Szkoła Podstawowa nr 4
w Andrychowie

BEZPIECZEŃSTWO CYFROWE

– JAK SIĘ CHRONIĆ PRZED ZAGROŻENIAMI CZEKAJĄCYMI W SIECI?

CZYM JEST BEZPIECZEŃSTWO CYFROWE ?

Bezpieczeństwo cyfrowe polega na zapewnianiu bezpieczeństwa sieci zasobów cyfrowych, procesów i działań w systemach informatycznych. Bezpieczeństwo cyfrowe oznacza odpowiednie korzystanie z zasobu Internetu – z zachowaniem wszelkich środków ostrożności i przy wykorzystaniu wiedzy na temat zagrożeń wynikających z szybkiego rozwoju technologicznego.

DO PODSTAWOWYCH ZAGROŻEŃ MOŻNA ZALICZYĆ:

Błędy człowieka

– kiedy do wycieku informacji dochodzi ze względu na zaniechanie, brak wiedzy albo umyślne działanie administratorów systemu lub jego użytkowników;

Katastrofy

– wszystkie zdarzenia mające charakter losowy, takie jak powodzie, trzęsienia ziemi, pożary oraz wypadki, w których zawinił człowiek, jak np. katastrofy budowlane czy komunikacyjne, prowadzące do zakłóceń funkcjonowania systemów;

Awarie

– problemy techniczne ze sprzętem czy oprogramowaniem, które uniemożliwiają jego normalne funkcjonowanie;

Celowe działania

– ataki ukierunkowane na kradzież sprzętu i zasobów informacji;

CYBERPRZEMOC

- Cyberprzemoc oznacza 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 (Wikipedia).
- Osobę dopuszczającą się takich czynów określa się stalkerem.
- Cyberprzemoc pojawiła się na przełomie XX i XXI w. Jest to przeniesienie przemocy i innych agresywnych zachowań z życia realnego do wirtualnego.
- W Internecie najczęstszą formą jest przemoc słowna, która może wyrządzić ogromne szkody, podobne do przemocy fizycznej. Jest szczególnie groźna, ponieważ kompromitujące (poniżające) materiały zostają udostępnione w krótkim czasie dla wielu osób. Pozostają w sieci na zawsze, jako kopie na wielu komputerach, nawet wówczas, gdy ustalono i ukarano sprawcę.

CYBERPRZEMOC

Zamieszczanie kompromitujących nagrań w sieci

Publikacja zdjęć i nagrań zawierających wizerunek osoby, która nie wyraziła na to zgody, jest niezgodna z przepisami dotyczącymi ochrony danych osobowych, w tym RODO.
W dzisiejszych czasach młodzi ludzie często dla zabawy robią sobie nawzajem zdjęcia lub nagrywają filmiki - publikowanie takich materiałów bez zgody osoby, która na nich widnieje, jest niezgodna z prawem.

CYBERPRZEMOC

Hejt

Hejt (z ang. hate – nienawiść) to tzw. mowa nienawiści.
Hejt w Internecie to zjawisko społeczne o charakterze poniżającym, obserwowane w środowisku Internetu.

Przejawia się najczęściej w formie pozostawienia w sieci negatywnej uwagi na temat konkretnej osoby lub grupy osób (np. w poście na portalu, w filmiku, a także w komentarzu pod czyimś zdjęciem czy postem).

Co ważne, nie ma na celu konstruktywnej krytyki (choć czasem próbuje przybrać jej pozory), a ośmieszenie, upokorzenie danej osoby czy agresję.

OCHRONA DANYCH OSOBOWYCH

Informacje raz umieszczone w Internecie nie giną nigdy, dlatego też ważne jest rozsądne korzystanie ze stron wymagających podania swoich danych personalnych takich jak imię, nazwisko, adres zamieszkania czy PESEL.
Za każdym razem, gdy właściciel strony prosi nas o podanie takich danych, musi również zamieścić informację o celu ich pozyskania, a także poprosić o wyrażenie zgody na ich przetwarzanie.

Kwestie prawne związane z ochroną danych osobowych, w szczególności zapewniające stosowanie przepisów ogólnego rozporządzenia o ochronie danych, zawarto w ustawie dnia 10 maja 2018 r. o ochronie danych osobowych.

OCHRONA PRAW AUTORSKICH

Ochrona danych osobowych dotyczy również praw autorskich, czyli tzw. własności intelektualnej. Ochrona prawem autorskim obowiązuje już w momencie tworzenia oryginalnego utworu i przysługuje twórcy z chwilą utrwalenia utworu, bez konieczności spełniania jakichkolwiek formalnych wymogów.

Na mocy przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych dozwolone jest wykorzystanie cudzej twórczości na prawach cytatu, należy jednak pamiętać zawsze o zaznaczeniu cytatu i wskazaniu źródła. Wiele osób zapomina, że dotyczy to również zdjęć zamieszczonych w Internecie – każde z nich ma jakiegoś autora, więc należy go wskazać.

OCHRONA WŁASNEGO WIZERUNKU

Zgodnie z zapisami art. 81 ustawy o prawie autorskim i prawach pokrewnych:

„1. Rozpowszechnienie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

2. Zezwolenia nie wymaga rozpowszechnienie wizerunku:
1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza”.

OCHRONA WŁASNEGO WIZERUNKU

W dobie rozwijających się szybko mediów społecznościowych (ang. social media) istotne jest uwrażliwianie na to, co zamieszczamy na swoich własnych kontach, np. na popularnym Facebooku czy Instagramie.
Użytkownicy mediów społecznościowych powinni zdawać sobie sprawę z konsekwencji, jakie niesie za sobą np. upublicznianie zdjęć z imprezy lub pokazujących sytuacje prywatne czy zawierających wizerunek osób trzecich.

Ponadto należy pamiętać, że dostęp do materiałów umieszczanych przez nas w sieci mogą pewnego dnia uzyskać osoby niepożądane (np. włamując się na konto na portalu), więc dla własnego bezpieczeństwa zawsze warto zastanowić się, co warto upublicznić, a co lepiej zachować dla siebie.

ZŁOŚLIWE OPROGRAMOWANIE

- To specjalne oprogramowanie stworzone po to, by zakłócić pracę komputera.
- Określane jest jako wirusy, robaki, programy szpiegujące lub konie trojańskie – w zależności od sposobu atakowania infrastruktury.
- Oprogramowanie takie może wykradać informacje poufne, spowolnić działanie komputera lub wysyłać fałszywe e-maile z konta użytkownika, często bez jego wiedzy.
- Szkodliwe oprogramowanie wprowadzają na urządzenia sami użytkownicy sprzętu komputerowego np. za pośrednictwem poczty elektronicznej, pobierając z Internetu bezpłatne programy, klikając linki, które zawierają ukryte złośliwe oprogramowanie, otwierając załączniki do wiadomości internetowej czy klikając zdjęcia-wirusy wysłane z portali społecznościowych.
- Wprowadzamy je również za pomocą urządzeń zewnętrznych (np. pendrive'a).

ZABEZPIECZENIE SPRZĘTÓW I KONT INTERNETOWYCH

- Złośliwe oprogramowanie może być również „schowane” w fałszywych komunikatach o błędach lub w wyskakujących okienkach informujących nas o potencjalnych cyberzagrożeniach. Dlatego tak ważna jest ostrożność i rozsądek.

- Powinno się instalować tylko legalne oprogramowania, aktualizować je oraz system operacyjny komputera, unikać podejrzanych stron, nie powinni klikać w wyskakujące okienka z prośbami o pobranie oprogramowania czy w nieznane linki, nie powinni pobierać plików, których źródła nie znają (np. załączników do e-maili od obcych nadawców).

- Szczególnie ostrożnym trzeba być w przypadku wiadomości, w których obiecywana jest adresatowi wygrana, np. po kliknięciu w dany link czy wysłaniu SMS-a na wskazany numer.

ZABEZPIECZENIE SPRZĘTÓW I KONT INTERNETOWYCH

- Warto też pamiętać, że zawsze należy stosować programy antywirusowe, jeśli pobieramy pliki z Internetu, a w przypadku korzystania z urządzeń mobilnych i z publicznej sieci Wi-Fi, należy odznaczyć pole dotyczące automatycznego połączenia w przyszłości.

- Przed włamaniem na nasze prywatne konta chronią nas hasła. Ważne jest, aby były one odpowiednio sformułowane. Nie mogą być zbyt łatwe, powinny raczej stanowić kombinację małych i dużych liter, cyfr oraz znaków specjalnych (np. dwukropek, średnik, nawias), ale z drugiej strony nie mogą być też tak skomplikowane, żeby nie można ich było zapamiętać, gdyż nierozsądnym działaniem jest utrwalanie haseł, np. w zeszycie czy w notatce w telefonie komórkowym, nawet gdy wydaje nam się, że nikt poza nami nie ma do nich dostępu.

WIARYGODNOŚĆ INFORMACJI W INTERNECIE

WAŻNE !

01. Internet stał się obecnie głównym źródłem informacji. Współcześnie rzadziej korzysta się z encyklopedii czy słowników drukowanych, a do zdobywania informacji wykorzystuje się zasoby Internetu. Nie jest to niczym złym. Komputer może być naszym sprzymierzeńcem w nauce, jednak ważne jest, by mądrze go używać.

02. Warto zwrócić uwagę, że treści umieszczane w Internecie są bardzo różne i nie zawsze wiarygodne. Nie podlegają one (tak jak w tradycyjnych środkach przekazu) krytyce wydawców i redaktorów. Kontrola informacji zawartych w Internecie również jest bardzo ograniczona.

03. Portale internetowe mogą publikować różne informacje, lecz to od nas zależy, czy uznamy je za wiarygodne i pochodzące ze źródła, któremu można wierzyć, czy też za nieprzydatne i nieprawdziwe. Na pewno zawsze warto sprawdzić, czy artykuły zamieszczane w poszczególnych serwisach pisane są w oparciu o rzetelne i obiektywne źródła, naukowe opracowania, czy też są przypadkowe i niepotwierdzone.

INTERNET JEST WSPANIAŁYM NARZĘDZIEM DO TEGO, BY POZNAWAĆ ŚWIAT, POSZERZAĆ HORYZONTY, UCZYĆ SIĘ I ROZWIJAĆ. WARTO ZAWSZE PAMIĘTAĆ BY KORZYSTAĆ Z NIEGO BEZPIECZNIE.

https://info.mobywatel.gov.pl/uslugi/bezpiecznie-w-sieciygreatsite.com

Infolinia dla Obywatela
+48 222 500 110

https://cyberprofilaktyka.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf