Bądź bezpieczny w cyfrowym świecie

Informacja dla rodziców

Kębło, 02.01.2017 rok

Szanowni Państwo!

Wasze dzieci a zarazem nasi uczniowie i podopieczni chętnie korzystają z możliwości jakie niesie elektroniczny system przekazu informacji. Telefon i komputer stały się codziennymi narzędziami komunikacji. Korzystanie z telefonu i komputera oprócz niewątpliwy korzyści niesie też pewien rodzaj zagrożeń w sferze wolności osobistych jak i możliwości poniesienia strat materialnych, często bardzo dużych. Nasi uczniowie ze względu na osobiste cechy charakteru są szczególnie podatni na manipulację również taką, która wypływa z komunikowania się z innymi osobami przy pomocy urządzeń elektronicznych.

Pragnę Państwu przybliżyć i przypomnieć najbardziej popularne metody stosowane w komunikacji elektronicznej mające cechy wkraczania w sferę wolności i naruszające godność osobistą jak również najpopularniejsze metody działania oszustów, których ofiarami padają ludzie posługujący się, do przesyłania informacji telefonem i komputerem

I. Niektóre rozpoznane rodzaje zagrożeń w sferze wolności osobistej stosowane w przekazie informacji przy pomocy urządzeń cyfrowych.

1. **Cyberprzemoc** - przemoc z użyciem technologii opartych na przekazie cyfrowym. Podstawowymi narzędziami stosowanymi w cyberprzemocy są telefony komórkowe i komputery.

Do takich działań zalicza się m.in. :

- wyzywanie,
- straszenie,
- poniżanie kogoś w Internecie lub przy użyciu telefonu,
- robienie komuś zdjęć lub filmów bez jego zgody, publikowanie ich i rozsyłanie
- podszywanie się pod kogoś w sieci.

Cyberprzemoc może dotknąć wszystkich użytkowników telefonów komórkowych i Internetu. Sprawcy cyberprzemocy mają przekonanie o swojej anonimowości i bezkarności, co stanowi główną zachętę do działania.

Akty cyberprzemocy, wyrządzają bardzo dużą krzywdę. Z pozycji dziecka stają się tragedią. Wrzucony do sieci Internetowej film przedstawiający atakowaną osobę w niezręcznej lub intymnej sytuacji np. toalecie, łazience, podczas przebierania itp. opatrzony złośliwymi komentarzami nieznajomych osób, budzi u dziecka przekonanie, że wszyscy już

film widzieli rodzi głębokie negatywne emocje, frustrację, poczucie bezradności, a w skrajnych przypadkach prowadzi do prób samobójczych.

Charakterystyczną cechą cyberprzemocy, jest ciągłość jej trwania. Cyberprzemoc nie kończy się na komputerze lub telefonie, przenosi się na życie młodego człowieka w środowisku rówieśniczym. Film lub inny przekaz raz wrzucony do sieci Internetowej pozostaje tam na zawsze. Atakowana osoba żyje w nieustannym poczuciu zagrożenia – obawia się następnych ataków lub reakcji kolejnych osób, które są świadkami jego upokorzenia.

Czy można pomóc?

W przypadku, kiedy dziecko padnie ofiarą cyberprzemocy, ważne jest udzielenie mu wsparcia, a równocześnie – zadbanie o zablokowanie ośmieszających publikacji lub krzywdzących materiałów, w tym celu należy skontaktować się z administratorem serwisu, w którym zostały opublikowane materiały. Wcześniej jednak należy zabezpieczyć dowody – mogą to być, w zależności od sytuacji: zrzuty ekranu, SMS-y z pogróżkami, zapis rozmów z komunikatorów internetowych lub czatowych, obraźliwe maile. Mogą one pomóc w zidentyfikowaniu sprawcy. Jeśli doszło do przestępstwa, należy o sprawie poinformować policję. Podobnie należy postąpić, jeśli sprawca pozostaje nieznany, policja może uzyskać dostęp do billingów telefonicznych lub logów z serwera administratora serwisu pozwalające na zidentyfikowanie go. Ważna jest świadomość możliwych konsekwencji prawnych takich działań.

2. <u>Szkodliwe treści – to materiały, które mogą wywoływać negatywne reakcje u odbiorcy lub promują niebezpieczne zachowania.</u>

Zaliczamy do nich między innymi:

- treści pornograficzne, w tym treści pedofilskie czyli materiały prezentujące seksualne wykorzystywanie dzieci;
- treści obrazujące przemoc, obrażenia fizyczne, deformacje ciała, np. zdjęcia lub filmy przedstawiające ofiary wypadków, okrucieństwo wobec zwierząt;
- treści nawołujące do samookaleczeń lub samobójstw, bądź zachowań szkodliwych dla zdrowia, np. zachęcanie do zażywania niebezpiecznych substancji np. leków czy narkotyków;
- treści dyskryminacyjne, nawołujące do wrogości, a nawet nienawiści wobec różnych grup społecznych lub jednostek.

Obecność tych treści w przestrzeni publicznej, a także w Internecie, nie zawsze jest regulowana przez prawo. Mogą to być materiały uznawane za legalne (choć niebezpieczne) jak również materiały nielegalne np.: pornografia z udziałem osób małoletnich czy nawoływanie do przemocy na tle rasowym, których rozpowszechnianie jest objęte w Polsce sankcjami prawnymi. W przewarzającej części materiały tego typu są legalne więc brak jest prawnych możliwości eliminowania ich z przestrzeni publicznej.

Treści szkodliwe są atrakcyjne i poszukiwane przez młodego odbiorcę na przykład:

- różnego rodzaju wyniszczające diety,
- zachęcanie do stosowania substancji zwiększających masę mięśniową,
- zaproszenie do wstąpienia do sekt.

Kontakt dzieci i młodzieży z treściami tego typu może spowodować długotrwałe negatywne konsekwencje emocjonalne i poznawcze. Może skutkować fałszywym postrzeganiem świata, podważyć poczucie bezpieczeństwa lub zbudować przekonanie, że patologiczne zachowania są normą. Ze względu na brak pełnej dojrzałości społecznej nasi uczniowie łatwiej poddają się wpływom, również tym związanym z nakłanianiem do nielegalnej działalności lub nielegalnych zachowań.

Jak chronić i zapobiegać?

Najważniejszym elementem chroniącym dzieci i młodzież przed skutkami oddziaływania szkodliwych treści odkrywanych w Internecie jest dyskretna rodzicielska obserwacja i rozmowa z dzieckiem na temat tych treści.

Do ograniczenia kontaktu dzieci i młodzieży z nielegalnymi i szkodliwymi treściami w Internecie może służyć oprogramowanie filtrujące, zainstalowane lokalnie na komputerze, telefonie komórkowym, przeglądarce lub udostępnione przez dostawcę Internetu. Filtrowanie treści internetowych odbywa się zazwyczaj w oparciu listę stron, które dziecko może lub nie może odwiedzać. Może to być równię filtr oparty o słowa kluczowe zawarte w treści strony. Dziecko może znaleźć treści szkodliwe i niebezpieczne również w swojej skrzynce mailowej, do której trafią pod postacią spamu. Oprogramowanie mające zwiększyć tak zwaną kontrole rodzicielską ma wiele ograniczeń i stosunkowo niewielką skuteczność w stosunku do treści graficznych praktyczne żadną. Oprogramowanie nie zastąpi świadomego zagrożeń i czujnego rodzica lub opiekuna. W przypadku zauważenia niebezpiecznych dla dziecka lub nielegalnych treści można ten fakt zgłosić zespołowi **dyżurnet.pl** - **www.dyzurnet.pl** . Zespół zajmuje się przyjmowaniem zgłoszeń dotyczących nielegalnych treści publikowanych w Internecie i ich analizą. Współpracuje w tym zakresie z policją.

3. Niebezpieczne kontakty

Komunikacja elektroniczna posiada wiele cech, np.: szybkość, dostępność i łatwość nawiązywania wirtualnych znajomości, będących jej zaletami, ale stwarza także realne zagrożenie szczególnie dla dzieci i młodzieży. Kontakty z nieznajomymi mogą być groźne, jeżeli prowadzą do spotkania w realnym świecie. Pozorna anonimowość Internetu i łatwość tworzenia fałszywych profili w portalach społecznościowych powoduje, że wśród znajomych dziecka poznanych w Internecie, mogą znaleźć się osoby, których jedynym celem jest wykorzystanie dziecka lub młodego człowieka służące zaspokojeniu wynaturzonych oczekiwań.

Przykładem takich zachowań jest możliwość uwiedzenia dziecka przez osobę dorosłą. Proces, podczas którego dorosły nawiązuje i buduje relacje z dzieckiem w celu uwiedzenia go, wykorzystania seksualnego lub skłonienia do prostytucji albo produkcji pornografii nazywany jest groomingiem. W czasie takiego kontaktu osoba dorosła poddaje dziecko procesowi psychomanipulacji przekonując dziecko że jest jedyną osobą która jest w stanie je zrozumieć. Jednocześnie zachęca dziecko o utrzymania tych „przyjacielskich„ relacji w tajemnicy przed bliskim. Po tych działaniach najczęściej zachęca dziecko do przesłania intymnych zdjęć lub do zachowań prostytucyjnych.

Od roku 2010 polskie prawo traktuje uwodzenie dzieci w Internecie jako przestępstwo. Kodeks Karny przewiduje do 2 lat pozbawienia wolności za składanie osobie małoletniej poniżej lat 15 propozycji obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych.

Pamiętaj i uświadom dziecku.

Nigdy nie wiadomo, czy osoba, z którą się kontaktujemy przez Internet jest tą, za którą się podaje.

4. Sexting

Zjawisko przesyłania treści o charakterze erotycznym, głównie swoich nagich lub półnagich zdjęć, za pomocą Internetu i telefonu komórkowego. Jest popularny wśród nastolatków, przede wszystkim z powodu chęci rozrywki, początku fascynacji seksem, zainteresowania płcią przeciwną, braku doświadczenia, ciekawości czy nieśmiałości. Konsekwencje takich zachowań są zwykle bardzo poważne dla ich autora. Niejednokrotnie wysłane przyjacielowi zdjęcie zostało przez niego wykorzystywane i trafiało do publicznego obiegu w celu ośmieszenia lub zemsty po tym jak osoba, która udostępniła zdjęcie zerwała ze swoją dziewczyną czy chłopakiem. Powszechne są również przypadki szantażu, w których

odbiorca tego typu zdjęć grozi ich ujawnieniem i opublikowaniem w Internecie, próbując skłonić w ten sposób ofiarę do określonego zachowania.

Oddzielnym zjawiskiem, kojarzoną z sekstingiem, jest oferowanie własnych zdjęć erotycznych w zamian za korzyści materialne np. doładowanie telefonu lub prezentowanie swojego ciała przy użyciu kamerki internetowej na jednym z wideo-chatów w zamian za „napiwki" czyli realne pieniądze przekazywane za pośrednictwem serwisu obsługującego wideo-chaty.

Pamiętaj, ku przestrodze.

Pamiętaj o tym, że raz udostępnione komuś zdjęcia mogą zostać użyte przeciwko nam i bardzo łatwo opublikowane na różnych stronach, co uniemożliwia ich całkowite usunięcie. Nawet po kilku latach takie zdjęcia mogą zostać znalezione i użyte czyniąc nieprzewidywalne szkody ich autorowi.

5. Uzależnienie od komputera i telefonu

Nadużywanie komputera i telefony (Internet, gry, komunikatory) prowadzi często do dezorganizacji codziennego życia, problemów z nauką, zaniedbania dotychczasowych zainteresowań na skutek intensywnego korzystania z gier lub komunikatorów.

W czasach gdy Internet zdominował komunikację i dostęp do informacji, trudno wyznaczyć jednoznaczne opisać sytuację pozwalające na odróżnienie „normalnego" od „patologicznego" korzystania komputera i telefonu. Jedynym kryterium nie może być ilość czasu spędzanego przed komputerem lub z telefonem lecz sposób wykorzystania tego czasu. Symptomami które powinny skłonić rodziców lub opiekunów do bacznego zwrócenia uwagi na dziecko spędzające czas przed komputerem lub z telefonem

- porzucenie dotychczasowych zainteresowań na rzecz komputera,
- zaniedbywanie obowiązków rodzinnych i szkolnych z powodu aktywności w Internecie;
- pojawianie się konfliktów rodzinnych związanych z Internetem;
- kłamstwa dotyczące czasu spędzanego w Internecie;
- podejmowanie nieudanych prób ograniczenia czasu spędzonego przed komputerem;
- reagowanie rozdrażnieniem lub nawet agresją, gdy korzystanie z komputera jest utrudnione lub niemożliwe.

Patologiczne użytkowanie komputera lub telefonu może szczególnie dotyczyć jednej lub kilku form aktywności online:

- gry internetowe, zwłaszcza te pozwalające na rywalizację online z innymi użytkownikami;

- aktywność na portalach społecznościowych;
- pornografia i cyberseks;
- hazard online.

Pod rozwagę.

W przypadku nadużywania Internetu lub telefonu nie jest właściwym rozwiązaniem odcięcie dostępu dziecka do tych urządzeń z wyjątkiem sytuacji gdy używanie zagraża zdrowiu lub życiu dziecka. Dziecko a tym bardziej uzależnione zawsze znajdzie dostęp do sieci w szkole lub u rówieśników. Znaczenie ma natomiast postawa dziecka wobec korzystania z usług udostępnianych w sieci Internetowej.

6. Naruszanie prywatności

Internet daje użytkownikom złudne poczucie anonimowości. Jednocześnie – dzięki wyszukiwarkom – pozwala na łatwe znalezienie i powiązanie wielu informacji dotyczących konkretnej osoby. Warto zatem zwrócić uwagę dzieci na ochronę ich prywatności podczas korzystania z Internetu. Dotyczy to:

- podawania swoich danych personalnych,
- adresu,
- nazwy szkoły,
- zdjęć, form spędzania wolnego czasu

W trosce o bezpieczeństwo dziecka warto zadbać, żeby publikowane przez nie zdjęcia były dostępne wyłącznie osobom, dla których są przeznaczone. Należy także pamiętać i uświadamiać dziecku, że ilość znajomości zawartych za pomocą portalu społocznościowego nie świadczy o naszej wartości. Ważnym elementem, na który warto zwrócić uwagę są usługi geolokalizacyjne – np. informacja, że dziecko zalogowało się w kinie, wraz z informacją, że to wspólne wyjście z rodzicami, to potencjalne ułatwienie dla złodzieja.

Istotnym aspektem bezpieczeństwa w sieci są hasła zabezpieczające skrzynkę pocztową, profil społecznościowy lub konto w grze internetowej. Dzieci udostępniają dane służące do logowania zarówno swoim znajomym np. w dowód przyjaźni, jak i obcym osobom np. z prośbą o przejście trudnego etapu gry lub w efekcie wyłudzenia. Sytuacja taka, rodzi konsekwencje, które potrafią realnie odbić się na życiu dziecka – publikowanie złośliwych wpisów w imieniu osoby, która utraciła kontrolę nad swoim kontem, może skutkować ośmieszeniem, niesłusznymi podejrzeniami i odrzuceniem środowiska, w którym dziecko żyje.

Pamiętaj i przypomnij dziecku.

Publikując dane o sobie należy pamiętać, że informacja: zdjęcie, wpis, komentarz raz umieszczona w Internecie zostaje w nim praktycznie na zawsze. Bezpieczne hasło – powinno być długiegie, wykorzystujące litery, cyfry i znaki specjalne, przechowywanie hasła tylko w głowie, nikomu nie udostępniamy hasła. Nie powinno się stosować tego samego hasła do wszystkich używanych przez serwisów i skrzynek pocztowych –kradzież hasła może wtedy oznaczać całkowite przejęcie internetowej tożsamości użytkownika. Sprawdzajmy przy pomocy wyszukiwarek jakie informacje w sieci rozpowszechniane są na nasz temat i naszych bliskich, pamiętajmy o tym aby zapytać osobę, o której informację lub zdjęcie publikujemy w sieci, o zgodę na publikacje.

II. Nie dajmy się oszukać w sieci

1. Wyłudzanie danych osobowych

Wyłudzanie danych osobowych na przekupnego policjanta – ransomware - trojan

Zarażony przez wirusa komputer w pewnym momencie wyświetla komunikat na cały ekran, opatrzony zwykle logo policji i napisem Rzeczpospolita Polska, a czasem nawet zdjęciem aktualnego prezydenta i bliżej nieznanego policjanta wyższego szczebla. Można w nim przeczytać, że sprzęt został zablokowany z powodu przeglądania przez użytkownika dziecięcej pornografii lub nielegalnego ściągania danych. Wystarczy wpłacić określoną sumę np. 500 zł na podany numer konta, by odblokować dostęp do komputera. Wirusa **ransomware** skutecznie usuwa oprogramowania antywirusowe.

Phishing bankowy - wyłudzanie danych osobowych z internetowego konta

Metoda doskonalona latami przez wielu przestępców. **Phishing bankowy** to **wyłudzanie danych osobowych**, polegające na podsunięciu ofierze fałszywej strony internetowej banku, by ta wpisała w niej swoje dane logowania. Na przeszkodzie oszustów stoją mocne zabezpieczenia w postaci konieczności autoryzacji przelewów za pomocą listy haseł lub esemesów. A i to udaje im się obejść - banki zazwyczaj oferują dodanie danych osoby zaufanej, do której transfery nie muszą być zatwierdzane. Wiedząc to, złodzieje muszą zdobyć tylko jeden kod potwierdzający. I ta sztuka im wychodzi, gdyż oszukują klienta banku, podsuwając mu informację o rzekomej zmianie numerów kont i potrzebie zatwierdzenia tego działania hasłem esemesowym.

Jak się ustrzec **phishingu bankowego**:

- czytaj informacje od banku - na oficjalnej stronie banku,

- nie ufaj każdemu mailowi, jaki przychodzi (rzekomo) z banku - przyglądajcie się adresom. zwróćcie uwagę, czy adres strony logowania się na konto jest prawidłowy np. nbank.pl zamiast mbank.pl itp.
- najbardziej wyrafinowanym przykładem phishingu jest rozsyłanie fałszywych maili z ostrzeżeniem o phishingu. W celu rzekomego zabezpieczenia swojego konta należało w odpowiedzi wysłać swoje obecne hasło.

Wyłudzanie danych osobowych - nigeryjski przekręt

Nigeryjski przekręt to klasyka wyłudzania danych osobowych. Na e-mail lub facebookowe konto przychodzi napisany pokraczną polszczyzną czasem też po angielsku list od zamorskiego bogacza, którego miejscowa władza chce zniszczyć. Prześladowany człowiek potrzebuje naszej pomocy - chce przetransferować swój majątek do Polski. Konieczny jest pośrednik na miejscu, a także uiszczenie "drobnej" opłaty manipulacyjnej, bogacz bowiem, jak przystało na bogacza, nie posiada gotówki lub podanie numeru karty kredytowej. Na czym polega korzyść „pośrednika", ogromna nagroda nawet kilka milionów dolarów. Czasem przekręt trwa krótko – zamorski prześladowany bogacz znika po przesłaniu mu danych do karty lub opłaty manipulacyjnej. Często jednak ciągnie się dłużej, bo na drodze do zrealizowania transferu gigantycznego majątku do Polski staje coraz więcej przeszkód, wymagających kolejnych opłat.

Wyłudzanie danych osobowych na Facebooku

Ostatnio można zaobserwować natężenie takich działań, jak **wyłudzanie danych osobowych na Facebooku** - przede wszystkim hasła. Statystyki wskazują że, znaczna część internetowej społeczności posiada jedno hasło do wielu zastosowań - tak, hasło do Facebooka często pasuje też do e-maila, Twittera, a nawet konta bankowego. Metoda, jaką posługują się oszuści, to wysyłanie fałszywych maili z informacją o konieczności zmiany hasła. Inne zjawisko to pojawiające się na tablicach użytkowników linki z dziwnymi fotografiami i podpisami typu: "Uwaga na czarny samochód…" itp. Po kliknięciu złośliwa aplikacja pyta użytkownika o możliwość publikacji treści w jego imieniu - wyrażając na to zgodę, dajemy oszustom prezent kończący się niejednokrotnie znacznymi kłopotami.

Wyłudzanie danych osobowych – „kup pan Viagrę"

Spam mailowy zawierający ofertę kupna Viagry lub innego „cudownego" medykamentu w rewelacyjnych cenach - na dodatek z zachowaniem pełnej dyskrecji. Jedyne, co trzeba zrobić, to podać swoje dane oraz numer karty kredytowej. Przekręt oczywiście występuje w wielu różnych wersjach - łączy je to, że dotyczą zakupu różnych dóbr z czarnego rynku, takich jak np. broń czy leki na receptę.

Adresy stron internetowych poświęcone cyberprzemocy i oszustwom internetowym.

1. www.dyzurnet.pl
2. http://dzieci.pl/
3. http://www.przemocwsieci.pl/
4. http://www.oszustwsieci.pl/

Opracował: Stanisław Widz