Artykuł finansowany z budżetu państwa w ramach dotacji celowej dla Powiatu Łukowskiego.

CO CZYHA W SIECI ???

Rozwój technologii spowodował powszechny dostęp do informacji. Z Internetu korzysta już niemal każdy człowiek. Jednakże, rozwój technologii spowodował też zwiększenie zagrożeń.

Artykuł niniejszy ma za zadanie przybliżyć i uświadomić czytelnika jakie zagrożenia związane są z użytkowaniem Internetu.

NIEBEZPIECZNE TREŚCI

Nie trzeba zagłębiać się w tak zwany deepnet by spotkać się z negatywnymi treściami internetowymi. Internet jest pełny materiałów pornograficznych, materiałów związanych z przemocą lub promujące przestępstwa, przy czym żadne z nich nie nadaje się dla nieletnich. W Internecie znajdziemy też mnóstwo wulgaryzmów czy innych obscenicznych treści.

Najistotniejsze w tym przypadku są zagrożenia wobec osób małoletnich. Warto pamiętać, iż każdy rodzić ma możliwość wprowadzenia tak zwanej kontroli rodzicielskiej. Polega ona na blokowaniu niektórych stron czy treści.

CYBERPRZEMOC

Relacje w Internecie miedzy osobami mogą mieć negatywne skutki. Niezdrowe relacje mogą przybrać formy przemocy jednakże dokonane w Internecie. Jedną z podstawowych form jest tak zwany hejt.

Osoby umieszczające informację w Internecie musza liczyć się z byciem ocenianym. Niektóre wypowiedzi przekraczają jednak dopuszczalne normy społeczne. „Hejt" stanowi stosunkowo nowe zjawisko jednak zatacza coraz większe kręgi. Nie ma definicji „hejtu" słowo to pochodzi z języka angielskiego „*hate*"- nienawidzić. Zatem mianem „hejtera" określa się osobę umieszczająca w Internecie obraźliwe komentarze, celem sprowokowania kłótni lub obniżenia samooceny ocenianej osoby.

Chociaż polskie prawo nie przewiduje przestępstwa „hejtu" to przewiduje mechanizmy odpowiedzialności karnej lub cywilnej. „Hejt" najczęściej będzie zatem stanowił naruszenie dóbr osobistych, pomówienie czy znieważenie. Zatem w zależności od klasyfikacji czynu może zostać orzeczona kara grzywny, ograniczenia wolności a nawet pozbawienia wolności. Należy przy tym pamiętać , iż używanie pseudonimów czy anonimowych kont nie chroni przed rozpoznaniem bowiem organy ścigania mają coraz lepsze narzędzia celem ustalenia tożsamości przestępców.

Najlepszą metoda by ustrzec się „hejtu" jest ignorowanie złośliwych komentarzy. Warto też korzystać z możliwości usuwania komentarzy czy blokowania „hejterów". Każda osoba zniesławiona lub pomówiona ma również prawo domagać się ochrony pranej.

Inną formą przemocy, jest zjawisko wyłudzania zdjęć w szczególności o charakterze erotycznym zwane „doxingiem". Termin ten pochodzi od angielskiego słowa documents (skrót dox, docs). Polega to na poszukiwaniu śladów dotyczących danego użytkownika celem zgromadzenia jak największej ilości informacji. Następnie informacje te mają być udostępnione jak najszerszemu gronu lub mają służyć do szantażu użytkownika, którego dotyczą, a co za tym idzie uzyskania środków finansowych.

Ofiarą „doxingu" może paść niemal każdy. Im więcej informacji o sobie udostępniamy tym więcej danych posiadają przestępcy. Biorąc jednak pod uwagę, iż celem „doxingu" jest głównie szantaż i uzyskanie z tego środków finansowych ofiarami ataków stają się głównie celebryci, politycy oraz inne znane osobę.

Celem ochrony przed zagrożeniem warto zadbać o prywatność w portalach społecznościowych. Warto też używać innych nicków i haseł na forach i portalach. Dodatkowo warto używać innych adresów email do publikowania w sieci a w innych do porozumienia się z zaufanymi odbiorcami.

Poza „doxingiem" użytkownik Internetu narażony jest na tak zwany „scam" i „phishing".

„Phishing" to metoda mająca za zadanie wyłudzenie danych wrażliwych. Atak cyberprzestępców może doprowadzić do utraty dostępu do maila ale też środków zgromadzonych na rachunku bankowym.

Przestępcy wykorzystując fałszywe maile czy sms- y ale też portali społecznościowych, podszywając się pod znane firmy czy instytucje, próbują nakłonić ofiarę do wejścia w

zamieszczony w wiadomości link. Prowadzą one do strony internetowej spreparowanej przez oszustów. Z pomocą tej strony przestępcy uzyskują dane niezbędne do zalogowania się w systemie na przykład systemie banku. Przestępcy następnie wykorzystują tak zdobyte dane do dokonania oszustwa.

„Scam" to inaczej oszustwo. Ma one za zadanie wzbudzenie czyjegoś zaufania, celem wyłudzenia środków finansowych. Najczęściej ofierze proponuje się udział w ogromnych zyskach, przy minimalnym wkładzie własnym. Po przelaniu przez ofiarę wkładu pieniądze te otrzymuje oszust i znika. Oszust jest zazwyczaj przedstawicielem spadkodawcy, znanego przedsiębiorcy lub kogoś wzbudzającego zaufania.

Najlepszą obroną przed oszustami jest zasada ograniczonego zaufania w stosunku do maili czy smsów. Nie klikajmy przesyłanych nam linków,. Pod żadnym pozorem nie podawaj nikomu swoich danych osobowych, nawet jeśli wiązałoby się to z duża wygraną czy dawało możliwość przeczytania ciekawego artykułu. Jeśli chcemy komuś pomóc poprzez wsparcie zbiórki pamiętajmy by najpierw się upewnić czy przekazane przez nas środki na pewno trafią do osób potrzebujących.

WIRUSY

Wirus jest programem mających za zadanie uszkodzić komputer użytkownika lub śledzić jego działalnie w sieci. Również wirusy umożliwiają przestępcy zdobycie naszych danych, a co za tym idzie wykorzystać je do oszustw czy szantażu. Celem uchronienia się od niepożądanych skutków nie otwierajmy plików z nieznanych źródeł lub nieznanego typu, w szczególności od nieznanego dostawcy. Stosujmy oryginalne programy antywirusowe.

Podsumowując, poszerzajmy swoją wiedzę w zakresie zagrożeń internetowych bowiem jest to najlepszy sposób na uniknięcie bycia ofiarą oszustwa.

Adwokat

Paulina Warząchowska

Zadanie zostało sfinansowane z budżetu państwa w ramach dotacji celowej przekazanej Powiatowi Łukowskiemu