MOJA LEKCJA
ODPOWIEDZIALNOŚCI

CENTRUM SZKOLENIA POLICJI

Cyberprzestępczość

NIE LAJKUJĘ, REAGUJĘ!

Hejt dla Ciebie to tylko złośliwy komentarz pod zdjęciem, a dla kogoś może być to początek koszmaru....

HEJT

(ang. *hate* – nienawiść) to jedna z form cyberprzemocy polegająca na publikowaniu obraźliwych i agresywnych treści, które ośmieszają lub poniżają inną osobę.

Hejterzy to najczęściej osoby anonimowe i właśnie to poczucie anonimowości sprawia, że w sieci są bardzo agresywni. Hejterów należy ignorować, aby nie eskalować ich zachowań.

Cyberprzemoc jest przestępstwem, za które grozi odpowiedzialność karna

CYBERPRZEMOC

to przemoc z użyciem technologii informacyjnych i komunikacyjnych, a jej przejawy to:

- nękanie, straszenie, szantażowanie w sieci
- publikowanie ośmieszających, wulgarnych komentarzy i postów
- publikowanie poniżających filmów lub zdjęć bez zgody osób, których wizerunek udostępniamy
- włamania na konta pocztowe lub konta serwisów społecznościowych
- tworzenie kompromitujących stron internetowych, filmów, fotomontaży
- podszywanie się w sieci pod inne osoby
- wykluczanie ze społeczności internetowych

CYBERPRZESTĘPCZOŚĆ

to wszelka aktywność, w której komputer lub sieć komputerowa stanowi narzędzie, przedmiot albo środowisko działalności przestępczej.

Najpopularniejsze rodzaje cyberprzestępstw

Phishing to metoda oszustwa, w której celem przestępcy jest uzyskanie ważnych danych, np. danych logowania, numeru karty kredytowej, jak również numeru PESEL.

Phishing to jeden z najpopularniejszych typów ataków, za pomocą których cyberprzestępcy próbują nas oszukać. Podszywając się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych czy nawet naszych znajomych, starają się wyłudzić nasze dane do logowania, np. do kont bankowych lub używanych przez nas kont społecznościowych czy systemów biznesowych.

Nazwa phishing budzi skojarzenia z *fishingiem* – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę". Najczęściej wykorzystują do tego sfałszowane e-maile i SMS-y, ale coraz częściej także komunikatory i portale społecznościowe (np. poprzez „metodę na BLIKa").

Wiadomości phishingowe są tak przygotowywane przez cyberprzestępców, aby wyglądały na autentyczne, ale w rzeczywistości są fałszywe. Mogą próbować skłonić nas do ujawnienia poufnych informacji, zawierać link do strony internetowej rozprzestrzeniającej szkodliwe oprogramowanie (często przestępcy używają nazw witryn podobnych do autentycznych) lub mieć zainfekowany załącznik.

Hacking to włamania poprzez pokonywanie zabezpieczeń, umożliwiające zdalny, nielegalny dostęp do czyjegoś komputera. Hakerzy bardzo łatwo mogą się dostać do naszego komputera – zarówno z dostępem, jak i bez dostępu do internetu. Wchodząc do systemu innego użytkownika, lokalizują jego słabe punkty. Są nimi przede wszystkim te właściwości, które umożliwiają

dostęp do naszych danych, a dotyczy to systemów oprogramowania i ich legalności, zastosowanych zabezpieczeń i ich aktualności, a także stron, na które się logujemy.

Malware to uciążliwy lub złośliwy typ oprogramowania, który ma na celu potajemnie skraść dane, zniszczyć pliki, a nawet zablokować dostęp do urządzenia. Rodzaje złośliwego oprogramowania obejmują oprogramowanie szpiegujące (spyware), adware, phishing, wirusy, trojany, rootkity, zagrożenia typu ransomware oraz porywaczy przeglądarki.

Cyberstalking to zespół zachowań w sieci, które polegają głównie na nękaniu drugiej osoby przez internet, poprzez wysyłanie niechcianych wiadomości np. przez media społecznościowe, komunikatory, pocztę elektroniczną.

Cyberstalking, definiowany jako cyberprzemoc, to coraz bardziej powszechne zjawisko. Osoba, która się tego dopuszcza, określana jest mianem cyberstalkera. Może ona za swoją ofiarę obrać zarówno osobę prywatną, grupę osób, jak i instytucję czy organizację.

Cyberstalker nie ma w zamierzeniu uzyskania dostępu do danych wrażliwych czy wyłudzenia dostępu do konta internetowego. Jego głównym celem działania jest psychiczne nękanie osoby, w tym wzbudzenie strachu, czujności, zakłopotania czy poczucia bezwartościowości, tak by ofiara spełniła jego żądania. Mogą być nimi np. korzyści majątkowe czy realizacja określonych celów przez ofiarę.

Cyberstalking stosowany wobec ludzi młodych może doprowadzić nawet do zachowań skrajnych, jak np. próby samobójcze czy całkowite wyobcowanie z grupy rówieśników.

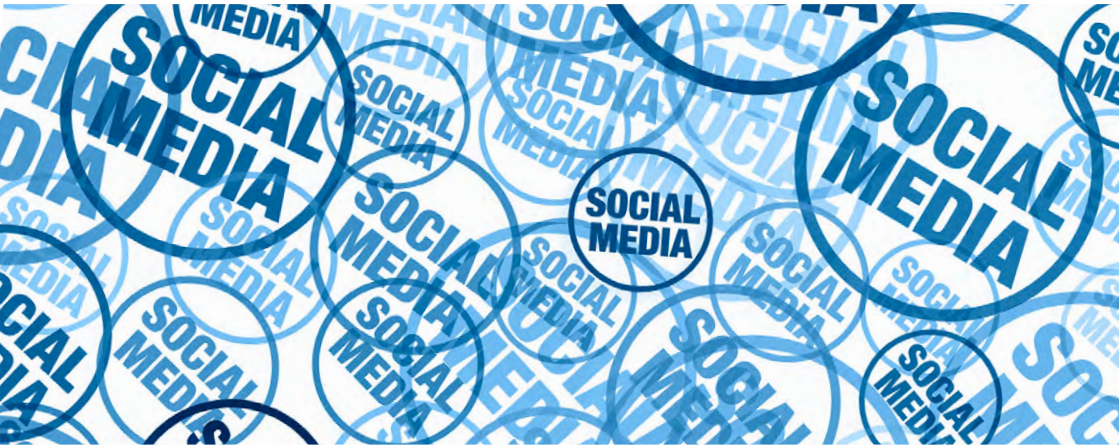
AKTYWNOŚĆ W INTERNECIE	ZAGROŻENIA Z INTERNETU
Serwisy społecznościowe	
• kontakt ze znajomymi (wpisy na tablicy i używanie komunikatorów) • dzielenie się zdjęciami i filmami • udostępnienie swojej obecności w danym miejscu	• kradzież konta lub podszywanie się pod Ciebie • powiązanie Twojej osoby z innymi osobami • ujawnianie informacji na temat miejsca oraz osób, z którymi obecnie jesteś
Serwisy streamingowe	
• wrzucanie swoich filmów do serwisu • oglądanie filmów udostępnianych przez inne osoby • live streaming (transmisja na żywo)	• obce osoby oglądają również Twoje filmy • oglądanie filmów nieodpowiednich dla Twojego wieku • ujawnianie poprzez streaming miejsca zamieszkania i rzeczy, które posiadasz • patostreaming
E-mail	
• korespondencja z innymi osobami • wysyłanie plików w załącznikach	• otwieranie wiadomości od obcych osób lub firm • udostępnienie swoich danych innym osobom • kradzież kont i dostępu do innych serwisów
Przeglądanie stron	
• nauka (książki, poradniki, wikipedia) • przeglądanie w poszukiwaniu informacji • zakupy przez internet	• wchodzenie na obce strony, udostępnienie danych • zainfekowanie komputera przez strony internetowe • przeglądanie stron z treściami nieodpowiednimi do wieku
Gry	
• granie wspólnie ze znajomymi oraz oddzielnie • zakładanie kont w serwisach z grami • relacje z osobami podczas grania online	• kradzież kont lub przedmiotów z konta • podawanie loginów i haseł innym osobom • niezweryfikowanie ratingu wiekowego „PEGI” • uzależnienie od gier

JAK NIE STAĆ SIĘ OFIARĄ CYBERPRZEMOCY?

- pamiętaj, że po umieszczeniu czegoś w sieci tracisz nad tym kontrolę
- zastanów się, czy ufasz osobie, której udostępniasz swoje prywatne zdjęcia i filmy, ponieważ Wasza relacja może się zmienić i to, co wcześniej udostępniłeś, może zostać użyte w celu skompromitowania Cię czy też szantażowania
- zabezpiecz telefon przed dostępem innych osób, tak aby nikt nie mógł się pod Ciebie podszyć
- korzystaj z programów antywirusowych
- stwórz silne hasła i co jakiś czas zmieniaj je na urządzeniach elektronicznych, z których korzystasz
- nie udostępniaj swoich loginów i haseł, chroń swoje konta w serwisach społecznościowych
- jeżeli korzystasz z czyjegoś komputera, pamiętaj, aby zawsze się wylogować
- nigdy nie podawaj swoich prawdziwych danych
- nigdy nie podawaj nieznanym osobom swojego adresu zamieszkania i numeru telefonu
- pamiętaj, że nigdy nie wiesz, z kim rozmawiasz w internecie
- jeśli otrzymałeś wiadomość, która jest obraźliwa lub wulgarna, powiadom od razu rodziców lub zaufaną osobę
- w internecie traktuj innych użytkowników tak, jak sam chcesz być traktowany
- podczas spotkań z osobami poznanymi w internecie zachowaj szczególną ostrożność; na takie spotkanie zabierz ze sobą osobę zaufaną i powiadom o tym swoich rodziców lub opiekunów
- w internecie nikt nie jest bezkarny, każdy nasz ruch zostaje odnotowany; każdy podejrzany o popełnienie przestępstwa lub wykroczenia w internecie może zostać namierzony
- pamiętaj, że długi czas spędzony przy komputerze lub konsoli wpływa negatywnie na Twoje zdrowie i może prowadzić do uzależnienia
- zakupów w internecie dokonuj rozważnie i zawsze sprawdzaj sprzedawcę, np. poprzez sprawdzenie w wyszukiwarce jego numeru telefonu lub adresu email, czy nie pojawił się on

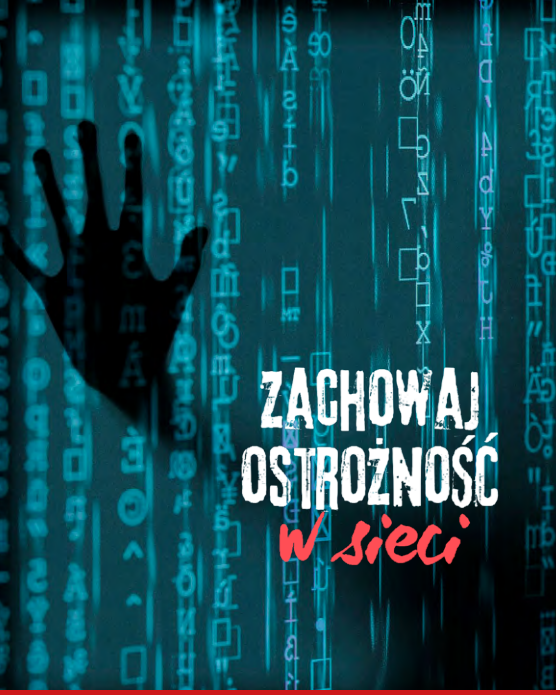
na innych aukcjach lub w ofertach, w których internauci zostali oszukani

- dbaj o dobre zachowania w internecie, nie rób rzeczy, które mogłyby narazić Ciebie lub innych na utratę życia lub zdrowia
- publikując coś w internecie jako żart, zawsze poświęć jakiś czas na zastanowienie się, czy wszystkie osoby, których to dotyczy, będą odbierać to tak samo
- pamiętaj, dane umieszczone w internecie pozostają w nim na zawsze!
- usunięcie zdjęcia, filmu czy wpisu nie oznacza, iż całkowicie usunęliśmy je z internetu, czy – tym bardziej – z pamięci ludzi



GDY PADNIESZ OFIARĄ CYBERPRZEMOCY, PAMIĘTAJ, ABY:

- nie wchodzić w ponowny kontakt z agresorem, gdyż może to go prowokować do dalszych ataków na Ciebie
- powiedz rodzicom o tym, co Cię spotkało
- zgłoś się do szkolnego psychologa lub pedagoga
- zachowaj dowody, tzn. zrób zrzut ekranu, zachowaj SMS-y lub wiadomości
- zgłoś administratorom serwisów społecznościowych wszelkie niewłaściwe zachowania
- powiadom organy ścigania (Policję, prokuraturę)



Cyberprzemoc nie zostawia śladów na ciele, a w psychice człowieka, dlatego SZUKAJ POMOCY!!!

Pomoc możesz uzyskać pod następującymi numerami telefonów:

800 12 12 12 – Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka **(czynny 7 dni w tygodniu, 24 godziny na dobę)**

116 111 – Telefon Zaufania dla Dzieci i Młodzieży **(czynny 7 dni w tygodniu, 24 godziny na dobę)**

Jeżeli widzisz w sieci coś, co Cię niepokoi, możesz to zgłosić na następujących stronach internetowych:

https://incydent.cert.pl

https://dyzurnet.pl

https://policja.pl/pol/form/dodaj153,Formularz-kontaktowy-Cyberprzestepczosc.html

Opracowanie merytoryczne:
Zakład Służby Kryminalnej

Opracowanie graficzne i druk:
Wydział Wydawnictw i Poligrafii

Zdjęcia: pixabay.com

Centrum Szkolenia Policji w Legionowie
www.csp.edu.pl

Materiał informacyjny na stronie: