingu (znajdziesz je na podanych powyżej stronach). * znacznie pogłębić zagadnienie:   <https://okkoala.com/pl/articles/rodzaje-atakow-phishingowych> [dostęp 1.10.2022]. |

1. **Ćwiczenie/aktywność**

**Tytuł: Wycieki danych. Miniwykład i praca z telefonami komórkowymi**

**Czas trwania: 10 min.**

**Cele:**

* **poznanie mechanizmu wycieku danych ze stron internetowych,**
* **uświadomienie konieczności tworzenia trudnych, czyli bardziej bezpiecznych haseł.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **wyciek danych, hasło** |

**Opis aktywności:**

|  |
| --- |
| Wyjaśnij, czym są tzw. wycieki z kont, podaj kilka ich przykładów (znajdziesz je w linkach podanych w tym ćwiczeniu). Poproś, aby uczestniczki/cy, korzystając ze swoich telefonów komórkowych, weszli na stronę: [www.haveibeenpwned.com](http://www.haveibeenpwned.com/) i wpisali swój adres e-mail. Zapytaj, jakie informacje wyświetlają się na ekranach telefonów. Jeżeli strona ma kolor czerwony, oznacza to, że e-mail wyciekł z jakiejś strony internetowej. Lista pod spodem pokazuje, jakie to strony. Jeżeli widzimy kolor zielony, e-mail nie wyciekł z żadnej strony. Następnie poproś, aby uczestniczki/cy, również przy pomocy telefonów komórkowych, weszli na stronę: <https://www.security.org/how-secure-is-my-password/>, a potem wpisali hasło podobne do tego, które mają ustawione na swojej skrzynce pocztowej. Wyjaśnij, że strona pokazuje, jaki czas jest potrzebny, by „złamać” dane hasło. Podkreśl, że łamaniem haseł nie zajmują się dziś poważni cyberprzestępcy. Dziś robią to programy komputerowe, które przez cyberprzestępców są nam „podrzucane” i instalowane na naszych komputerach. Zatem wskazany poniżej hasła czas odnosi się do działania programu, a nie do działania człowieka.  **Przed zajęciami możesz:**   * zgłębić temat, korzystając ze stron:   <https://www.f-secure.com/pl/home/free-tools/identity-theft-checker> [dostęp 1.10.2022].  <https://www.nazwa.pl/blog/najwieksze-wycieki-danych-i-sposoby-ochrony> [dostęp 1.10.2022].  <https://www.youtube.com/watch?v=garf0n_ocFI> [dostęp 1.10.2022].   * przetestować samodzielnie podane w ćwiczeniu strony * przygotować nazwy stron lub kody QR i wyświetlić je na prezentacji (skorzystaj z generatora kodów, np.: <https://www.qr-online.pl/>) * poznać listę „najgorszych” haseł, by polecić tę lekturę uczestnikom/czkom:   <https://www.wirtualnemedia.pl/artykul/hasla-internetowe-najgorsze-najprostsze-na-czele-123456-i-password> [[dostęp 1.10.2022].](http://www.haveibeenpwned.com/) |

1. **Ćwiczenie/aktywność**

**Tytuł: Bezpieczne hasło. Burza mózgów**

**Czas trwania: 10 min**

**Cele:**

* **omówienie i przyswojenie zasad tworzenia bezpiecznych haseł.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **bezpieczne hasło** |

**Opis aktywności:**

|  |
| --- |
| Omów wraz z uczestnikami/czkami zasady tworzenia bezpiecznych haseł. Wypisz te zasady na flipcharcie lub wirtualnej białej tablicy:   * Hasło nie powinno być słowem, które można znaleźć w słowniku. * Hasło nie może również zawierać cyfr z numeru PESEL, dowodu osobistego czy paszportu. * Hasło powinno być kombinacją dużych i małych liter, cyfr oraz znaków specjalnych. * Hasło powinno zawierać od 12 do 18 znaków (choć może więcej). * Hasła nie powinniśmy zapisywać na komputerze ani na żadnej kartce doklejonej np. do monitora. * Nie używamy jednego hasła do wszystkich kont. Każde konto (np. skrzynka e-mail czy konto bankowe) powinno mieć inne hasło.   Pokaż metody na stworzenie bezpiecznego hasła i zapamiętanie go (informacje znajdziesz w podanych poniżej linkach). Jeżeli masz wystarczająco dużo czasu i ćwiczenia przebiegają sprawnie, możesz na końcu tej części poprosić uczestników/czki, aby ustawili bezpieczne hasła na swoich skrzynkach pocztowych.  **Przed zajęciami możesz:**   * zgłębić wiedzę, oglądając pierwszą część filmu dotyczącą bezpiecznych haseł (do ok. 15 minuty):   <https://www.youtube.com/watch?v=wXUxRB0S5qI&t=1027s> [dostęp 1.10.2022].   * zgłębić wiedzę, korzystając z artykułów:   <https://www.infor.pl/prawo/prawa-konsumenta/konsument-w-sieci/5246482,Bezpieczne-haslo-czyli-jakie.html> [dostęp 1.10.2022].  <https://www.dobreprogramy.pl/swiatowy-dzien-hasla-2022-zobacz-jak-zadbac-o-bezpieczenstwo,6763454921321248a> [dostęp 1.10.2022]. |

1. **Ćwiczenie/aktywność**

**Tytuł: Bezpieczne WiFi. Dyskusja kierowana**

**Czas trwania: 10 min.**

**Cele:**

* **omówienie zasad korzystania z WiFi,;**
* **przedstawienie zagrożeń wynikających z korzystania z publicznego WiFi.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **WiFi, połączenie szyfrowane i nieszyfrowane, klucz szyfrujący, bezpieczeństwo danych** |

**Opis aktywności:**

|  |
| --- |
| Zapytaj uczestników/czki, kto korzystał kiedykolwiek z WiFi w kawiarni lub innym publicznym miejscu. Zbierz głosy i zadaj kolejne pytanie: Czy jest to bezpieczne działanie w sieci? Po wysłuchaniu uczestników/czek poinformuj, że WiFi jest połączeniem nieszyfrowanym, a więc dane, które wpisujemy, np. login i hasło do konta bankowego, nie są zabezpieczone kluczem szyfrującym. Łatwo więc je przejąć i takie sytuacje mają rzeczywiście miejsce. Dlatego też możemy korzystać z WiFi w miejscu publicznym, gdy chcemy przejrzeć wiadomości z kraju lub świata albo poczytać prasę. Nie korzystamy jednak z tego rozwiązania, gdy musimy się gdziekolwiek zalogować. Wtedy korzystamy z internetu naszego operatora.  **Przed zajęciami możesz:**   * przeczytać artykuł: <https://trybawaryjny.pl/polaczenia-szyfrowane/> [dostęp 1.10.2022]. * pokazać slajdy z zamkniętą kłódką, by ten znak utrwalił się w pamięci uczestników/czek. |

1. **Ćwiczenie/aktywność**

**Tytuł: Typy wirusów. Wykład**

**Czas trwania:**

**Cele:**

* **przedstawienie podstawowych wiadomości na temat typów wirusów,**
* **uświadomienie konieczności instalowania i aktualizowania programów antywirusowych nie tylko na komputerach czy laptopach, ale też tabletach i smartfonach.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **wirus, instalowanie i aktualizowanie programów antywirusowych, bezpieczeństwo smartfona** |

**Opis aktywności:**

|  |
| --- |
| Omów podstawowe typy wirusów, opowiedz, jakie szkody wyrządzają i jak należy się przed nimi chronić. Razem z uczestniczkami/kami wypisz te zasady, np.:   * należy instalować i na bieżąco aktualizować oprogramowanie antywirusowe; * ochrona antywirusowa powinna dotyczyć wszystkich urządzeń, nie tylko komputerów czy laptopów, ale też tabletów i smartfonów; * należy raz w tygodniu skanować cały komputer w poszukiwaniu niebezpiecznych programów; * nie należy klikać w nieznane linki ani otwierać nieznanyche załącznikówi, które np. dostajemy pocztą mailową,; * nie należy klikać w żadne pop-up'y, czyli wyskakujące okienka, które pojawiają się na ekranie; * należy obserwować wydajność naszego komputera (np. czy działa wolno).   Typy wirusów znajdziesz w linkach pod spodem.  **Przed zajęciami możesz:**   * przeczytać artykuły:   <https://bitdefender.pl/jakie-sa-rodzaje-wirusow-ktore-moga-zainfekowac-komputer/> [dostęp 1.10.2022].  <https://www.omegasoft.pl/blog/rodzaje-wirusow-komputerowych/> [dostęp 1.10.2022].  <https://www.dell.com/support/kbdoc/pl-pl/000132699/jakie-s%C4%85-rodzaje-wirus%C3%B3w-oraz-szpieguj%C4%85cego-i-z%C5%82o%C5%9Bliwego-oprogramowania-kt%C3%B3re-mog%C4%85-zainfekowa%C4%87-m%C3%B3j-komputer> [dostęp 1.10.2022].  <https://scroll.morele.net/poradniki/czym-jest-wirus-komputerowy/> [dostęp 1.10.2022].   * przygotować slajd lub kilka slajdów, które w obrazowy sposób pomogą Ci wytłumaczyć, czym są wirusy i jakie są miedzy nimi różnice. |

1. **Ćwiczenie/aktywność**

**Tytuł: Zakończenie**

**Czas trwania: 5 min**

**Cele:**

* **podsumowanie warsztatu,**
* **uzyskanie informacji zwrotnej (np. które treści zdaniem uczestników/czek były najbardziej, a które najmniej przydatne)**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **informacja zwrotna, podziękowanie, pożegnanie** |

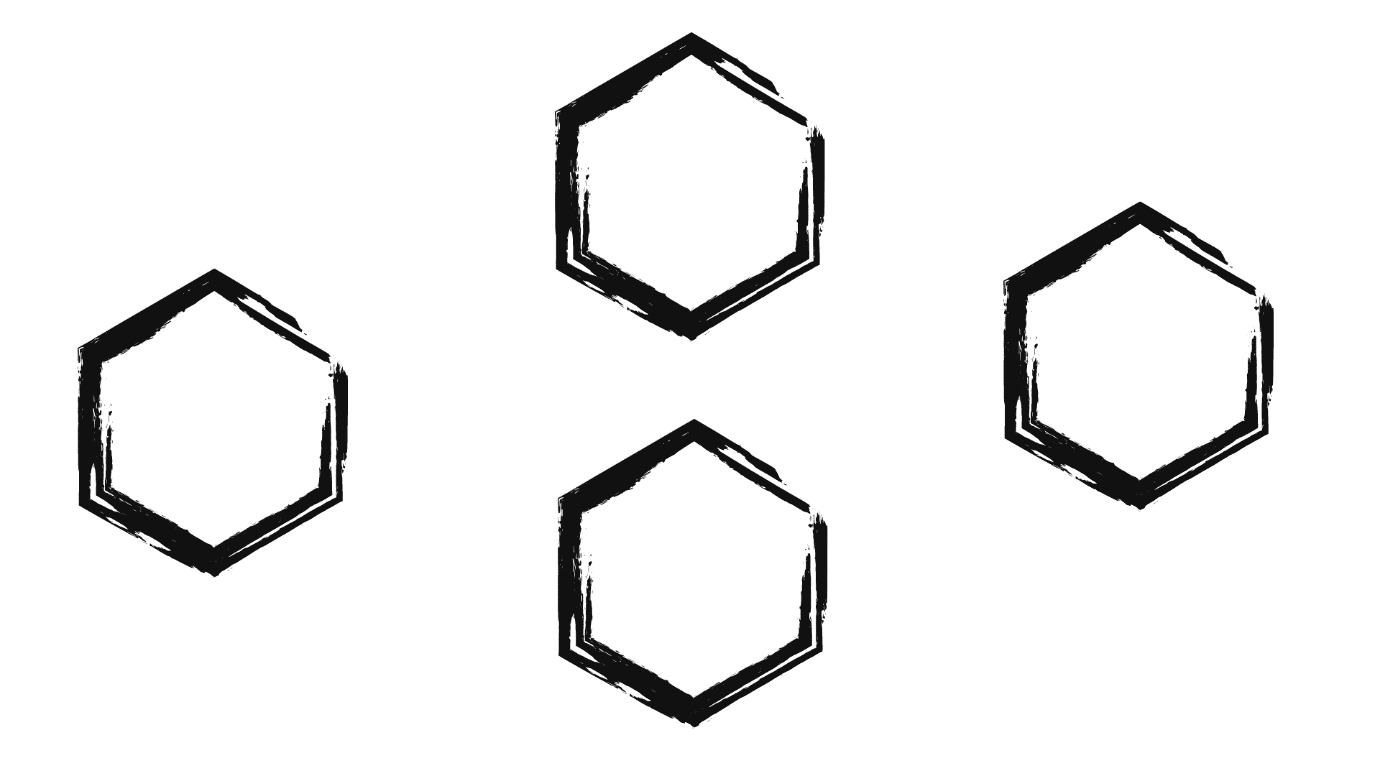
**Opis aktywności:**

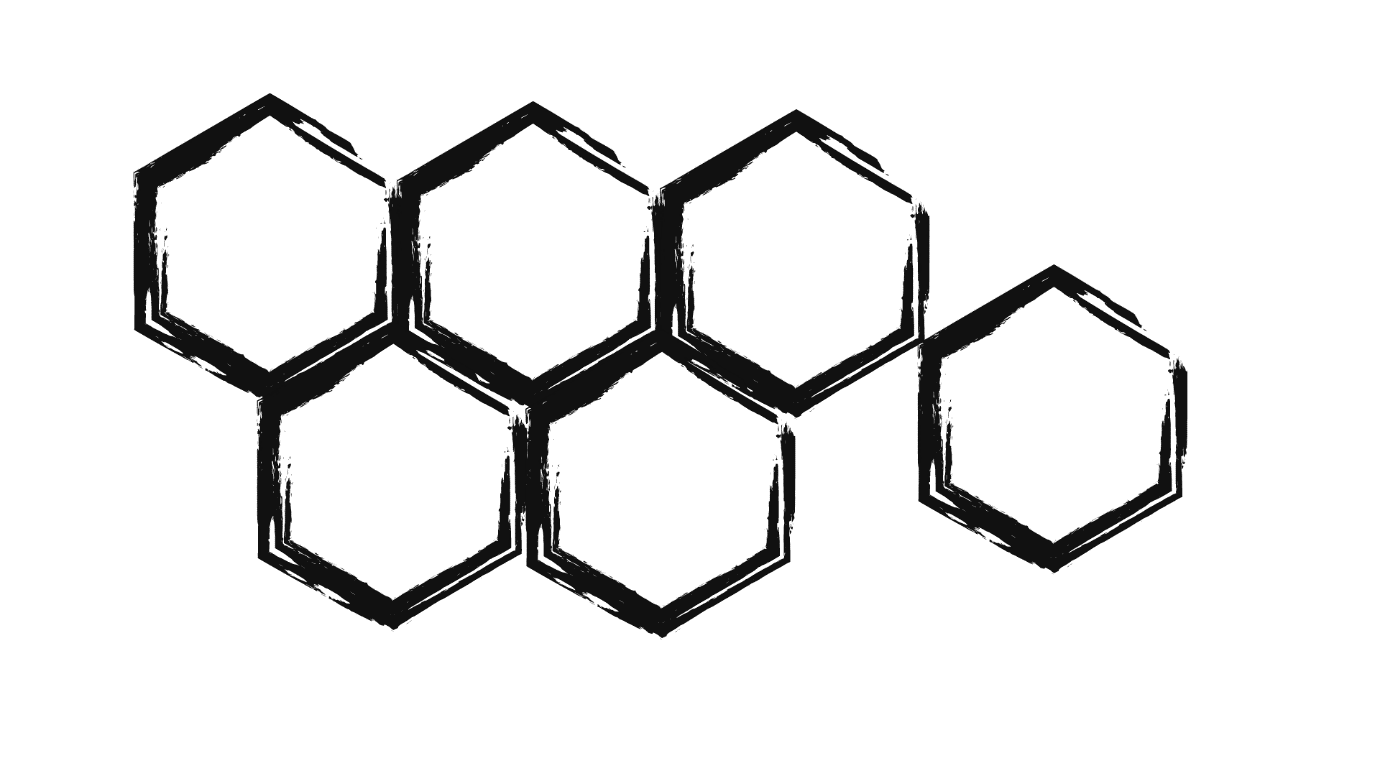
|  |
| --- |
| Zadaj pytanie: Co uczestnicy/czki biorą dla siebie, które informacje są dla nich najbardziej, a które najmniej przydatne? Pozbieraj odpowiedzi i podsumuj warsztat. Nie zapomnij podziękować uczestnikom/czkom za udział.  Jeżeli przeprowadzasz warsztat online lub jeżeli chcesz wzbogacić warsztat stacjonarny, skorzystaj z narzędzia Mentimeter, by zebrać odpowiedzi. Możesz ustawić opcję tworzenia chmury słów i skojarzeń.  **Przed zajęciami możesz:**   * [założyć bezpłatne konto:](https://www.mentimeter.com/) * <https://www.mentimeter.com/> * poznać narzędzie Mentimenter:   <https://mcdn.nazwa.pl/DORADCY/sykulska/Mentimeter.pdf> [dostęp 1.10.2022]. |

**Załącznik nr 1.**

Plastry miodu

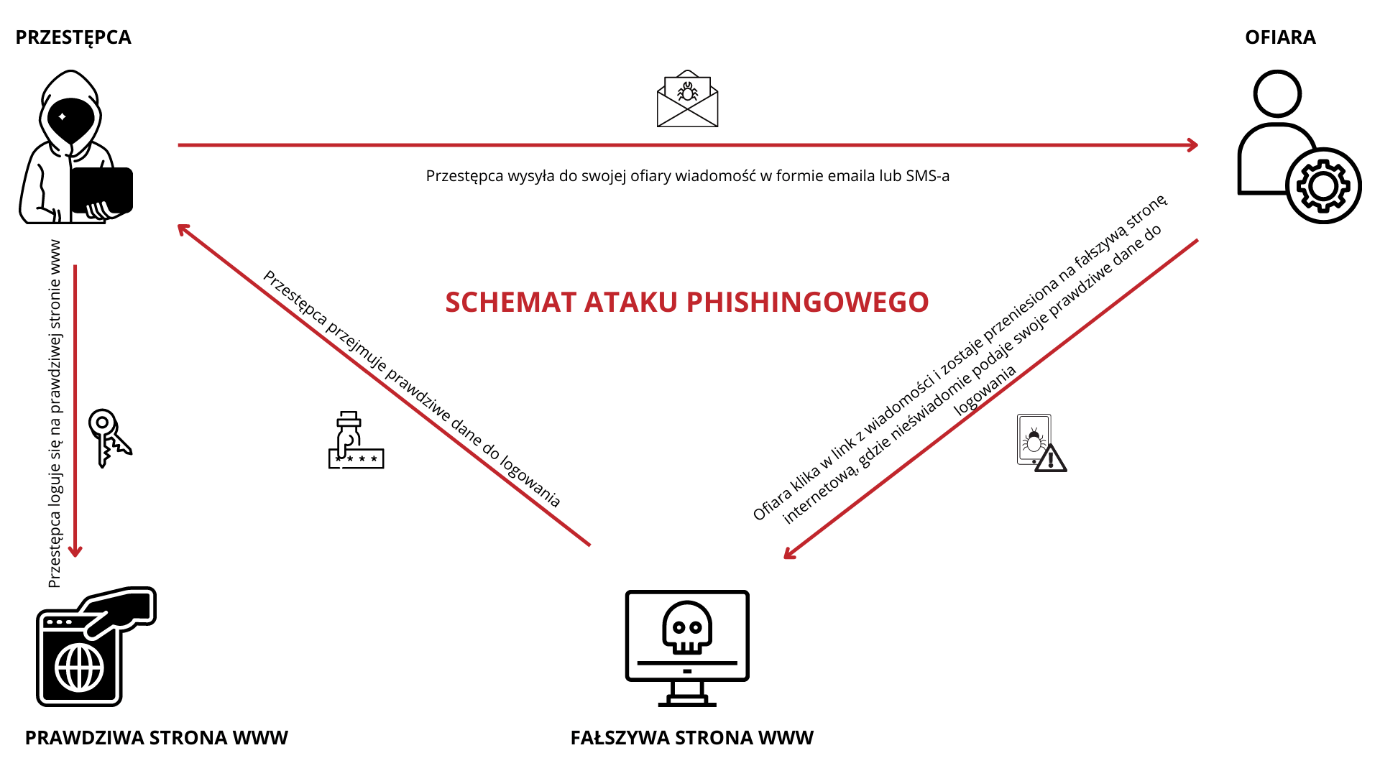
Wytnij dowolnej wielkości pojedyncze plastry i wręcz je uczestnikom i uczestni/czkom. Po wpisaniu skojarzeń poproś, aby utworzyli mapę, łącząc ze sobą pojedyncze elementy.





Załącznik nr 2.

**Schemat ataku phishingowego:**



**Przykładowe persony:**



**SCENARIUSZ 8**

**Tytuł warsztatu:**

|  |
| --- |
| Cyberbezpieczeństwo – poznaj zagrożenia i bądź bezpieczny/a w sieci |

**Opracowanie**: Małgorzata Bazan

**Odbiorcy:** bibliotekarze/rki z bibliotek naukowych, nauczyciele/ki akademiccy/ckie

**Liczebność grupy:** 15-20 osób

**Miejsce spotkania:** warsztaty mogą być przeprowadzone zdalnie lub stacjonarnie w sali z dostępem do komputera, internetu i rzutnika

**Czas trwania:** 120 min

**Cele ogólne:**

|  |
| --- |
| poznanie podstawowych zasad cyberbezpieczeństwa. |

**Metody:**

* prezentacja multimedialna,
* metody aktywne (plastry miodu, nasza aktywność w sieci, praca z personami, praca ze stronami internetowymi),
* dyskusja,
* mini-wykład,
* pokaz filmu.

**Formy pracy warsztatowej:**

* indywidualna,
* zespołowa,
* interaktywna.

**Materiały:**

* linki do istotnych informacji i narzędzi,
* załączniki.

**Narzędzia:**

* MS Teams, Jitsi, Zoom lub inne narzędzia pozwalające na aktywny udział wszystkich uczestników/czek w zajęciach zdalnych,
* narzędzia pozwalające na wzbogacenie zajęć: Jamboard, Mentimenter, Miro, Wisemapping,
* telefony komórkowe uczestników i uczestniczek/ów,
* flipchart, karteczki post-it, mazaki, flamastry, długopisy dostępne w sali podczas zajęć stacjonarnych.

**Przebieg warsztatu:**

Warsztat podzielony został na kilka tematów. W zależności od przebiegu warsztatu i czasu możesz wykorzystać wszystkie ćwiczenia, ale możesz także wybrać te, które wydają Ci się najbardziej interesujące.

1. **Ćwiczenie/aktywność**

**Tytuł: Wprowadzenie**

**Czas trwania: 5-7 min**

**Cele:**

* poznanie uczestników/czek,
* diagnoza zainteresowań i umiejętności uczestników/czek,
* integracja,
* przedstawienie programu szkolenia.

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **aplikacja, program, strona internetowa, cyberbezpieczeństwo, wykradanie danych, phishing, WiFi, wirus** |

**Opis:**

|  |
| --- |
| Zacznij od rundy zapoznawczej. Przedstaw się i powiedz, czym się zajmujesz, a także, jakie jest Twoje ulubione narzędzie/aplikacja. O to samo poproś pozostałe osoby.  Przedstaw ramowy plan warsztatów/program szkolenia. |

1. **Ćwiczenie/aktywność**

**Tytuł: Z czym kojarzy Ci się cyberbezpieczeństwo? – ćwiczenie z wykorzystaniem plastrów miodu. Rozmowa, dyskusja, refleksja.**

**Czas trwania: 10 min**

**Cele:**

* **wprowadzenie do tematu cyberbezpieczeństwa,**
* **diagnoza wiedzy uczestników/czek,**
* **zainteresowanie uczestniczek/ów tematem,**
* **zwrócenie uwagi na skalę zjawiska cyberbezpieczeństwa.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **haker, wykradanie danych, hejt, przemoc w sieci, kradzież z kont bankowych, kradzież tożsamości, ostrożność, bezpieczne hasła** |

**Opis aktywności:**

|  |
| --- |
| Rozpocznij ćwiczenie wstępne. Połóż przygotowane wcześniej plastry miodu (przykład znajdziesz w załączniku nr 1) na podłodze i poproś, aby uczestnicy/czki wpisali w nie wszystko, co kojarzy im się z zagadnieniem bezpieczeństwa w sieci, a następnie ułożyli mapę myśli lub mozaikę z pojedynczych plastrów. Jeżeli będziesz prowadzić zajęcia online, wykonaj to ćwiczenie, korzystając z bezpłatnego narzędzia, jakim jest Jamboard. Jest to najprostsza biała tablica, którą możesz udostępnić uczestnikom/czkom. Znajdziesz ją w narzędziach Google, gdy masz założone konto. Kiedy uruchomisz Jamboard, w panelu po lewej stronie ekranu znajdziesz przycisk „Notatka”. Są to wirtualne karteczki post-it. Poproś, aby wszystkie osoby wpisywały swoje skojarzenia na tych karteczkach, a później ułożyły z nich mapę myśli.  Po wykonanym ćwiczeniu odczytaj napisy w komórkach i krótko je omów. Zwróć uwagę, jak szeroki jest to temat i jak ważny dla współczesnego człowieka. Porozmawiaj z uczestnikami/czkami na temat skali problemu bezpieczeństwa w sieci (dotyczy wszystkich użytkowników/czek sieci). Jeżeli jesteś po lekturze trylogii Jakuba Szamałka pt.: *Ukryta sieć*, możesz zachęcić uczestników/czki do jej przeczytania, zwracając uwagę na pierwszą część (pt. *Cokolwiek wybierzesz*), która mówi o wykradaniu danych. |

1. **Ćwiczenie/aktywność: Nasza aktywność w sieci.**

**Czas trwania: 10 min**

**Cele:**

* **poznanie pojęcia: cyfrowy ślad,**
* **uświadomienie uczestniczkom/kom, że dbałość o bezpieczeństwo w sieci zaczyna się od własnych działań.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **cyfrowy ślad, dbałość o własne bezpieczeństwo w sieci** |

**Opis aktywności:**

|  |
| --- |
| Przeprowadź ćwiczenie nr 2, pt. *Nasza aktywność w sieci*. Poproś uczestników/czki o wypisanie na karteczkach post-it wszystkich aplikacji i stron internetowych, z których korzystają każdego dnia, zgodnie z zasadą: jedna karteczka – jedna aktywność (strona, aplikacja). Po wykonaniu zadania poproś, aby położyli karteczki na podłodze. W ten sposób stwórz obraz wszystkich działań uczestników/czek w internecie. Możesz powiedzieć, że jest to jak gdyby portret zbiorowy grupy. Omów poszczególne aplikacje i strony internetowe (np. powiedz: „Korzystacie z map Google. Jeżeli nie macie odpowiednich ustawień, pozostawiacie w sieci swoje dane geolokalizacyjne”. Albo: „Korzystacie z Facebooka, wrzucając do sieci swoje zdjęcia. Pozostawiacie w internecie informacje na temat swoich upodobań i preferencji”.), zwracając uwagę, że z punktu widzenia hakera wszystkie te aktywności to ślady pozostawione w internecie. Zakończcie ćwiczenie, mówiąc, że ochrona prywatności w sieci zaczyna się od własnych działań.  Ćwiczenie to możesz wykonać online, korzystając z poznanego już Jamboarda.  **Przed zajęciami możesz:**   * poznać inne narzędzia cyfrowe, z pomocą których wykonasz to ćwiczenie online, np.:   <https://miro.com/>, <https://en.linoit.com/>, <https://www.wisemapping.com/>. |

1. **Ćwiczenie/aktywność**

**Tytuł: Film i burza mózgów**

**Czas trwania: 25 min**

**Cele:**

* **poznanie działań wpływających na bezpieczeństwo w sieci.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **profile na portalach społecznościowych, ustawienia prywatności, publikacja zdjęć, oszczędne gospodarowanie danymi w sieci** |

**Opis aktywności:**

|  |
| --- |
| Odtwórz jeden z poniższych filmów:   * Norbert Rudaś, *Cyberprzemoc*:   <https://www.youtube.com/watch?v=XMcr2-Ke3I4> [dostęp: 1.10.2022].   * Rafał Jarząbek, *Uważaj, co udostępniasz. Social media stalker*:   <https://www.youtube.com/watch?v=CLRBYhd7e4Q> [dostęp: 1.10.2022].   * *Cyberbezpieczeństwo to nie tylko modne słowo.* Wywiad z Piotrem Koniecznym. Niebezpiecznik.pl:   <https://www.youtube.com/watch?v=jxTKGQoHjEw> [dostęp: 1.10.2022].  Po projekcji zapytaj uczestników/czki o wrażenia i refleksje związane z tym, co obejrzeli. Zainicjuj dyskusję na temat ochrony prywatności związanej z własnymi działaniami w sieci, z własną aktywnością. Wspólnie wypiszcie na flipcharcie wszystkie te zasady, które mogą nam pomóc chronić swoją prywatność w sieci.  Przykładowe zasady:   * korzystając z ustawień prywatności, „zamykamy” swoje profile w mediach społecznościowych tak, aby wyłącznie znajomi mieli dostęp do publikowanych przez nas informacji; * nie przyjmujemy do grona znajomych osób, których nie poznaliśmy w świecie pozawirtualnym; * nie publikujemy swoich intymnych zdjęć w internecie (np. w kostiumach kąpielowych); * nie oznaczamy nieustannie miejsc, w których przebywamy; * nie publikujemy tras naszych aktywności sportowych; * nie chwalimy się w sieci bogactwem; * nie publikujemy zdjęć z wyjazdów zagranicznych, na których obecnie przebywamy, gdy nasze mieszkanie pozostaje bez opieki.   **Przed zajęciami możesz:**   * pogłębić swoją wiedzę, poświęcając czas na obejrzenie jednego lub kilku dłuższych filmów związanych z cyberbezpieczeństwem, np.:    Dr Michał Jankowski Lorek, *Cyberbezpieczeństwo*:  <https://www.youtube.com/watch?v=evsJKRIK_nk> [dostęp 1.10.2022].  Piotr Konieczny, SECURE 2018, Niebezpiecznik.pl:  <https://www.youtube.com/watch?v=NsMw7hL5idw> [dostęp 1.10.2022].  Piotr Konieczny, *3 mity cybersecurity*, TEDxKatowice:  <https://www.youtube.com/watch?v=wDGAkp1sHM4> [dostęp 1.10.2022]. |

1. **Ćwiczenie/aktywność**

**Tytuł: Phishing. Czy łatwo kogoś zaatakować? Praca w parach/grupach/ indywidualna**

**Czas trwania: 20 min.**

**Cele:**

* **poznanie i zrozumienie zjawiska phishingu,**
* **uświadomienie, jak łatwo kogoś zaatakować w sieci, gdy nieroztropnie zostawia zbyt dużo informacji o sobie w sieci.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **phishing, kradzież danych, haker, kradzież pieniędzy, nierozsądne gospodarowanie danymi w sieci** |

**Opis aktywności:**

|  |
| --- |
| Wytłumacz uczestniczkom/kom, czym jest phishing i omów różne jego typy. Pokaż schemat ataku phishingowego, a następnie rozdaj wcześniej przygotowane persony (przykłady w załączniku nr 2).  Przeprowadź ćwiczenie nr 3. Poproś, aby uczestniczki/cy, pracując indywidualnie lub w grupach (decyzja należy do Ciebie), wyobrazili sobie, że są hakerami i na podstawie informacji z person atakują konkretne osoby. Ich zadanie polega na napisaniu maila skierowanego do wybranej osoby tak, aby wyłudzić od niej dane. Po upływie wyznaczonego czasu (ok. 5 min) poproś kilka osób (lub przedstawicieli/ek grup) o odczytanie swoich e-maili. Zapytaj, czy zadanie to było łatwe czy trudne. Zastanów się, w jaki sposób hakerzy zdobywają dane o użytkownikach sieci. Wróć do *Naszej aktywności w sieci* i obejrzanego filmu, mówiąc o tym, że sporo osób nie zwraca uwagi na oszczędne gospodarowanie swoimi danymi w sieci. Zaznacz, że ćwiczenie to służy jedynie uświadomieniu, iż nierozsądne gospodarowanie swoimi danymi w sieci, np. publikowanie zdjęć na niezabezpieczonych, otwartych kontach w mediach społecznościowych, prowadzi do narażenia na wykradanie danych. Ćwiczenie to nie jest natomiast zachętą do działań cyberprzestępczych.  **Przed zajęciami możesz:**   * zapoznać się z definicją i przykładami phishingu, np. na stronach:   <https://pl.wikipedia.org/wiki/Phishing> [dostęp 1.10.2022].  <https://kwestiabezpieczenstwa.pl/phishing/> [dostęp 1.10.2022].  <https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/> [dostęp 1.10.2022].  <https://niebezpiecznik.pl/post/jak-internetowi-zlodzieje-okradaja-bankowe-konta-polakow/> [dostęp 1.10.2022].   * przygotować, np. w formie prezentacji multimedialnej, kilka przykładów phishingu (znajdziesz je na podanych powyżej stronach). * znacznie pogłębić zagadnienie:   <https://okkoala.com/pl/articles/rodzaje-atakow-phishingowych> [dostęp 1.10.2022]. |

1. **Ćwiczenie/aktywność**

**Tytuł: Wycieki danych. Miniwykład i praca z telefonami komórkowymi**

**Czas trwania: 10 min.**

**Cele:**

* **poznanie mechanizmu wycieku danych ze stron internetowych,**
* **uświadomienie konieczności tworzenia trudnych, czyli bardziej bezpiecznych haseł.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **wyciek danych, hasło** |

**Opis aktywności:**

|  |
| --- |
| Wyjaśnij, czym są tzw. wycieki z kont, podaj kilka ich przykładów (znajdziesz je w linkach podanych w tym ćwiczeniu). Poproś, aby uczestniczki/cy, korzystając ze swoich telefonów komórkowych, weszli na stronę: [www.haveibeenpwned.com](http://www.haveibeenpwned.com/) i wpisali swój adres e-mail. Zapytaj, jakie informacje wyświetlają się na ekranach telefonów. Jeżeli strona ma kolor czerwony, oznacza to, że e-mail wyciekł z jakiejś strony internetowej. Lista pod spodem pokazuje, jakie to strony. Jeżeli widzimy kolor zielony, e-mail nie wyciekł z żadnej strony. Następnie poproś, aby uczestniczki/cy, również przy pomocy telefonów komórkowych, weszli na stronę: <https://www.security.org/how-secure-is-my-password/>, a potem wpisali hasło podobne do tego, które mają ustawione na swojej skrzynce pocztowej. Wyjaśnij, że strona pokazuje, jaki czas jest potrzebny, by „złamać” dane hasło. Podkreśl, że łamaniem haseł nie zajmują się dziś poważni cyberprzestępcy. Dziś robią to programy komputerowe, które przez cyberprzestępców są nam „podrzucane” i instalowane na naszych komputerach. Zatem wskazany poniżej hasła czas odnosi się do działania programu, a nie do działania człowieka.  **Przed zajęciami możesz:**   * zgłębić temat, korzystając ze stron:   <https://www.f-secure.com/pl/home/free-tools/identity-theft-checker> [dostęp 1.10.2022].  <https://www.nazwa.pl/blog/najwieksze-wycieki-danych-i-sposoby-ochrony> [dostęp 1.10.2022].  <https://www.youtube.com/watch?v=garf0n_ocFI> [dostęp 1.10.2022].   * przetestować samodzielnie podane w ćwiczeniu strony * przygotować nazwy stron lub kody QR i wyświetlić je na prezentacji (skorzystaj z generatora kodów, np.: <https://www.qr-online.pl/>) * poznać listę „najgorszych” haseł, by polecić tę lekturę uczestnikom/czkom:   <https://www.wirtualnemedia.pl/artykul/hasla-internetowe-najgorsze-najprostsze-na-czele-123456-i-password> [[dostęp 1.10.2022].](http://www.haveibeenpwned.com/) |

1. **Ćwiczenie/aktywność**

**Tytuł: Bezpieczne hasło. Burza mózgów**

**Czas trwania: 10 min**

**Cele:**

* **omówienie i przyswojenie zasad tworzenia bezpiecznych haseł.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **bezpieczne hasło** |

**Opis aktywności:**

|  |
| --- |
| Omów wraz z uczestnikami/czkami zasady tworzenia bezpiecznych haseł. Wypisz te zasady na flipcharcie lub wirtualnej białej tablicy:   * Hasło nie powinno być słowem, które można znaleźć w słowniku. * Hasło nie może również zawierać cyfr z numeru PESEL, dowodu osobistego czy paszportu. * Hasło powinno być kombinacją dużych i małych liter, cyfr oraz znaków specjalnych. * Hasło powinno zawierać od 12 do 18 znaków (choć może więcej). * Hasła nie powinniśmy zapisywać na komputerze ani na żadnej kartce doklejonej np. do monitora. * Nie używamy jednego hasła do wszystkich kont. Każde konto (np. skrzynka e-mail czy konto bankowe) powinno mieć inne hasło.   Pokaż metody na stworzenie bezpiecznego hasła i zapamiętanie go (informacje znajdziesz w podanych poniżej linkach). Jeżeli masz wystarczająco dużo czasu i ćwiczenia przebiegają sprawnie, możesz na końcu tej części poprosić uczestników/czki, aby ustawili bezpieczne hasła na swoich skrzynkach pocztowych.  **Przed zajęciami możesz:**   * zgłębić wiedzę, oglądając pierwszą część filmu dotyczącą bezpiecznych haseł (do ok. 15 minuty):   <https://www.youtube.com/watch?v=wXUxRB0S5qI&t=1027s> [dostęp 1.10.2022].   * zgłębić wiedzę, korzystając z artykułów:   <https://www.infor.pl/prawo/prawa-konsumenta/konsument-w-sieci/5246482,Bezpieczne-haslo-czyli-jakie.html> [dostęp 1.10.2022].  <https://www.dobreprogramy.pl/swiatowy-dzien-hasla-2022-zobacz-jak-zadbac-o-bezpieczenstwo,6763454921321248a> [dostęp 1.10.2022]. |

1. **Ćwiczenie/aktywność**

**Tytuł: Bezpieczne WiFi. Dyskusja kierowana**

**Czas trwania: 10 min.**

**Cele:**

* **omówienie zasad korzystania z WiFi,;**
* **przedstawienie zagrożeń wynikających z korzystania z publicznego WiFi.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **WiFi, połączenie szyfrowane i nieszyfrowane, klucz szyfrujący, bezpieczeństwo danych** |

**Opis aktywności:**

|  |
| --- |
| Zapytaj uczestników/czki, kto korzystał kiedykolwiek z WiFi w kawiarni lub innym publicznym miejscu. Zbierz głosy i zadaj kolejne pytanie: Czy jest to bezpieczne działanie w sieci? Po wysłuchaniu uczestników/czek poinformuj, że WiFi jest połączeniem nieszyfrowanym, a więc dane, które wpisujemy, np. login i hasło do konta bankowego, nie są zabezpieczone kluczem szyfrującym. Łatwo więc je przejąć i takie sytuacje mają rzeczywiście miejsce. Dlatego też możemy korzystać z WiFi w miejscu publicznym, gdy chcemy przejrzeć wiadomości z kraju lub świata albo poczytać prasę. Nie korzystamy jednak z tego rozwiązania, gdy musimy się gdziekolwiek zalogować. Wtedy korzystamy z internetu naszego operatora.  **Przed zajęciami możesz:**   * przeczytać artykuł: <https://trybawaryjny.pl/polaczenia-szyfrowane/> [dostęp 1.10.2022]. * pokazać slajdy z zamkniętą kłódką, by ten znak utrwalił się w pamięci uczestników/czek. |

1. **Ćwiczenie/aktywność**

**Tytuł: Typy wirusów. Wykład**

**Czas trwania:**

**Cele:**

* **przedstawienie podstawowych wiadomości na temat typów wirusów,**
* **uświadomienie konieczności instalowania i aktualizowania programów antywirusowych nie tylko na komputerach czy laptopach, ale też tabletach i smartfonach.**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **wirus, instalowanie i aktualizowanie programów antywirusowych, bezpieczeństwo smartfona** |

**Opis aktywności:**

|  |
| --- |
| Omów podstawowe typy wirusów, opowiedz, jakie szkody wyrządzają i jak należy się przed nimi chronić. Razem z uczestniczkami/kami wypisz te zasady, np.:   * należy instalować i na bieżąco aktualizować oprogramowanie antywirusowe; * ochrona antywirusowa powinna dotyczyć wszystkich urządzeń, nie tylko komputerów czy laptopów, ale też tabletów i smartfonów; * należy raz w tygodniu skanować cały komputer w poszukiwaniu niebezpiecznych programów; * nie należy klikać w nieznane linki ani otwierać nieznanyche załącznikówi, które np. dostajemy pocztą mailową,; * nie należy klikać w żadne pop-up'y, czyli wyskakujące okienka, które pojawiają się na ekranie; * należy obserwować wydajność naszego komputera (np. czy działa wolno).   Typy wirusów znajdziesz w linkach pod spodem.  **Przed zajęciami możesz:**   * przeczytać artykuły:   <https://bitdefender.pl/jakie-sa-rodzaje-wirusow-ktore-moga-zainfekowac-komputer/> [dostęp 1.10.2022].  <https://www.omegasoft.pl/blog/rodzaje-wirusow-komputerowych/> [dostęp 1.10.2022].  <https://www.dell.com/support/kbdoc/pl-pl/000132699/jakie-s%C4%85-rodzaje-wirus%C3%B3w-oraz-szpieguj%C4%85cego-i-z%C5%82o%C5%9Bliwego-oprogramowania-kt%C3%B3re-mog%C4%85-zainfekowa%C4%87-m%C3%B3j-komputer> [dostęp 1.10.2022].  <https://scroll.morele.net/poradniki/czym-jest-wirus-komputerowy/> [dostęp 1.10.2022].   * przygotować slajd lub kilka slajdów, które w obrazowy sposób pomogą Ci wytłumaczyć, czym są wirusy i jakie są miedzy nimi różnice. |

1. **Ćwiczenie/aktywność**

**Tytuł: Zakończenie**

**Czas trwania: 5 min**

**Cele:**

* **podsumowanie warsztatu,**
* **uzyskanie informacji zwrotnej (np. które treści zdaniem uczestników/czek były najbardziej, a które najmniej przydatne)**

**Główne przekazy, myśli lub zdania, które mają zapamiętać osoby uczestniczące:**

|  |
| --- |
| **informacja zwrotna, podziękowanie, pożegnanie** |

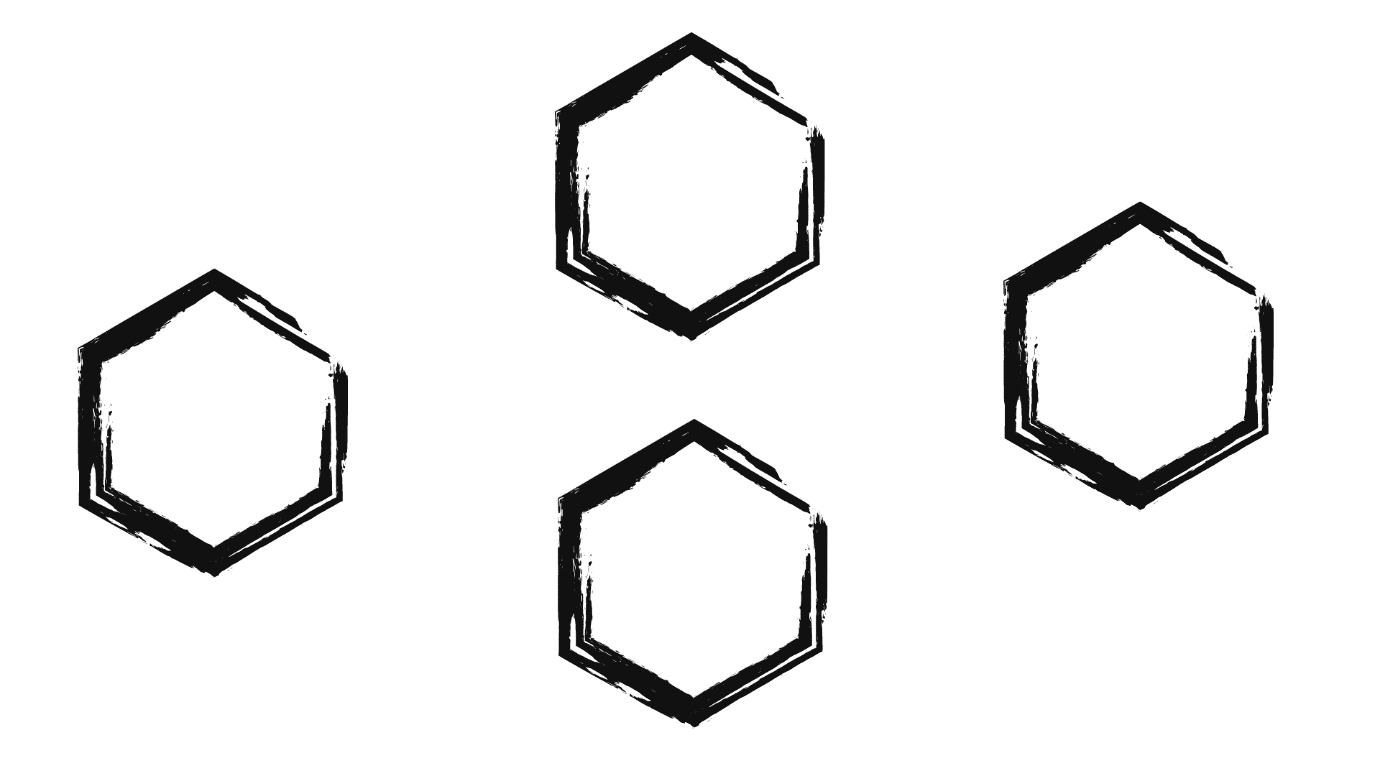
**Opis aktywności:**

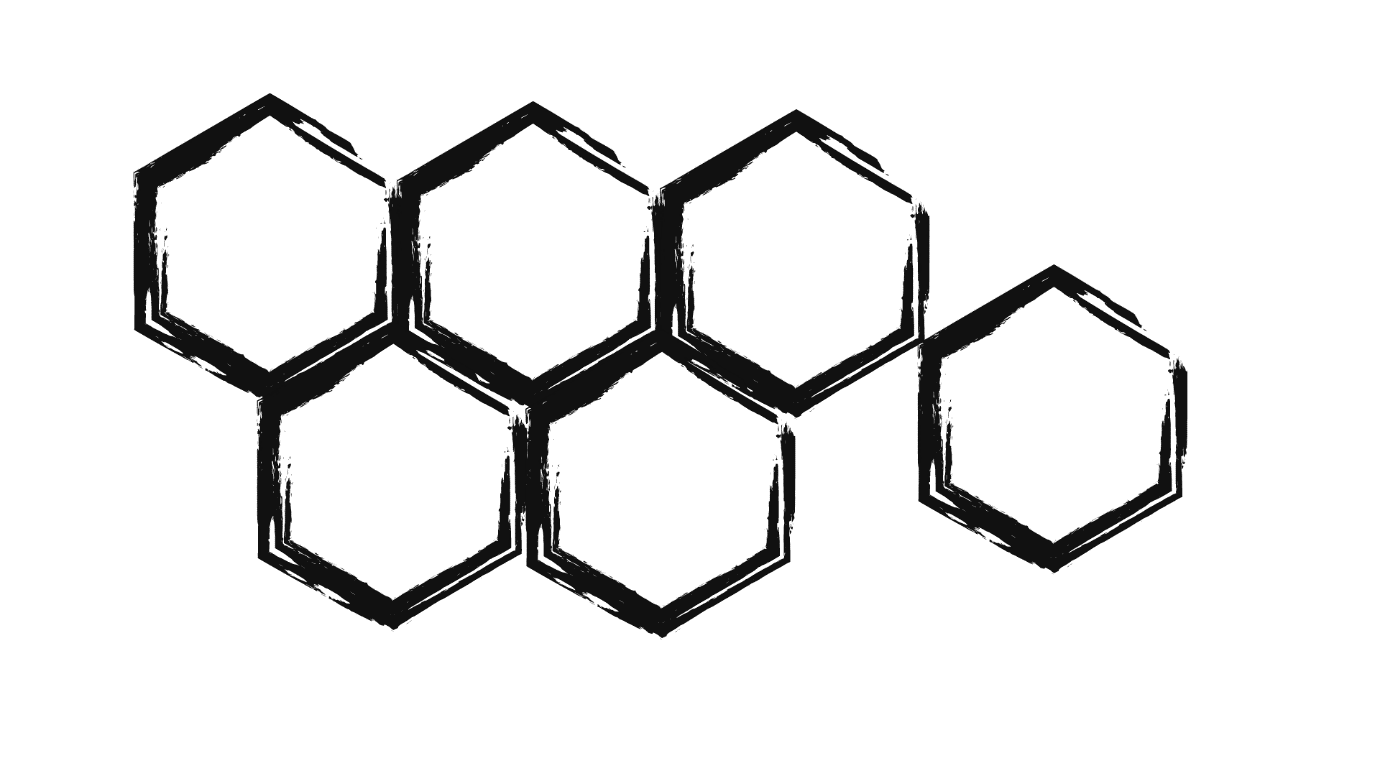
|  |
| --- |
| Zadaj pytanie: Co uczestnicy/czki biorą dla siebie, które informacje są dla nich najbardziej, a które najmniej przydatne? Pozbieraj odpowiedzi i podsumuj warsztat. Nie zapomnij podziękować uczestnikom/czkom za udział.  Jeżeli przeprowadzasz warsztat online lub jeżeli chcesz wzbogacić warsztat stacjonarny, skorzystaj z narzędzia Mentimeter, by zebrać odpowiedzi. Możesz ustawić opcję tworzenia chmury słów i skojarzeń.  **Przed zajęciami możesz:**   * [założyć bezpłatne konto:](https://www.mentimeter.com/) * <https://www.mentimeter.com/> * poznać narzędzie Mentimenter:   <https://mcdn.nazwa.pl/DORADCY/sykulska/Mentimeter.pdf> [dostęp 1.10.2022]. |

**Załącznik nr 1.**

Plastry miodu

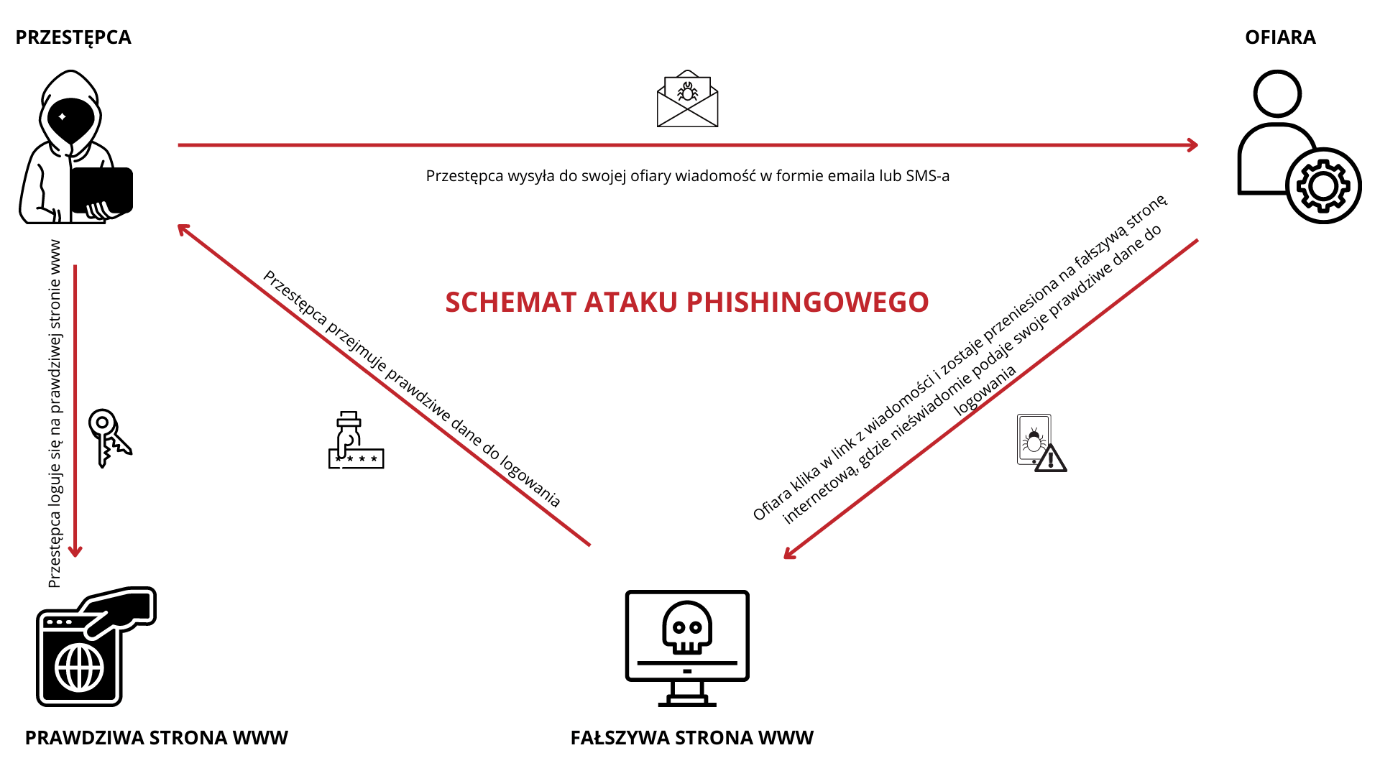
Wytnij dowolnej wielkości pojedyncze plastry i wręcz je uczestnikom i uczestni/czkom. Po wpisaniu skojarzeń poproś, aby utworzyli mapę, łącząc ze sobą pojedyncze elementy.





Załącznik nr 2.

**Schemat ataku phishingowego:**



**Przykładowe persony:**

