

BEZPIECZNY INTERNET

Przygotowały:

Lidia Dzieńiszewska

Elżbieta Piszczałowska





Cyberprzemoc- agresja elektroniczna, elektroniczna przemoc rówieśnicza – stosowanie przemocy poprzez: prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem Internetu i narzędzi typu elektronicznego takich jak: SMS, e-mail, witryny internetowe, fora dyskusyjne w Internecie, portale społecznościowe i inne. Osobę dopuszczającą się takich czynów określa się **stalkerem**.



Cyberzagrożenia to – najogólniej rzecz biorąc – „zagrożenia stworzone przez nowoczesne technologie cyfrowe”.

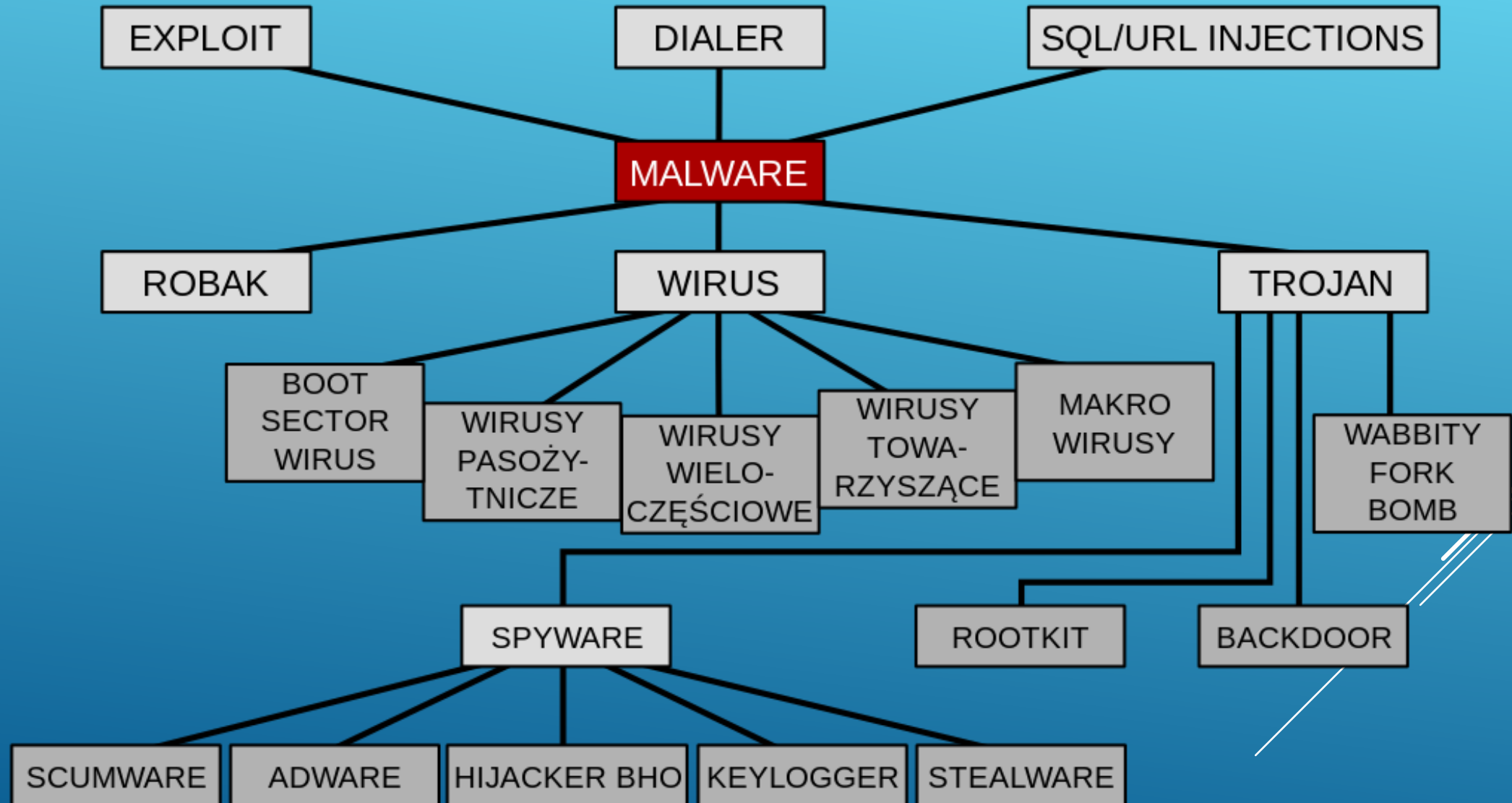
CYBERZAGROŻENIA



1. Złośliwe oprogramowanie – „szkodliwe oprogramowanie” (ang. *malware* – zbitka słów *malicious* „złowrogi, złośliwy” i *software* „oprogramowanie”) – ogół programów o szkodliwym działaniu w stosunku do systemu komputerowego lub jego użytkownika.

Mianem *malware* określa się wyłącznie oprogramowanie, które zostało przeznaczone do złych celów i działa wbrew oczekiwaniom użytkownika; określenie to nie obejmuje aplikacji, które mogą wyrządzić niezamierzoną szkodę z powodu jakiejś niedoskonałości.

Rodzaje szkodliwego oprogramowania



CYBERZAGROŻENIA



2. Spam to niechciana korespondencja trafiająca do Twojej skrzynki e-mail. Zaraz obok wirusów jest to obecnie największa udręka użytkowników Internetu. Spam wydłuża czas który potrzebny jest na sprawdzenie poczty, wywołuje irytację i zmusza do ręcznego kasowania bądź podejmowania innych czynności które również nie należą do przyjemnych. W skrócie można powiedzieć, że spam to nadmiar informacji zbędnych dla odbiorców wiadomości. Spamem mogą być również reklamy na stronie, które np. w niekontrolowany sposób otwierają się samoczynnie w nowych okienkach.

CYBERZAGROŻENIA



3. Kradzież tożsamości, a ściślej fałszerstwo tożsamości – celowe używanie danych osobowych innej osoby, adresu zameldowania, numeru PESEL, najczęściej w celu osiągnięcia korzyści majątkowej.

CYBERZAGROŻENIA

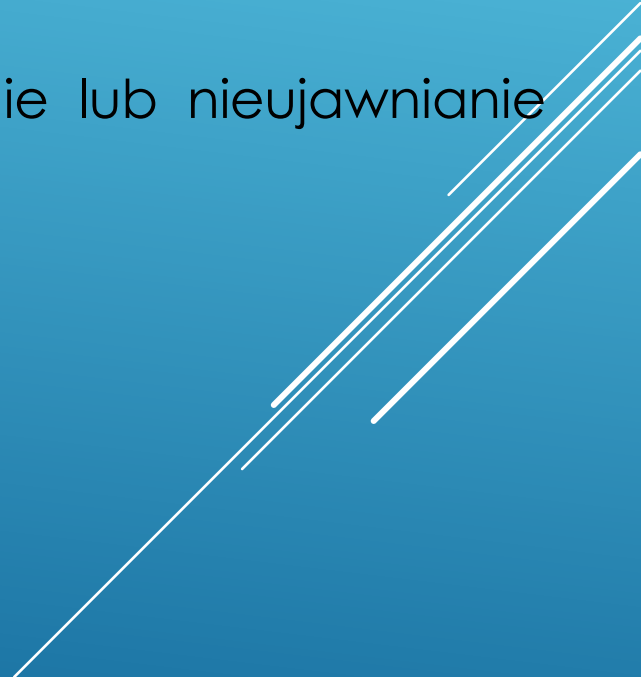


4. Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

INNE CYBERZAGROŻENIA

- 5. Ataki z wykorzystaniem złośliwego kodu na stronach internetowych
 - 6. Ataki na aplikacje internetowe
 - 7. Ataki DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu
 - 8. Naruszenie poufności, integralności lub dostępności danych
 - 9. Zagrożenia wewnętrzne powodowane przez pracowników
- 
- Several white lines of varying lengths and orientations are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

INNE CYBERZAGROŻENIA

- 10. Botnet-y – sieci komputerów przejętych przez przestępców
 - 11. Ingerencja fizyczna, uszkodzenia oraz kradzież
 - 12. Wyciek danych
 - 13. Ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych
 - 14. Cyberszpiegostwo
 - 15. Kradzież kryptowalut (cryptojacking)
- 

Jak radzić sobie z cyberprzemocą :

Several thin, parallel white lines of varying lengths and slopes are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

► Jak radzić sobie z cyberprzemocą :

1. **Porozmawiaj z bliską ci osobą – poszukaj wsparcia i pomocy**

rozmowa z przyjacielem bądź zaufaną osobą dorosłą pomoże ci zapanować nad emocjami i poczuć się lepiej. Omówienie problemu z różnych perspektyw może w wielu przypadkach pomóc ci ochłonąć i na spokojnie zaplanować kolejne działania.

2. **Zachowaj dowody**

zanim podejmiesz próby usunięcia obraźliwych wiadomości - pamiętaj, że są ważnym dowodem nękania. Zabezpiecz dowody w postaci wydruków lub screenshota (zrzut ekranu).

► Jak radzić sobie z cyberprzemocą :

3. Zgłoś incydent

zwróć się o pomoc do rodziców lub innej zaufanej osoby dorosłej (wychowawcy, pedagoga szkolnego, dyrektora). Pomogą ci rozwiązać problem i udzielią wsparcia. Skorzystaj z telefonu zaufania 116 111. Jeśli czujesz się zagrożony powiadom policję (cyberprzemoc w świetle prawa jest czynnością karalną).

4. Prowadź rozmowę na swoich zasadach- nie daj się wciągnąć w spiralę agresji

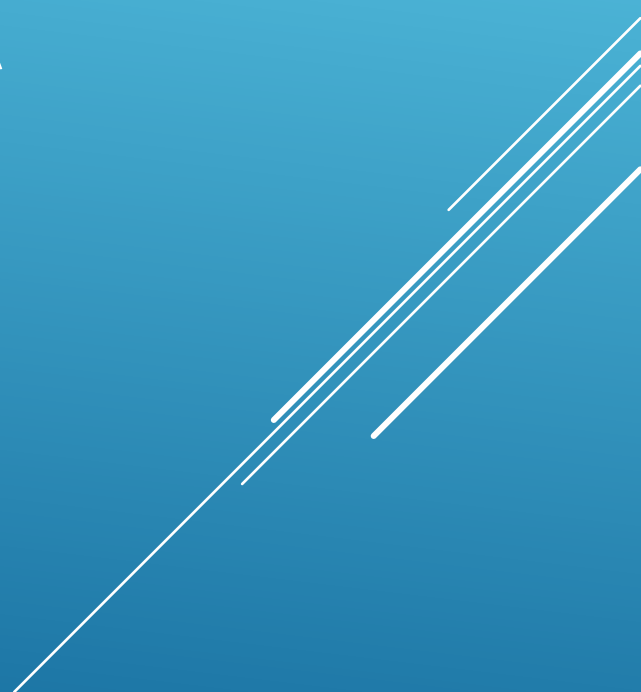
zachowanie cyberprzemocowe to próba dominacji - nie daj się. To kim jesteś i jak się postrzegasz zależy tylko od ciebie. Nie pozwól się sprowokować. Zaskocz agresora przyjaznym nastawieniem - to może zmienić ciąg wydarzeń.

► Jak radzić sobie z cyberprzemocą :

5. Odetnij się od agresora

na wielu portalach społecznościowych możesz zablokować osobę, która cię prześladowa. Także telefony posiadają funkcję blokowania innych numerów. Możesz również zgłosić się z prośbą do administratora o usunięcie obraźliwych treści lub fałszywego konta - pamiętając aby najpierw zapisać dowody nękania.

CYROWE ŚLADY I REPUTACJA ONLINE





Cyfrowy ślad (ang. digital footprint) to indywidualna historia wszystkich aktywności użytkownika w sieci. Tworzą ją zarówno informacje, które pozostawiane są świadomie (jak np. wpisy na blogu, komentarze w mediach społecznościowych) jak i te, które pozostawiamy biernie – automatycznie lub półautomatycznie – korzystając z Internetu (np. numer IP, informacje o używanym systemie operacyjnym). Informacje te, połączone ze sobą, mogą przestawić charakterystyczne dla danego użytkownika wzorce korzystania z sieci, jego preferencje, poglądy, wybory.

Czy wiesz, jak dbać o swój wizerunek online?

Sprawdź na jakie rzeczy powinnaś/powinieneś zwrócić uwagę, a czego unikać!

- ☐ Nie zapomnij o ustawieniach prywatności, dzięki którym będziesz miała/miał większą kontrolę nad informacjami na swój temat. Jeśli chcesz, aby Twój profil był publiczny, uważnie wybieraj informacje, które na nim umieszczasz.
- ☐ Wyszukaj się. Sprawdź, jakie informacje o sobie możesz znaleźć online. Użyj różnych wyszukiwarek, pamiętaj też o zdjęciach i filmach.
- ☐ Uporządkuj swoje profile. Przyjrzyj się zawartości swojego konta i usuń treści, z którymi się już nie identyfikujesz czy nie zgadzasz. Równie krytycznie spójrz na strony, które kiedyś polubiłaś/polubiłeś. Co o Tobie mówią?

Czy wiesz, jak dbać o swój wizerunek online?

Sprawdź na jakie rzeczy powinnaś/powinieneś zwrócić uwagę, a czego unikać!

- ❑ Sprawdź swoją listę znajomych, którym udostępniasz treści w sieci. Przejrzyj również listę osób, które obserwujesz i które obserwują Ciebie. Czy utrzymujesz kontakty ze wszystkimi, czy publikowane przez nich treści są dla Ciebie ciekawe i inspirujące? Usuń z kontaktów te osoby, z którymi naprawdę nic Cię nie łączy.
- ❑ Zanim opublikujesz – pomyśl dwa razy. Zastanów się, czy naprawdę chcesz zamieścić daną treść w sieci. Czy za kilka lat nadal chciałabyś/chciałbyś, aby inne osoby miały dostęp do takiej informacji na Twój temat? Rozważ, czy dana informacja może Ci zaszkodzić w przyszłości, np. utrudnić znalezienie wymarzonej pracy lub zniechęcić do Ciebie osobę, na której Ci zależy?
- ❑ Bądź świadomym użytkownikiem. Kontroluj publikowane treści i dbaj, aby pokazywały Twoją najlepszą stronę. Zawsze!

Jakie mogą być skutki niedbania o wizerunek w sieci?

Utrata
dobrego
imienia

Hejt i
cyberprzemoc

Utrata
możliwości
rozwoju

Sextortion

Kradzież tożsamości i danych

Fake news, dezinformacja w sieci.
Internet wie wszystko, ale czasem
kłamie.



W każdej minucie na całym świecie powstają miliony wpisów internetowych, nowych stron, publikowane są tysiące zdjęć i tworzone są do nic podpisy.

Często, jeśli nie znamy odpowiedzi na jakieś pytanie, wpisujemy je w wyszukiwarkę.

Czy zawsze otrzymujemy odpowiedzi w 100 procentach ściśle?

Ile razy napotykamy na bzdury??

.....

No właśnie.

CO TO JEST FAKE NEWS?

Fake news to fałszywa informacja w sieci, stworzona specjalnie, by wprowadzić w błąd.



Co zrobić by być czujnym na fake newsy i dezinformację"



Czy informacja pochodzi z autoryzowanego źródła (np. urząd, poważna gazeta, autorytet naukowy)?



Czy jest to świeży news, a nie odgrzana sensacja sprzed lat?



Czy pierwszy raz widzimy bulwersujące nas zdjęcie (może widzieliśmy już je kiedyś, tylko z innym podpisem)?



Czy mamy pewność, że to zdjęcie nie jest fotomontażem?



Czy jesteśmy pewni, że ta informacja lub zdjęcie po udostępnieniu nie robi nikomu krzywdy??

Gdzie zgłaszać fake newsy??

Ponieważ istnieją fake newsy, istnieją też ludzie i firmy zajmujące się ich śledzeniem, na przykład:

AFP Sprawdzam
-sprawdzam.afp.com

Stowarzyszenie
Demagog-
Demagog.org.pl

Konkret24
Konkret24.tvn24.pl

Demaskator24.pl
Demaskator24.pl

- Jeśli widzisz fake newsa na portalach społecznościowych, zgłoś to do moderatora danego portalu (kliknij w górnym prawym rogu postu i wybierz odpowiednią opcję)
- Jeśli znajomy, kolega, przyjaciółka opublikuje fake newsa, dobrą praktyką jest napisanie do niego i poinformowanie go, że opublikował „wkrętkę”. Dobrze zostawić komentarz do tej wiadomości i **#OznaczDezinfo**.
- Można też wyjaśnić , skąd wiemy, że podana informacja jest nieprawdziwa (np. podać instytucję, która ją sprostowała)

Dziękujemy za uwagę! 😊

Włącz krytyczne myślenie!

***Nie wierz we wszystko co znajdziesz
w Internecie***