Opracowanie: Fundacja Młodzi Ludziom

Bezpieczeństwo w sieci.

Powszechny dostęp do globalnej sieci jaką jest Internet stał się nieodzownym elementem naszej codzienności. Można stwierdzić, że Internet jest aktualnie wykorzystywany praktycznie w każdej dziedzinie życia – w pracy, nauce, zabawie, wymianie informacji, a także w kontaktach międzyludzkich.
Z powszechną dostępnością do Internetu nierozłącznie wiążą się również zagrożenia związane cyberprzestępczością, bowiem za jego pośrednictwem popełniana jest cała gama różnego rodzaju przestępstw, natomiast użytkownicy Internetu nie zawsze zadają sobie sprawę z tego jak zachować bezpieczeństwo w sieci.

Wśród najpopularniejszych przestępstw komputerowych wymieniane są:

Phising - polegający na działaniu mającym na celu zdobycie danych wrażliwych (poufnych), takich jak np. hasła do aplikacji. Najczęściej do phisingu wykorzystywana jest korespondecja mailowa. Przestępcy podszywają się pod podmioty, które są nam znane, wykorzystując w tym celu np. serwisy społecznościowe, banki lub systemy płatności, sklepy internetowe.
Tego rodzaju wiadomości mailowe, rzekomo pochodzące od znanych nam podmiotów czy instytucji niełatwo jest odróżnić od oryginalnych. Zazwyczaj bowiem jedyną różnicą jest to, że zawierają odnośnik phishingowy – w postaci linku lub pliku, których kliknięcie lub otworzenie może powodować przekierowanie do fałszywej strony do logowania, celem pozyskania naszych danych.

Oszustwo na „nigeryjskiego księcia" - uznawane za najstarszy rodzaj oszustwa komputerowego. Polega on na wysłaniu za pośrednictwem maila obietnicy, uzyskania majątku od nieznanego wcześniej krewnego lub też prawnika działającego w imieniu zmarłego milionera w zamian za dokonanie płatności z góry określonej kwoty potrzebnej na "załatwienie formalności".

Kradzież tożsamości - do tego typu przestępstw dochodzi najczęściej w taki sposób, iż sprawca za pośrednictwem maila przesyła ofertę atrakcyjnej pracy, nie wymagającej dużego wysiłku, bądź doświadczenia, z którą związane jest wysokie wynagrodzenie. Od potencjalnej ofiary wymaga się przesłania cv wraz z kopią dokumentów tożsamości, numeru konta bankowego. W przypadku spełnienia przez użytkownika wskazanych wymagań, sprawca posiada wszystkie informacje, aby posłużyć się tożsamością ofiary i wykorzystać to w celu popełnienia kolejnych przestępstw.

Malware - to przestępstwo komputerowe, do którego wykorzystywane jest złośliwe oprogramowanie. Ma to miejsce najczęściej poprzez szpiegowanie w sieci, tzw. konie trojańskie, czy rejestrator klawiszy, a także wirusy

Skimming – to przestępstwo polegające na nielegalnym skopiowaniu zawartości paska magnetycznego lub chipa karty płatniczej. Odbywa się to bez wiedzy posiadacza karty. Celem skimmingu jest stworzenie kopii dla realizacji płatności za towary i usługi lub wypłat z bankomatów, bez wiedzy i zgody posiadacza karty.

Reasumując, ważne jest, aby korzystając z globalnej sieci pamiętać, że istnieje cyberprzestępczość.
Otrzymując wiadomości od firm, czy serwisów, z których się nie korzysta, powinno zachować się ostrożność przy odczytywaniu takiej korespondencji, bądź ją usunąć. W sytuacji otrzymywania korespondencji od nadawców podających się za podmioty, z usług których korzystamy - np. banków, operatorów telekomunikacyjnych, należy dokładnie taką korespondencję przeczytać, zwrócić uwagę na jej treść, zawarte w niej linki, bądź przekierowania. Naszą czujność również powinno zwiększyć żądanie podawania loginów i haseł. Warto również zachować zdrowy rozsądek w sytuacji rzekomo wyjątkowo korzystnych ofert (pracy, sprzedaży), a także w przypadku korespondencji od nieznanych nam rzekomych krewnych lub innych osób.