sieć na kulturę

SKRYPT

BEZPIECZNE ZACHOWANIA W SIECI

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
FWZR
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

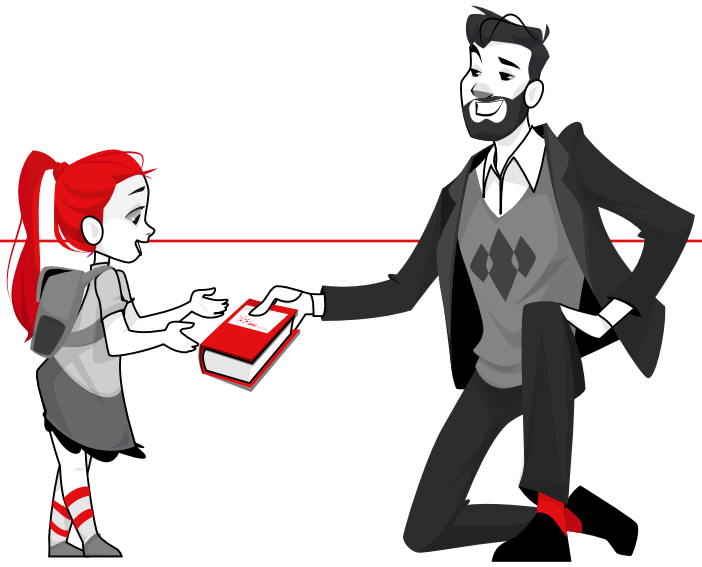
Program

1. GDZIE SZUKAĆ INFORMACJI ZWIĄZANYCH Z BEZPIECZEŃSTWEM W SIECI
   - Problemy z wyciekiem danych z serwisów
   - Oszustwa
2. ANALIZA NARZĘDZI DO KOMUNIKACJI (Szyfrowane, Nieszyfrowane)
3. JAK TRAFIAJĄ DO NAS WIRUSY
   - Maile i załączniki
   - Pobieranie plików
   - Instalowanie oprogramowania
4. JAK BEZPIECZNIE PRZECHOWYWAĆ PLIKI I DANE
   - Nośniki zewnętrzne
   - W chmurze
5. CO ZROBIĆ, GDY ZAATAKUJE NAS WIRUS?
   - Rodzaje wirusów i ich niebezpieczeństwo
   - Procesy bezpieczeństwa
   - Narzędzia

Spotkanie

- Rejestracja uczestników
- Poznajmy się!
- Wstępny test umiejętności

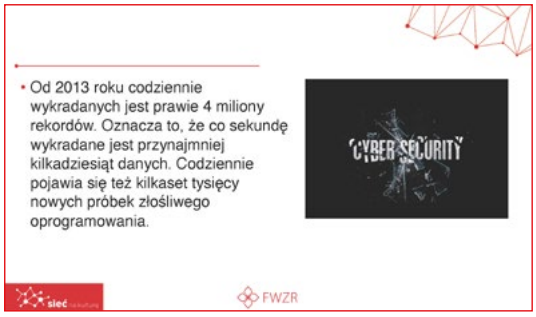
Poznajmy się



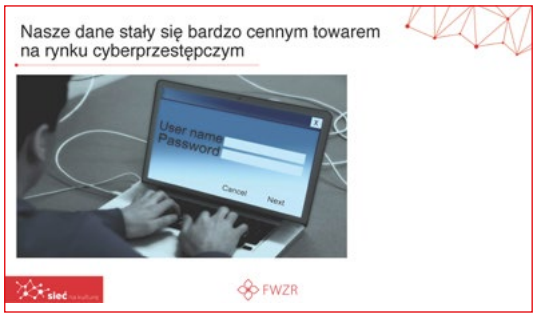
Gdzie szukać informacji związanych z bezpieczeństwem w sieci

PROBLEMY Z WYCIEKIEM DANYCH Z SERWISÓW

Żyjemy w świecie, w którym liczba urządzeń podłączonych do sieci jest większa niż liczba ludzi żyjących na planecie Ziemia. Prawie każdy z nas ma swój komputer, a niekiedy także dodatkowo smartfon czy tablet. Nie zapominajmy też o różnych konsolach do gier (także sieciowych), czy inteligentnych telewizorach, lodówkach, samochodach, pralkach, a nawet żarówkach. Jakby na to nie patrzeć, to także swego rodzaju komputery lub urządzenia bezpośrednio z nimi połączone. W związku z tym wszyscy nieustannie jesteśmy zagrożeni, a rzadko kiedy zdajemy sobie sprawę z liczby i źródeł niebezpieczeństw.



Szacuje się, że od 2013 roku codziennie wykradanych jest prawie 4 miliony rekordów. Oznacza to, że co sekundę wykradane jest przynajmniej kilkadziesiąt danych. Codziennie pojawia się też kilkaset tysięcy nowych próbek złośliwego oprogramowania.



Nasze dane stały się bardzo cennym towarem na rynku cyberprzestępczym. Dostęp do wiedzy na temat naszych loginów, haseł, ale także informacji o naszych znajomych, planach, wydatkach, hobby jest dziś dość wartościowy.

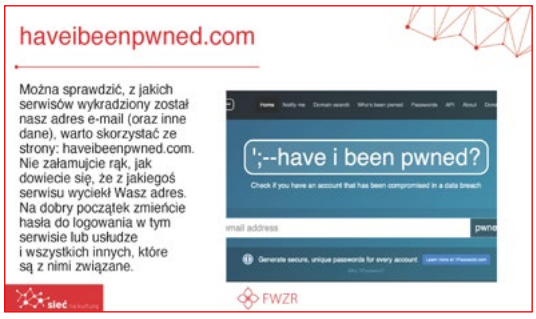
Kiedy z jakiegoś portalu lub innego miejsca w sieci, które wymaga logowania, wycieknią nasze dane, konsekwencje mogą nas nieprzyjemnie zaskoczyć.

Łatwo wyobrazić sobie, co mogą zrobić cyberprzestępcy, znając login i hasło np. do banku czy serwisu społecznościowego.

Zakupem takich informacji zainteresowani są także tzw. **brokerzy danych**. Skupują oni informacje o ludziach, aby później sprzedać je np. firmom ubezpieczeniowym, agencjom HR, agencjom reklamowym, agencjom odpowiedzialnym za kampanie polityczne.

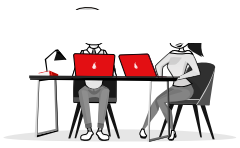
Pojawia się pytanie, co my sami możemy zrobić, aby czuć się trochę bardziej bezpiecznie?

- Po pierwsze (i najważniejsze), nie powinno używać się tego samego loginu i hasła do wielu usług i serwisów.
- Po drugie, myśleć o tym, komu i w jakim celu udostępniamy nasze dane. Nie każdy serwis musi wiedzieć o nas wszystko. Już w momencie podawania rozmaitych danych podczas rejestracji niekiedy powinno zapalić się nam w głowie czerwone światło ostrzegawcze.
- Po trzecie, jeżeli mamy taką możliwość, zawsze powinniśmy korzystać z uwierzytelniania dwuetapowego (np. potwierdzenie logowania kodem SMS, odciskiem palca czy korzystać z systemu rozpoznawania twarzy).



Aby sprawdzić, z jakich serwisów wykradziony został nasz adres e-mail (oraz inne dane), warto skorzystać ze strony: **haveibeenpwned.com.** Nie załamujcie rąk, jak dowiecie się, że z jakiegoś serwisu wyciekł Wasz adres. Na dobry początek zmieńcie hasła do logowania w tym serwisie lub usłudze i wszystkich innych, które są z nimi związane.

Niebezpiecznik.pl to jeden z najstarszych i najpopularniejszych rodzimych serwisów internetowych informujących o różnego typu zagrożeniach, które każdego dnia pojawiają się w cyfrowym świecie.



TED (Technology, Entertainment and Design – Technologia, Rozrywka i Design) – marka konferencji naukowych organizowanych corocznie przez amerykańską fundację non-profit Sapling Foundation. Celem konferencji jest popularyzacja – jak głosi motto – „idei wartych propagowania"

Źródło: https://pl.wikipedia.org/wiki/TED_(konferencja)

Czym jest TEDx?

Konferencje TEDx są niezależne od TED, jednak stosują format analogiczny do tej konferencji. Mogą zostać zorganizowane przez kogokolwiek, kto otrzyma bezpłatną licencję od organizacji oraz będzie stosował się do ściśle określonych reguł. Konferencje nie mogą przynosić zysków, a koszty pokrywać mogą opłaty za wstęp lub sponsorzy. Prelegenci nie otrzymują wynagrodzenia i zgadzają się na publikację nagrania na koncie TEDx w portalu YouTube na licencji takiej samej, jak prelekcje TED oraz na ewentualny montaż nagrania i emisję na stronie TED.com.

Źródło: https://pl.wikipedia.org/wiki/TED_(konferencja)

ROZSZERZENIE

Inne wystąpienia Piotra Koniecznego:
Niech Halina w to nie klika! A ja i tak w kliknę, proszę pana!
youtube.com/watch?v=NsMw7hL5idw

Dobrym pomysłem jest także korzystanie ze strony: **https://plblog.kaspersky.com/**, na której można znaleźć wiele przydatnych informacji na temat bezpieczeństwa w sieci.

Współczesna kultura popularna stara się odnosić do wszelkich zagrożeń w sieci. Takim przykładem są dwie powieści Jakuba Szamałka. Więcej informacji lub przydatne cytaty znajdziesz pod linkiem: **https://jakubszamalek.pl/**

Gdzie szukać informacji związanych z bezpieczeństwem w sieci

OSZUSTWA

Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.

Źródło: pl.wikipedia.org/wiki/Phishing

https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/

https://www.avast.com/pl-pl/c-phishing

ROZSZERZENIE

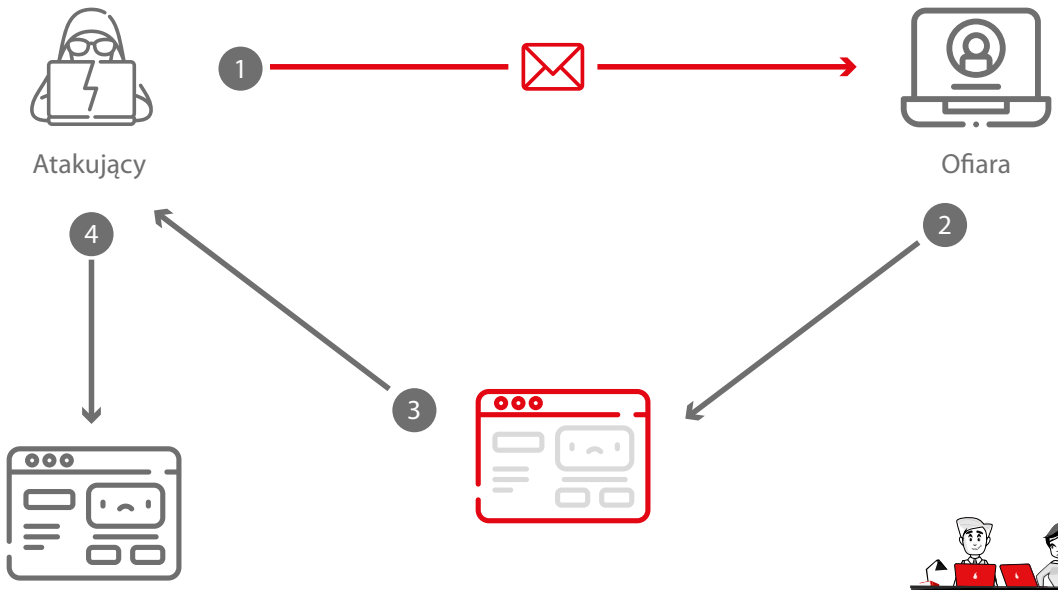
https://pl.malwarebytes.com/phishing/ — BARDZO DOBRE ŹRÓDŁO!

https://phishinsight.trendmicro.com/en/ — PLATFORMA EDUKACYJNA PO ANGIELSKU

https://plblog.kaspersky.com/phishing-spam-hooks/10141/

https://www.westernunion.com/pl/pl/fraudawareness/fraud-types.html

Oto schemat działania phishingowego:



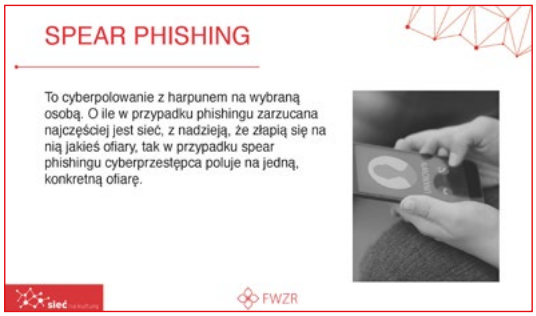
1. Przestępca wysyła ofierze informację z linkiem, który ma zostać otwarty. Może to być rzekomy list z banku, w którym mamy konto, albo dokumenty od jakiejś państwowej instytucji. Innym razem wiadomość od szefa z ważnymi danymi lub powiadomienie z jakiegoś serwisu (np. społecznościowego lub rozrywkowego). Może to także być np. informacja o wygranej na loterii… Trzymajmy się tu przykładu banku.

2. W e-mailu lub niekiedy w wiadomości MMS, wyraźnie jest napisane, aby otworzyć link i wykonać jakieś działanie, np. zalogować się do banku.

3. Kiedy ofiara cyberprzestępstwa otworzy link, pojawi się strona bardzo podobna do strony prawdziwego banku lub instytucji. Ofiara wtedy loguje się prawdziwym loginem i hasłem, ale nie wie, że te dane są przechwytywane przez cyberprzestępcę, ponieważ nie jest to strona autentyczna.

4. Dalej już nic nie stoi na przeszkodzie, aby cyberprzestępca zalogował się, używając naszych prawdziwych danych, do banku i … ukradł nam pieniądze.

SPEAR FISHING



To cyberpolowanie z harpunem na wybraną osobą. O ile w przypadku phishingu zarzucana najczęściej jest sieć, z nadzieją, że złapią się na nią jakieś ofiary, tak w przypadku spear phishingu cyberprzestępca poluje na jedną, konkretną ofiarę.

CLONE PHISHING

Clone phishing jest typem phishingu, w którym prawdziwy e-mail posiadający załącznik lub link zostaje użyty przez przestępcę jako wzór przy tworzeniu wiadomości na potrzeby oszustwa. Załączniki lub linki zostają zastąpione złośliwymi wersjami, a następnie wysłane z adresu email sfałszowanego tak, aby wyglądał jak ten należący do oryginalnego nadawcy.

Ta technika może zostać użyta pośrednio, przy pomocy wcześniej zainfekowanej maszyny do stworzenia następnej wykorzystując zaufanie społeczne do wnioskowanego adresu email, ponieważ obie strony otrzymują oryginalny email.

WHALING

Whaling - część ataków phishingowych została skierowana w szczególności do kierownictwa wyższego szczebla i innych ważnych celów z branży biznesowej. Z tego powodu ataki te nazwano whaling (z języka angielskiego „wielorybnictwo"). W przypadku ataków tego typu, sfałszowana witryna lub wiadomość jest tworzona z uwzględnieniem np. stanowiska ofiary w firmie. Treść e-maili często przypomina pisma pochodzące z kancelarii prawnych lub urzędów państwowych. Taka wiadomość może zawierać załącznik w postaci złośliwego oprogramowania i nakłaniać ofiarę do jego instalacji np. w celu uzyskania dostępu do ważnego dokumentu.

Źródło: https://pl.wikipedia.org/wiki/Phishing

FAŁSZYWA POMOC TECHNICZNA

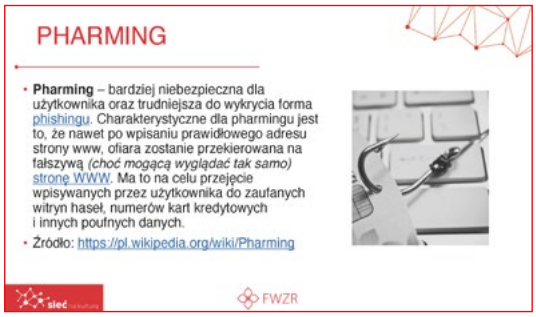
Fałszywa pomoc techniczna – metoda oszustwa internetowego, w której przestępca próbuje zastraszyć ofiarę i skłonić ją do zapłacenia za zbędną pomoc techniczną. Metoda ta wykorzystuje brak wiedzy informatycznej ofiary.

Oszuści prowadzący fałszywą pomoc techniczną mogą zadzwonić do ofiary, podając się za przedstawicieli producenta oprogramowania (np. Microsoftu). W innym wariancie ataku połączenie nawiązuje ofiara, nakłoniona przez komunikat zamieszczony na stronie internetowej (czasami blokujący przeglądarkę i trudny do zamknięcia). Przestępcy proszą o zainstalowanie aplikacji dającej zdalny dostęp do urządzenia. Następnie mogą informować ofiarę o rzekomych problemach na komputerze, np. poprzez wskazywanie niegroźnych ostrzeżeń i błędów z systemowego podglądu zdarzeń lub „skanowanie" komputera komendą

tree w wierszu poleceń. Ostatecznie oszust proponuje zakup pomocy technicznej, która ma wyeliminować rzekome usterki.

Źródło: https://pl.wikipedia.org/wiki/Fałszywa_pomoc_techniczna

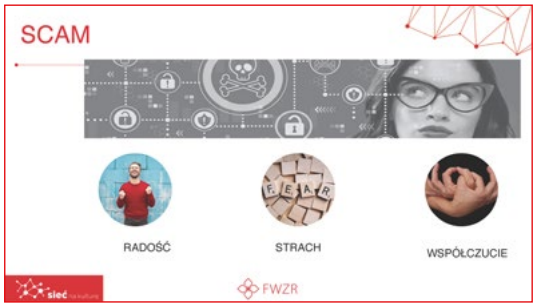
PHARMING



Pharming – bardziej niebezpieczna dla użytkownika oraz trudniejsza do wykrycia forma phishingu. Charakterystyczne dla pharmingu jest to, że nawet po wpisaniu prawidłowego adresu strony www, ofiara zostanie przekierowana na fałszywą (choć mogącą wyglądać tak samo) stronę WWW. Ma to na celu przejęcie wpisywanych przez użytkownika do zaufanych witryn haseł, numerów kart kredytowych i innych poufnych danych.

Źródło: https://pl.wikipedia.org/wiki/Pharming

SCAM



Scam – oszustwo polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy lub innych składników majątku. Osoba wzbudzająca fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych, takich jak: pycha i chciwość, ale też empatia i altruizm.

Źródło: https://pl.wikipedia.org/wiki/Scam

Scam różni się od phishingu tym, że cyberprzestępca musi wzbudzić nasze zaufanie. Jedną z najbardziej popularnych form scamu jest historia z otrzymanym przez kogoś spadkiem.

Pamiętaj, że dziś istnieje wiele portali, które zajmują się legalną zbiórką pieniędzy na różne cele. Robią to zgodnie z prawem i opisują prawdziwe historie. Jeżeli masz potrzebę, by kogoś wesprzeć finansowo, skorzystaj z nich.

Nigdy nie wierz, że ktoś obcy chce podarować Ci olbrzymie pieniądze za drobną usługę. Takie sytuacje zdarzają się jedynie w baśniach, a i tam nie zawsze kończą się happy endem.

NIGERYJSKI SZWINDEL

Nigeryjski szwindel (afrykański szwindel) – rodzaj spamu-oszustwa polegający na wciągnięciu ofiary w fikcyjny transfer wielkiej kwoty pieniędzy (rzędu kilku milionów USD) najczęściej z któregoś z krajów afrykańskich (początkowo głównie do Nigerii).

Źródło: https://pl.wikipedia.org/wiki/Nigeryjski_szwindel

SMS PHISHING

SMS phishing – atak socjotechniczny podobny do phishingu polegający na rozsyłaniu SMS-ów, które mają skłonić ofiarę do podjęcia określonego działania.

Źródło: https://pl.wikipedia.org/wiki/SMS_phishing

Pamiętaj, że SMS phishing może próbować skłonić Cię do wysłania wiadomości SMS lub oddzwonienia na podany numer telefonu. Często w tym celu wykorzystywane są tzw. SMS PREMIUM lub połączenia PREMIUM. Za ich wysłanie lub wykonanie naliczane są często bardzo wysokie opłaty, które później doliczone zostaną do rachunku telefonicznego.

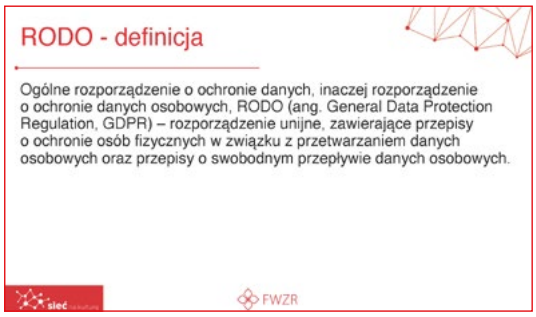
Jak się przed problemami z wyciekiem danych z serwisów oraz oszustwem zabezpieczyć?

PLIKI COOKIES

W zasadzie są niezbędne do prawidłowego funkcjonowania stron internetowych. Poprawiają nasz komfort użytkowania różnych portali i serwisów. Informują też nadawców,

jakie treści cieszą się większym, a jakie mniejszym zainteresowaniem. Zresztą zazwyczaj jesteśmy o nich informowani po wejściu pod konkretny adres w sieci. Nie ma w nich nic złego.

Zanim na kolejnej stronie zaakceptujecie jednym kliknięciem wszystkie zgody na działanie „ciasteczek", wczytajcie się dokładnie, czego one dotyczą. Pewnie warto poświęcić kilka sekund więcej i dostosować stosowne zgody do własnych potrzeb.



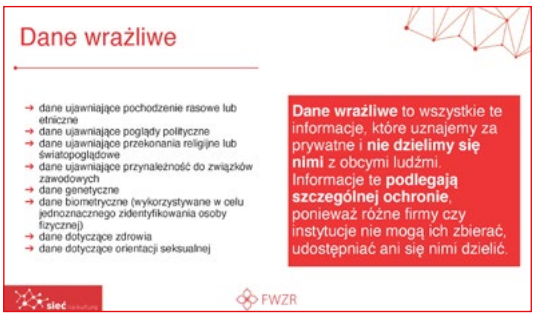
To mit, że **RODO** wymaga naszej zgody na każde ciastko zaserwowane przez przeglądarkę i każdy uruchomiony skrypt.

RODO pozostaje neutralne technicznie: jego zakres zastosowania nie zależy od tego, jaka technika śledzenia/identyfikacji została wykorzystana, ale od tego, czy rzeczywiście dochodzi do identyfikacji.

Kiedy zatem mówimy o identyfikacji? Naturalnie nie tylko wtedy, kiedy w grę wchodzą dane ujawniające społeczną tożsamość danej osoby (imię, nazwisko, adres etc). Taka sytuacja rzadko ma miejsce przy standardowym przeglądaniu stron internetowych (inaczej np. jest na Facebooku). Na gruncie RODO wystarczy, że podmiot przetwarzający dane (np. wydawca portalu) jest w stanie pośrednio zidentyfikować użytkownika w oparciu o dane spseudonimizowane (takie, które dla kogoś innego byłyby tylko przypadkowym numerem, ale w jego „systemie" łączą się z konkretną osobą).

Źródło: https://panoptykon.org/wiadomosc/cookies-informacje-sledzace-rodo

DANE WRAŻLIWE

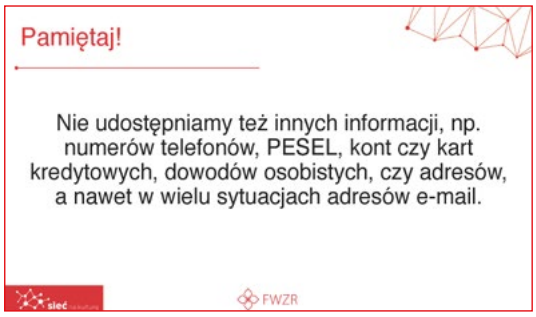


To jest lista danych wrażliwych:

- dane ujawniające pochodzenie rasowe lub etniczne,
- dane ujawniające poglądy polityczne,
- dane ujawniające przekonania religijne lub światopoglądowe,

- dane ujawniające przynależność do związków zawodowych,
- dane genetyczne,
- dane biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej),
- dane dotyczące zdrowia,
- dane dotyczące seksualności lub orientacji seksualnej.

Zrzeczenie się prywatności jednostki oznacza odebranie prywatności całemu społeczeństwu. Podobnie jest z kampanią pokojową, cenzurą czy wolnością słowa. Są to spostrzeżenia Edwarda Snowdena zawarte w książce *Pamięć nieulotna*.



Jeżeli chcemy się zabezpieczyć przed wyciekiem danych, sami ich nie udostępniajmy. Im mniej informacji podajemy na swój temat w sieci, tym jesteśmy bardziej bezpieczni.

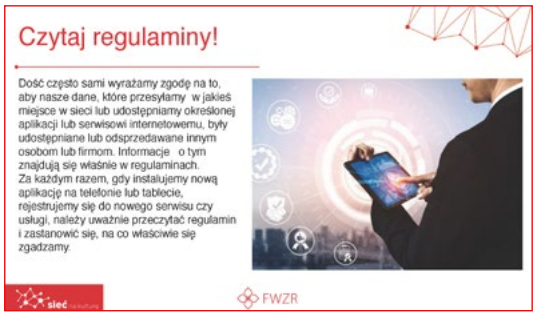
PAMIĘTAJ!

Nie udostępniamy też innych informacji, np. numerów telefonów, PESEL, kont czy kart kredytowych, dowodów osobistych, czy adresów, a nawet w wielu sytuacjach adresów e-mail.

Oto lista zdjęć, których raczej nie powinno się publikować w sieci:

- zdjęcia, na których jesteśmy niekompletnie ubrani,
- zdjęcia wnętrz mieszkań,
- zdjęcia drogich przedmiotów,
- zdjęcia z wakacji, gdy na nich właśnie przebywamy,
- zdjęcia z prywatnych spotkań.

CZYTAJ REGULAMINY!



Dość często sami wyrażamy zgodę na to, aby nasze dane, które przesyłamy w jakieś miejsce w sieci lub udostępniamy określonej aplikacji lub serwisowi internetowemu, były udostępniane lub odsprzedawane innym osobom lub firmom. Informacje o tym znajdują się właśnie w regulaminach. Za każdym razem, gdy instalujemy nową aplikację na telefonie lub tablecie, rejestrujemy się do nowego serwisu czy usługi, należy uważnie przeczytać regulamin i zastanowić się, na co właściwie się zgadzamy.

CZYM JEST HASŁO?

Hasło to ciąg liter, liczb i znaków specjalnych, które służyć mają uwierzytelnieniu, czyli udowodnieniu, kim jesteśmy. Kiedy logujemy się do naszej poczty elektronicznej, bankowości online, dokonujemy zakupów albo uzyskujemy dostęp do rozmaitych urządzeń, korzystamy z haseł. W dzisiejszym świecie internetu używamy ich w zasadzie bez przerwy.

Użytkownicy internetu, aby łatwiej zapamiętać hasła, używają na przykład imion swoich zwierząt i dodają do nich rok swoich urodzin. I tak popularnym hasłem jest np. "Burek 2005". Takie hasło można złamać w zasadzie w kilka sekund.

Hasło silne nie jest słownikowym wyrazem, zawiera długi ciąg dużych i małych liter, cyfr i znaków specjalnych.

BEZPIECZNE HASŁA

Jeżeli chcesz sprawdzić swoje hasło, skorzystaj z tej strony: **howsecureismypassword.net**

Zielony kolor oznacza wysoki stopień bezpieczeństwa.

UWIERZYTELNIANIE DWUETAPOWE

Uwierzytelnianie wielopoziomowe – sposób zabezpieczenia oraz autoryzacji podczas logowania przed skorzystaniem z konta użytkownika przez niepowołane osoby poprzez zdobycie przez nią identyfikatora użytkownika i hasła uwierzytelniającego. Oprócz podania tych danych logowania, użytkownik musi (w kolejnych etapach) podać uzyskany kod lub frazę np. ze swojego przenośnego urządzenia internetowego (np. smartfon, tablet), poprzez przepisanie go z e-maila wysłanego przez serwis, na którym użytkownik próbuje się zalogować, czy też za pomocą specjalnej karty, linii papilarnych palca itp.

Źródło: https://pl.wikipedia.org/wiki/Uwierzytelnianie_wielopoziomowe

Aby być bardziej bezpiecznym w sieci, należy posiadać oprogramowanie antywirusowe, wiedzę o tym, jak zabezpieczać swój komputer i stosować odpowiednie nawyki. Ten trzeci element jest zawsze najsłabszy.

BEZPIECZEŃSTWO - ZDROWY ROZSĄDEK

Często w wyborze słusznej drogi pomaga nam zdrowy rozsądek. Zgodnie z nim, jeżeli mamy wątpliwości, czy coś powinniśmy robić, po prostu szukajmy wiedzy lub tego nie róbmy. I bądźmy czujni.

Analiza narzędzi do komunikacji

Internet został wymyślony po to, by ludzie się porozumiewali szybciej, łatwiej, wygodniej i na duże odległości. Dlatego daje wiele okazji i narzędzi do komunikacji. Są to zarówno skrzynki pocztowe, z których wysyłane są e-maile, jak i strony z chatami, programy do prowadzenia wideokonferencji, komunikatory służące do wysyłania krótkich informacji. Aby połączyć się z bliskimi z odległego krańca świata, zobaczyć ich na wielkim ekranie lub wspólnie uczestniczyć w oglądaniu filmu, wystarczy kilka kliknięć.

W ostatnich latach najszybszą formą wymiany informacji są komunikatory. To programy komputerowe, które służą natychmiastowej wymianie informacji poprzez internet. W komunikatorach ludzie wymieniają nie tylko informacje tekstowe, ale też zdjęcia, filmy, dokumenty, linki, emotikony, mogą prowadzić wideorozmowy. Znasz pewnie wiele komunikatorów. Do najpopularniejszych należą: **Messenger, WhatsApp, Gadu-Gadu, Signal.**

ZASADY KOMUNIKACYJNYCH ZACHOWAŃ LUDZKICH

Oto lista tych czynności, których na pewno nie powinno się robić:

- rozmowa z nieznajomymi, poza przypadkami uzasadnionymi (np. sprzedawcą w sklepie internetowym, profesorem z uczelni wyższej, od którego oczekujemy konsultacji, lekarzem itd). Wszystkie osoby, z którymi nawiązujemy kontakt nie powinny być anonimowe, tzn. nieznane z imienia i nazwiska. Podobnie i Wy, jeżeli nawiązujecie kontakt formalny, powinniście się przedstawić.
- wysyłanie nieznajomym plików, w tym zdjęć i filmów (w szczególności dotyczących naszej intymności, prywatności i rodziny),
- przesyłanie spamu, w tym tzw. łańcuszków szczęścia,
- otwieranie wiadomości z podejrzanymi linkami (mogą zawierać wirusy).

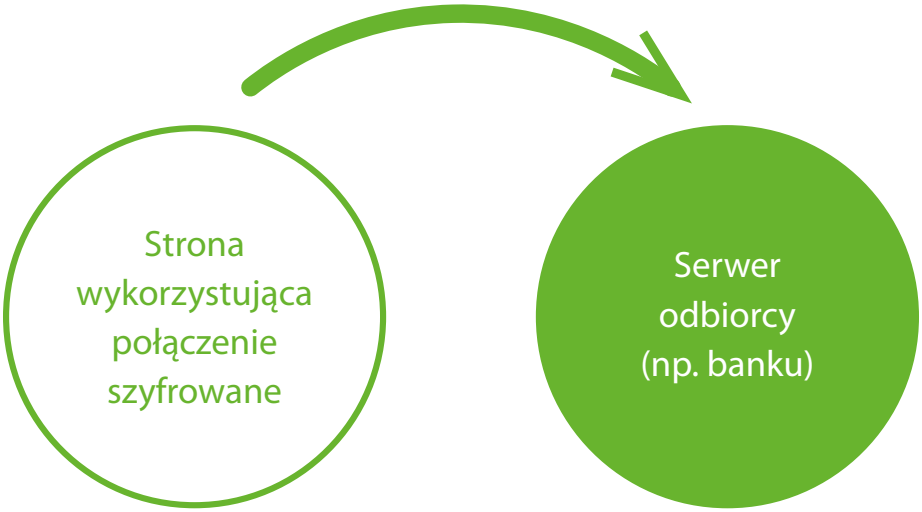
Zasady netykiety:

- niepisanie całych zdań wielkimi literami, to oznacza, że krzyczymy, a nikt nie lubi, jak się na niego podnosi głos,
- używanie emotikonek z rozsądkiem,
- nieprzeszkadzanie osobie, która ma widoczny status: Zajęty,
- traktowaniu innych użytkowników sieci z należytym szacunkiem,
- komunikowanie się w języku znanym rozmówcy, z uwzględnieniem wszystkich zasad poprawności językowej,
- duże załączniki przekazujemy za pośrednictwem chmury,
- szanuj prywatność innych
  (np. stosuj w komunikacji mailowej funkcję UDW — Ukryte Do Wiadomości),
- nie zmuszaj swego rozmówcy, aby musiał długo czekać na Twoją odpowiedź/reakcję,
- staraj się pisać konkretnie i zrozumiale.

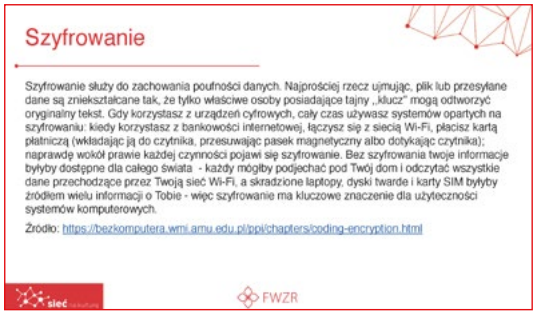
ZASADY ZWIĄZANE Z TECHNOLOGIĄ

Połączenia szyfrowane

UWAGA! Do szyfrowania przesyłanych wiadomości potrzebna jest chęć wszystkich stron uczestniczących w komunikacji.



SZYFROWANIE


Szyfrowanie

Szyfrowanie służy do zachowania poufności danych. Najprościej rzecz ujmując, plik lub przesyłane dane są zniekształcane tak, że tylko właściwe osoby posiadające tajny „klucz" mogą odtworzyć oryginalny tekst. Gdy korzystasz z urządzeń cyfrowych, cały czas używasz systemów opartych na szyfrowaniu: kiedy korzystasz z bankowości internetowej, łączysz się z siecią Wi-Fi, płacisz kartą płatniczą (wkładając ją do czytnika, przesuwając pasek magnetyczny albo dotykając czytnika); naprawdę wokół prawie każdej czynności pojawi się szyfrowanie. Bez szyfrowania twoje informacje byłyby dostępne dla całego świata - każdy mógłby podjechać pod Twój dom i odczytać wszystkie dane przechodzące przez Twoją sieć Wi-Fi, a skradzione laptopy, dyski twarde i karty SIM byłyby źródłem wielu informacji o Tobie - więc szyfrowanie ma kluczowe znaczenie dla użyteczności systemów komputerowych.

Źródło: https://bezkomputera.wmi.amu.edu.pl/ppi/chapters/coding-encryption.html

Źródło: https://bezkomputera.wmi.amu.edu.pl/ppi/chapters/coding-encryption.html

SIGNAL

HTTPS

Kiedy korzystasz z poczty, banku lub sklepu internetowego oraz wszystkich stron, na których musisz podać swoje dane (login i hasło), sprawdzaj, czy połączenie jest szyfrowane. Adres w pasku adresu powinien zawierać kłódkę i napis: **https** ("S" oznacza secure, czyli bezpieczny).

OPROGRAMOWANIE

Ważne jest, aby nie tylko komputery, ale i smartfony chronić odpowiednim oprogramowaniem, które ułatwia identyfikację zagrożenia wirusowego i pozwala te wirusy skutecznie zwalczać.

Dobre praktyki zastosowań narzędzi do komunikacji

WIDEOKONFERENCJE

Wideokonferencja to rodzaj komunikacji multimedialnej, która odbywa się za pomocą komputerów, ale też smartfonów, czy tabletów. Polega na przesyłaniu z dużą szybkością obrazu i dźwięku w czasie rzeczywistym między nadawcą a odbiorcą (te role są zmienne) znajdującymi się w odległości od siebie. W takiej komunikacji

wymieniane są między osobami dźwięk i obraz, ale nowoczesne programy pozwalają też na wymianę plików, prezentacji, filmów itd. Większość tego typu połączeń można nagrać, aby później móc do nich wrócić.

SKYPE

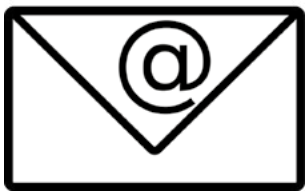
MS TEAMS

GOOGLE MEET

FACEBOOK MESSENGER

Komunikacja na messsengerze nie jest szyfrowana.

EMAIL



E-mail to inaczej list elektroniczny, czyli wiadomość tekstowa, do której mogą być dołączone pliki. Na skrzynce pocztowej możesz np. gromadzić wiadomości, tworzyć foldery, archiwizować wiadomości, tworzyć listę adresową. Skrzynkę e-mail zakłada się na największych portalach, takich jak: Onet, WP, Google itd.

W komunikacji listownej obowiązują pewne zasady. Przede wszystkim:

- nie zaczynaj listu od słowa „Witam", jest to niegrzeczne, podobnie jak kończenie go zwrotem „Żegnam",
- używaj uniwersalnych formuł wstępu: „Dzień dobry" lub „Szanowna Pani/Szanowny Panie",
- używaj uniwersalnych formuł zakończenia: „Pozdrawiam" lub „Z wyrazami szacunku",
- pisz poprawnie, nie popełniaj błędów ortograficznych i interpunkcyjnych,
- nadawaj tytuły wiadomościom, to ułatwia ich porządkowanie,
- zwracaj się do odbiorcy z użyciem wielkiej litery: Ci, Tobie, Twoim,
- nie nadużywaj wielkich liter,
- nie nadużywaj formatowania (różne kolory, różne kroje i wielkości czcionek).

TRELLO.COM

Trello

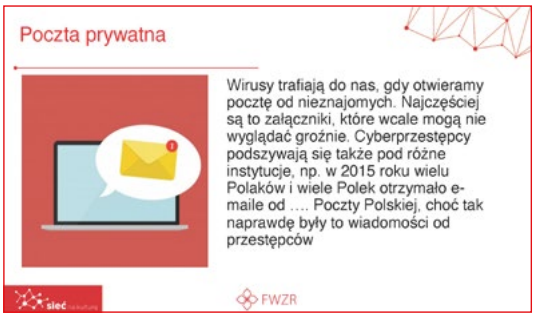
SLACK.COM

slack

ASANA.COM

Jak trafiają do nas wirusy, czyli dobre praktyki w bezpiecznym korzystaniu z narzędzi online

POCZTA PRYWATNA



Wirusy trafiają do nas, gdy otwieramy pocztę od nieznajomych. Najczęściej są to załączniki, które wcale mogą nie wyglądać groźnie. Cyberprzestępcy podszywają się także pod różne instytucje, np. w 2015 roku wielu Polaków i wiele Polek otrzymało e-maile od... Poczty Polskiej, choć tak naprawdę były to wiadomości od przestępców.

Zwróć uwagę, że z poczty służbowej wysłany mail do podwładnego lub współpracownika zawsze zostanie otwarty. Poza tym działa to też w drugą stronę. Czasami służbowe komputery i usługi cyfrowe są słabiej zabezpieczone niż nasze prywatne, więc szansa na zainfekowanie prywatnego sprzętu jest też dość duża.

Oto film *Anatomia ataku ransomware,* który pokazuje, w jaki sposób często dochodzi do ataku hakerskiego rozpoczynającego się właśnie od przesłania zawirusowanego emaila:

youtube.com/watch?reload=9&v=HwqVv94ODgU

HAKER

Haker to dziś bardziej psycholog, który śledzi różne ludzkie działania w sieci, by wiedzieć, jak zaatakować.

Pobieranie plików z **Chomikuj.pl** lub innych seriwsów oferujących hosting plików, **Torrenty** i inne systemy wymiany plików pomiędzy użytkownikami to kolejne źródło, dzięki któremu wirusy rozprzestrzeniają się w prosty i skuteczny sposób.

Zazwyczaj od innych użytkowników pobieramy pliki z nielegalnie rozpowszechnionymi filmami, grami, programami, aplikacjami, książkami, a niekiedy także wciąż z muzyką.

Często są to pliki zawierające treści w tej samej jakości co oryginał. I równie często pobierając je z sieci na dysk komputera, zarażamy go wirusem dołączonym do pożądanego pliku.

Nigdy zaś nie należy klikać w link w wyskakującym okienku z informacją, aby pilnie coś zainstalować. Takie wyskakujące okienka często są pułapką. Linki, które są w nich zawarte, uaktywniają ściganie na nasz komputer pliku. Kiedy my jesteśmy przekonani, że jest to np. plik instalacyjny lub aktualizacyjny, tak naprawdę ściągamy do siebie złośliwe oprogramowanie.

WYBIERZ COŚ DLA SIEBIE

Szczególną ostrożność w kwestii pobierania pliku instalacyjnego bądź aktualizacyjnego należy zachować w przypadku różnych programów antywirusowych.

Avast

AVG

Kaspersky

Jak bezpiecznie przechowywać pliki i dane

Kopie plików, szczególnie tych cennych, najlepiej przechowywać na nośnikach zewnętrznych i w chmurze — jednocześnie.

Pamięć USB, pendrive, pendrajw – urządzenie przenośne zawierające pamięć nieulotną, zaprojektowane do współpracy z komputerem przez port USB i używane do przenoszenia danych między komputerami oraz urządzeniami obsługującymi pamięci USB.

Pamiętaj, że pendrive łatwo zgubić.

Może zostać skradziony, np. razem z kluczami lub portfelem, w którym go przechowujemy, aby zawsze mieć go ze sobą.

Pamiętaj, że kiedy oddajemy komuś nasz pendrive, np. w punkcie druku, osoba niepowołana może otworzyć nasze inne dokumenty, które na nim się znajdują.

Pamiętaj! Port USB, do którego podpinasz swój pendrive, to najprostsza droga do zawirusowania komputera. Zeskanuj pendrive przed podłączeniem do komputera programem antywirusowym.

CHMURA

Chmurę definiować można na dwa sposoby. Pierwszym z nich jest **chmura obliczeniowa, z angielskiego *cloud computing***, drugim zaś chmura publiczna, tudzież dyski w chmurze, oferowane przez największych potentatów świata IT, przez niezależne firmy czy organizacje oraz przez producentów sprzętu, komputerów, smartfonów, tabletów, a nawet przez firmy telekomunikacyjne.

Źródło: https://www.komputerswiat.pl/poradniki/internet/czym-jest-popularna-chmura/5nhxw4c

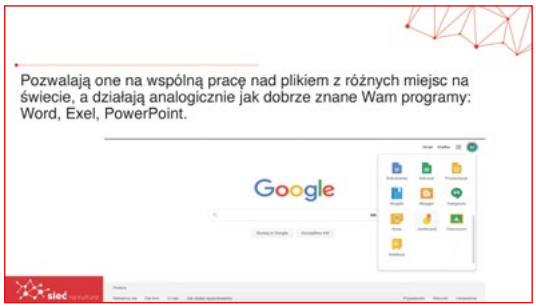
Miejsce, gdzie znajdują się serwery popularnych chmur przechowujące np. jakieś dokumenty, trudno jest wskazać. Jeżeli tak jest, tracimy tak naprawdę kontrolę nad naszymi danymi. Czy to oznacza, że nie powinniśmy pracować w chmurze? Oczywiście nie, ale nie trzymajmy tam w nieskończoność ważnych dokumentów. Po wykonanej pracy, usuwajmy je.

Chmura służy do tego, aby ułatwić pracę osobom pracującym np. w różnych miejscach. Mogą oni **współedytować pliki**, dzielić się komentarzami, dodawać pliki, linki itd. Ważne jednak, aby wypracowali wcześniej zasady działania w chmurze (aby np. ktoś nie kasował treści wpisanych przez kogoś innego).

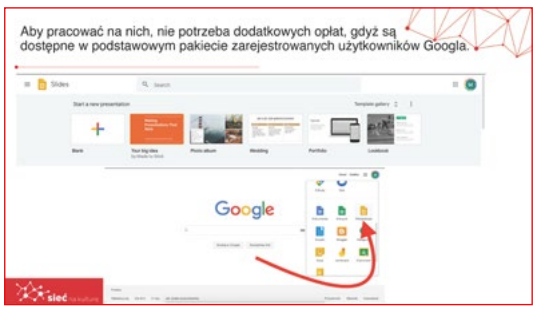
GOOGLE ONE

one.google.com

W tej chmurze z usługą Googla połączonych jest wiele innych usług, a posiadanie przestrzeni dyskowej do przechowywania materiałów graficznych znacznie ułatwia np. wspólne projektowanie prezentacji.



Pozwalają one na wspólną pracę nad plikiem z różnych miejsc na świecie, a działają analogicznie jak dobrze znane Wam programy: Word, Exel, PowerPoint.



Aby pracować na nich, nie potrzeba dodatkowych opłat, gdyż są dostępne w podstawowym pakiecie zarejestrowanych użytkowników Googla.

DROPBOX

dropbox.com

Oferuje 2GB bezpłatnej przestrzeni dyskowej. Dropbox był

jedną z pierwszych takich usług na rynku i to właśnie jemu zawdzięczamy popularność przechowywania danych w chmurze.

ONEDRIVE

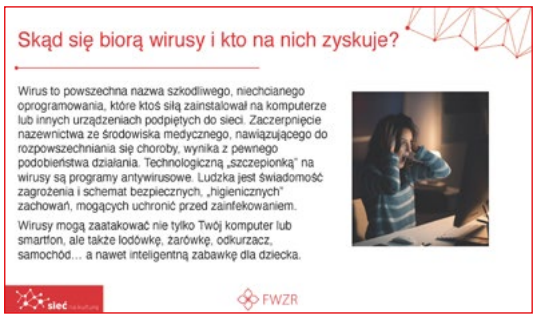
onedrive.live.com

Oferowana jest użytkownikom pakietu Microsoft, czyli wszystkim użytkownikom Windowsa, przestrzeń na swoich serwerach. Usługa połączona jest z produktami pakietu Office.

Co zrobić, gdy zaatakuje nas wirus?

PROCESY BEZPIECZEŃSTWA

Skąd się biorą wirusy i kto na nich zyskuje?

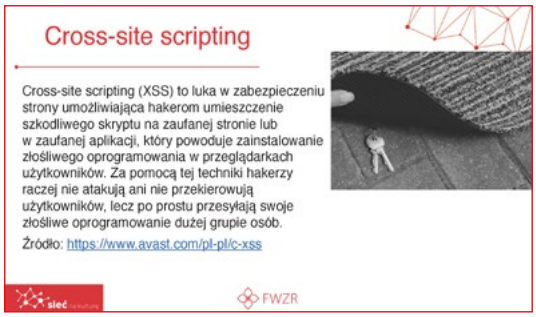


Wirus to powszechna nazwa szkodliwego, niechcianego oprogramowania, które ktoś siłą zainstalował na komputerze lub innych urządzeniach podpiętych do sieci. Zaczerpnięcie nazewnictwa ze środowiska medycznego, nawiązującego do rozpowszechniania się choroby, wynika z pewnego podobieństwa działania. Technologiczną „szczepionką" na wirusy są programy antywirusowe. Ludzka jest świadomość zagrożenia i schemat bezpiecznych, „higienicznych" zachowań, mogących uchronić przed zainfekowaniem.

Wirusy mogą zaatakować nie tylko Twój komputer lub smartfon, ale także lodówkę, żarówkę, odkurzacz, samochód… a nawet inteligentną zabawkę dla dziecka.

CROSS-SITE SCRIPTING

Cross-site scripting (XSS) to luka w zabezpieczeniu strony umożliwiająca hakerom umieszczenie szkodliwego skryptu na zaufanej stronie lub w zaufanej aplikacji, który powoduje zainstalowanie złośliwego oprogramowania w przeglądarkach użytkowników.



Za pomocą tej techniki hakerzy raczej nie atakują ani nie przekierowują użytkowników, lecz po prostu przesyłają swoje złośliwe oprogramowanie dużej grupie osób.

Źródło: https://www.avast.com/pl-pl/c-xss

KOŃ TROJAŃSKI

Podobnie jak drewniany koń z poematu, konie trojańskie lub po prostu trojany to oszustwa i metody inżynierii społecznej, zachęcające niczego niepodejrzewających użytkowników do uruchamiania pozornie łagodnych programów komputerowych, które ukrywają jednak złośliwy kod.

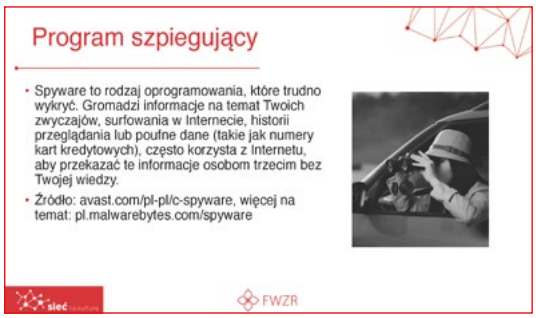
Źródło: pl.malwarebytes.com/trojan, więcej na temat: avast.com/pl-pl/c-trojan

ROBAKI

Robaki komputerowe to zagrożenia, które mogą same się powielać i spowalniać drastycznie Twój komputer.

Źródło: avast.com/pl-pl/c-computer-worm

PROGRAM SZPIEGUJĄCY



Spyware to rodzaj oprogramowania, które trudno wykryć. Gromadzi informacje na temat Twoich zwyczajów, surfowania w Internecie, historii przeglądania lub poufne dane (takie jak numery kart kredytowych), często korzysta z Internetu, aby przekazać te informacje osobom trzecim bez Twojej wiedzy.

Źródło: avast.com/pl-pl/c-spyware, więcej na temat: pl.malwarebytes.com/spyware

MALWARE

Malware to różnego rodzaju szkodliwe programy, które usiłują zainfekować komputer lub urządzenie mobilne. Hakerzy wykorzystują malware do różnych celów — wykradania danych osobowych, haseł i pieniędzy oraz blokowania dostępu do urządzeń. Przed zagrożeniem typu malware można się uchronić, stosując odpowiednie zabezpieczenia.

Źródło: https://www.avast.com/pl-pl/c-malware

ADWARE

Adware to rodzaj wolnego oprogramowania wspieranego przez reklamy, które pojawiają się w wyskakujących oknach lub na pasku narzędzi na komputerze lub w przeglądarce. Większość adware jest denerwująca, ale nie jest niebezpieczna. Jednak niektóre z tego typu zagrożeń zbierają Twoje prywatne informacje, śledzą strony, które odwiedzasz, a nawet rejestrują sekwencje klawiszy.

Źródło: pl.malwarebytes.com/adware, więcej na temat: pl.malwarebytes.com/adware

ROOTKIT

Jakbyś się czuł, gdyby ktoś miał dostęp do Twojego komputera bez Twojej wiedzy? Niestety w przypadku rootkita to możliwe, może on zostać zainstalowany razem z różnymi rodzajami produktów i może zostać wykorzystany do zdalnej kontroli urządzenia.

Źródło: https://www.avast.com/pl-pl/c-rootkit

KEYLOGGER

Keylogger jest to rodzaj oprogramowania szpiegującego, które potajemnie rejestruje naciśnięcia klawiszy, więc złodzieje mogą uzyskać informacje o Twoim koncie, kartach kredytowych, nazwy użytkowników, hasła i inne dane osobowe.

Źródło: avast.com/pl-pl/c-keylogger

SNIFFERY

Sniffery przybierają różną postać. Są między innymi sniffery pakietowe, Wi-Fi, sieciowe czy IP. Wszystkie jednak mają jedną wspólną cechę – są to programy, które przechwytują wszystkie dane przepływające pomiędzy komputerem a siecią, z którą jest on połączony.

Źródło: avast.com/pl-pl/c-sniffer

RANSOMWARE

Oprogramowanie ransomware (znane również pod nazwą rogueware lub scareware) ogranicza dostęp do systemu komputerowego i wymaga zapłacenia okupu, aby blokada została usunięta. Najbardziej niebezpieczne ataki typu ransomware zostały spowodowane przez złośliwe oprogramowanie WannaCry, Petya, Cerber, Cryptolocker i Locky.

Źródła: avast.com/pl-pl/c-ransomware, pl.malwarebytes.com/ransomware

BOTNET

Słowo *botnet* pochodzi od słowa *bot*, które z kolei wywodzi się od określenia *web robot*. Oznacza ono aplikację, która wykonywała powtarzalne czynności w sieci – często tzw. *web spidering* czyli przeczesywanie sieci w celu jej archiwizacji bądź indeksowania. Większość takich robotów,

a niektórzy szacują, że nawet połowa ruchu sieciowego jest ich dziełem, jest grzeczna i nie narusza zasad.

A co mogą robić boty o złym charakterze? Oto kilka przykładów:

- Boty mogą poszukiwać adresów e-mailowych, numerów telefonów, adresów zamieszkania i innych danych osobistych opublikowanych na stronach internetowych. Zebrane informacje następnie mogą być sprzedane i użyte np. do spamowania.
- Boty mogą być również użyte do sztucznego obciążania stron internetowych, np. w celu wyeliminowania konkurencji bądź usunięcia niewygodnej politycznie strony.
- Można ich użyć również do kradzieży treści – po ściągnięciu treści oferowanych np. za opłatą bądź po obejrzeniu reklamy, udostępniane są one za darmo na pirackiej stronie.
- Boty są plagą wszelkich konkursów i stron, na których możemy się zarejestrować i otrzymać coś za darmo. Ktokolwiek próbował np. kupić bilety na popularny koncert lub wykorzystać opublikowany w sieci kod na darmową grę, wie o czym mówię.
- Boty – tym razem niezwiązane w WWW – są również wykorzystywane przez graczy w grach sieciowych. Potrafią one albo reagować szybciej niż człowiek, dając nieuczciwemu graczowi pewną przewagę bądź są w stanie *farmić* te same treści przez całe godziny, bez znudzenia, zarabiając w ten sposób wirtualne złoto bądź przedmioty

Źródło: https://www.spidersweb.pl/2019/02/botnet-cybertarcza.html

ROZSZERZENIE

- https://www.avast.com/pl-pl/c-botnet
- https://plblog.kaspersky.com/botnet/6302/
- https://www.securelist.pl/analysis/5859,biznes_botnetowy.html

OBJAWY ZAINFEKOWANIA TELEFONU

Istnieje kilka objawów, po których można stwierdzić, że nasz telefon jest zainfekowany przez wirusa. Jeżeli zauważysz, że któryś z nich się nasila, postaraj się zeskanować swój smartfon programem antywirusowym. Jeżeli i to nie pomoże, konieczna będzie interwencja specjalisty-informatyka.

- Nieprzeciętnie wysokie rachunki za telefon,
- Nieprzeciętnie duże zużycie pakietu danych,
- Nieprawidłowe działanie aplikacji, częste zawieszanie się,
- Przegrzewanie się telefonu,
- Szybsze niż zwykle wyczerpywanie baterii,
- Często pojawiające się reklamy.

Co zrobić, gdy zaatakuje nas wirus?

NARZĘDZIA

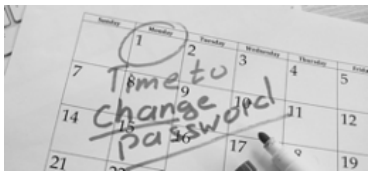
CHROŃ SWÓJ TELEFON

Program antywirusowy

Aktualne oprogramowanie

Wiarygodność aplikacji

Uważaj na publiczne WI-FI



Silne hasła

Uważaj na podejrzane SMS-y i emiale

AVG ANTYWIRUS

ANTYWIRUS MOBILNY KASPERSKY

AVAST ANTYWIRUS

ESET MOBILE SECURITY & ANTIVIRUS

AVIRA ANTIVIRUS

CHROŃ SWÓJ KOMPUTER

Procesy bezpieczeństwa

1. Nie wpadaj w panikę.
2. Aby wirus nie rozprzestrzeniał się dalej, koniecznie odłącz komputer od internetu. Uchronić to może także przed czynieniem przez wirusa różnych, czasami trudnych do odwrócenia, działań za pośrednictwem poczty, mediów społecznościowych, bankowości itp.
3. Jeżeli Twój komputer podłączony jest do lokalnej sieci (domowej, szkolnej, firmowej), koniecznie odłącz go od niej, aby nie zainfekował innych sprzętów do tej sieci podłączonych.

4. Jeżeli komputer przestał reagować na nasze polecenia lub nie chce się „normalnie" włączyć, spróbuj uruchomić go w trybie awaryjnym.
5. Jeżeli komputer wciąż działa, spróbuj skopiować swoje dane. Być może szybka reakcja uchroni Cię przed ich utratą.
6. Jeżeli dotychczas nie mieliście zainstalowanego programu antywirusowego, koniecznie spróbujcie zrobić to teraz. Najlepiej, jakby udało się to zrobić z zewnętrznego nośnika danych bez konieczności podłączania zawirusowanego komputera do sieci.

7. Z poziomu innego, niezainfekowanego komputera zaktualizuj bazę wirusów we wspomnianym programie antywirusowym.
8. Po wykonaniu powyższych czynności dokonaj pełnego skanowania komputera programem antywirusowym.

9. Jeżeli wirus nie zostanie usunięty z komputera, nie bagatelizuj sytuacji i skontaktuj się z informatykiem, który pomoże w rozwiązaniu Twojego problemu.

AVAST.COM

KASPERSKY.PL

AVG.COM

BITDEFENDER.PL

360TOTALSECURITY.COM

INSTRUKCJA KORZYSTANIA Z PLATFORMY „SIEĆ NA KULTURĘ”

LOGOWANIE

Dostęp do platformy wymaga posiadania konta.

Dane do logowania tj. nazwa Użytkownika (Uczestnika Projektu) oraz hasło do platformy Uczestnik Projektu otrzyma od Trenera prowadzącego szkolenie teoretyczne.

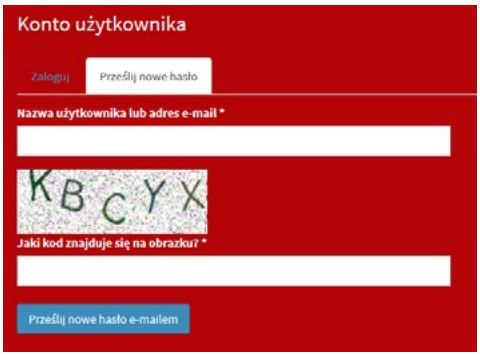
Uczestnik Projektu w celu zalogowania się wpisuje w przeglądarce internetowej adres **platforma.siecnakulture.pl**

Po wyświetleniu się strony głównej **Uczestnik Projektu wpisuje otrzymane dane** w odpowiednie pola.

EDYCJA PROFILU

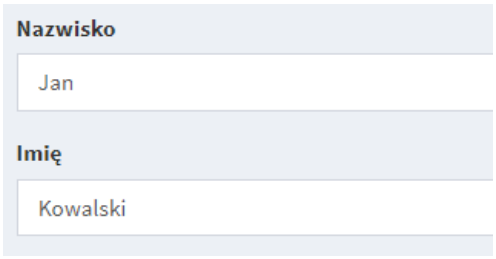
Po zalogowaniu się do platformy Uczestnik wchodzi w zakładkę **MÓJ PROFIL** i może go edytować:

- Uczestnik Projektu, który zapomniał hasła może je odzyskać, korzystając z opcji **Prześlij nowe hasło**. Podając dane w formularzu zmiany hasła (rysunek poniżej), zostanie wysłany link do zmiany hasła na adres mailowy podany przy rejestracji.

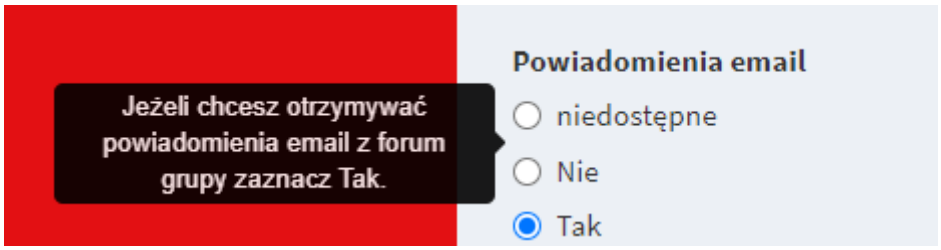


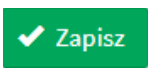
- **Uwaga:** W przypadku wpisania błędnego hasła więcej niż 5 razy konto zostanie zablokowane na 6 godzin.

- **Uczestnik** w danych profilowych musi **używać** swojego **Imienia i Nazwiska** (bez pseudonimów, nazw własnych, itp.)

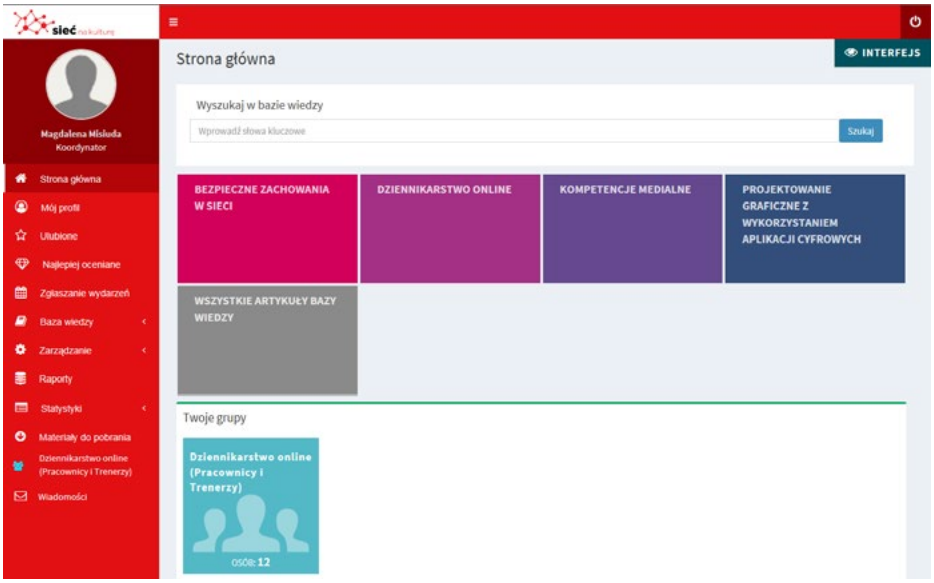


- W edycji profilu Uczestnik ma możliwość wybory **opcji otrzymywania powiadomień email** (o pojawianiu się nowych materiałów, zasobów czy komentarzy w grupach). Można to zrobić poprzez wybór/zaznaczenie:



- Po zakończeniu edycji profilu Uczestnik klika przycisk 

Jeżeli dane są poprawne Uczestnik Projektu uzyska dostęp do **platformy.**



MENU GŁÓWNE

Po lewej stronie znajduje się wysuwane menu. Poszczególne opcje menu:

Strona główna – powrót do strony głównej.

Mój profil – umożliwia wyświetlenie profilu i jego edycję (Uczestnik Projektu może zmienić wszystkie dane za wyjątkiem loginu).

Ulubione – lista zasobów dodanych, jako ulubione.

Najlepiej oceniane – lista zasobów, które są najlepiej oceniane przez Uczestnik Projektów.

Zgłoszenia wydarzeń – umożliwia dodawanie wydarzeń.

Baza wiedzy - zasoby bazy wiedzy podzielone są na różne ścieżki tematyczne z możliwością wyszukiwania potrzebnych informacji po słowach kluczowych.

Materiały do pobrania – lista materiałów do pobrania.

Grupa/y - jedna lub więcej grup, do których został przydzielony Uczestnik Projektu.

GRUPY

Każdy Uczestnik Projektu należy do grup:

Tematycznych – w zależności od wybranej ścieżki szkoleniowej i roli (dwie grupy: 1. tematyczna dla Pracowników, 2. tematyczna dla Pracowników i Trenerów).

Metodycznej – dotyczącej zagadnień związanych z prowadzeniem szkoleń niezależnie od specjalizacji, np. praca z grupą, radzenie sobie z typowymi trudnościami itp.

Forum dyskusyjne – Członkowie grupy mają możliwość swobodnej dyskusji, integracji w ramach tematów, które nie mieszczą się w obszarach ww. grup.

W zależności od grupy jej zawartość może się różnić, w każdej grupie są dostępne zakładki:

- **Opis** – informacje o grupie, trenerze oraz tablica informacyjna.
- **Zasoby** – zasoby z materiałami dostępne w grupie.
- **Kalendarz** – terminy zawierające zdarzenia przypisane do grupy.
- **Forum** – forum dyskusyjne grupy.

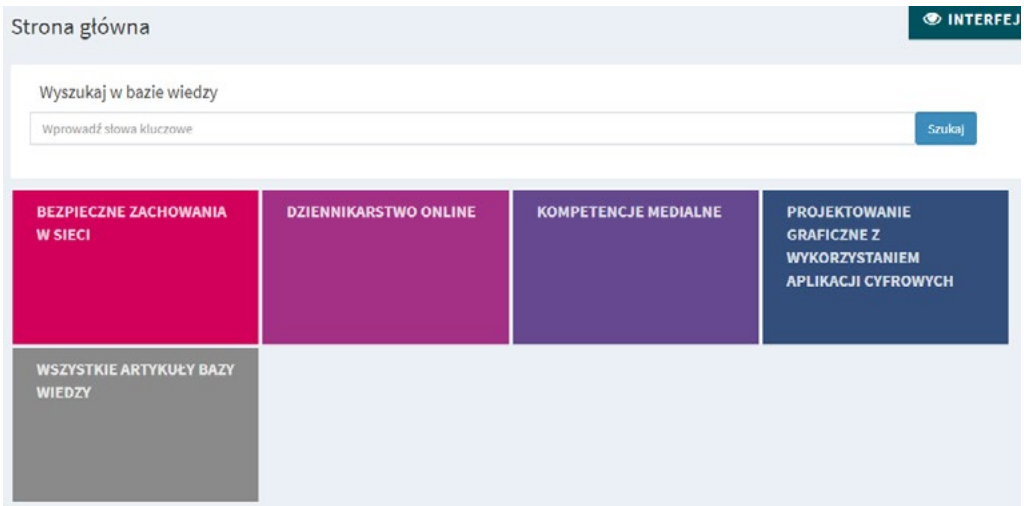
Użytkownicy korzystający z platformy są objęci grywalizacyjną formą budowania prestiżu, który jest prezentowany przy ich profilu oraz w miejscach, w których się wypowiadają. Prestiż Uczestnika Projektu wynika z oceny innych Uczestników Projektu i/lub Trenerów.

Użytkownicy mogą oznaczać posty i komentarze Trenerów, innych Uczestników jako wartościowe. Prestiż wyrażany jest w formie:

liczbowej ☆ 4 oraz **statusu** 2

BAZA WIEDZY

Po zalogowaniu się w oknie głównym wszyscy Uczestnicy Projektu mają dostęp do **BAZY WIEDZY.**

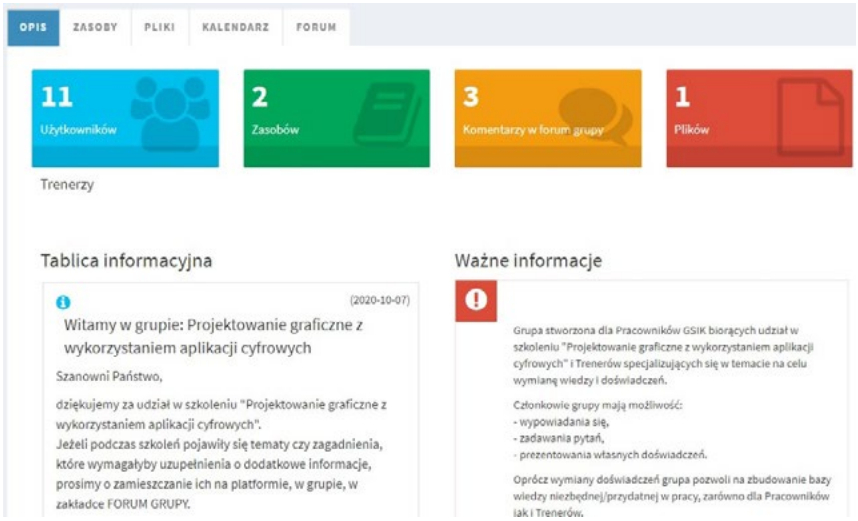


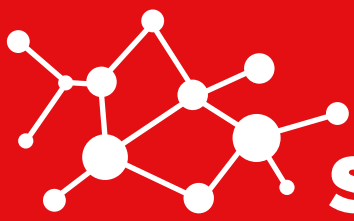
Baza wiedzy zawiera dodatkowe materiały dotyczące realizacji poszczególnych ścieżek tematycznych w postaci opisów, ilustracji, materiałów video oraz tzw. narzędziownię, czyli gotowe szablony, pliki prezentacji, materiały stosowane podczas szkoleń.

Każdy Uczestnik Projektu będzie mógł je pobrać i wykorzystać podczas zajęć z dziećmi i młodzieżą. Baza wiedzy będzie na bieżąco aktualizowana i poszerzana.

W przypadku, gdy Uczestnika Projektu przypisano do jednej z istniejących grup platformy to pod listą kategorii znajduje się lista **Twoje grupy.**

Kliknięcie w jedną z kategorii bazy wiedzy powoduje przejście do tej kategorii, natomiast kliknięcie nazwy grupy np. „Forum dyskusyjne (Pracownicy i Trenerzy)" powoduje przejście do panelu danej grupy.





sieć na kulturę

www.siecnakulture.pl

FUNDACJA **WSPIERANIA**
ZRÓWNOWAŻONEGO ROZWOJU