Przekształcenie tradycyjnej przestępczości w cyberprzestępczość

Wkład generała Emmanuela Sfakianakisa, dyrektora Wydziału Anty Cyberprzestępczości greckiej policji.

Wprowadzenie

Celem tej części jest wykazanie, w jaki sposób cyber i inne technologie elektroniczne są obecnie w służbie przestępcom, których działania wymagają śledczych z zaawansowanymi umiejętnościami cybernetycznymi. Powoli i konsekwentnie musimy zdawać sobie sprawę z tego, że w nadchodzącym stuleciu i za pośrednictwem Internetu nasze życie stanie się piękniejsze, przyjemniejsze, bardziej produktywne i dzięki wyjątkowym doświadczeniom, wbrew coraz bardziej wyrafinowanemu i rosnącemu cyberprzestępstwu. Musimy zdać sobie sprawę, że przestępcy - złodzieje, włamywacze, rabusie, terroryści itp. - powoli porzucają narzędzia epoki kamienia i wkraczają w erę zaawansowanych technologii, w której za pośrednictwem mediów elektronicznych będą mogli zaatakować nasze życie i osiągnąć swoje cele, tym razem online. Aby zrozumieć wagę możliwych nadużyć w cyberprzestrzeni, zadajmy sobie następujące pytania:

• Popełniania morderstw lub szantażu i zbierania pieniędzy na wymuszenia, nie pozostawiając po sobie śladu?

• Ingerować w operacje organizacyjne (samoloty, pociągi, metro, instytucje bankowe itp.)?

Niestety, dzisiaj przez Internet jest to możliwe i jest realizowane,codziennie. Obecna era online zmieniła wszystko wokół nas. Internet daje nam wiedzę, informacje, komunikację, ekonomię rozwój, dobre samopoczucie i wiele więcej. Może również sprawiać nam ból poprzez przestępstwa. Dzisiaj wiele osób demonizuje Internet, zamiast akceptować fakt, że jest on jak elektryczność. Energia elektryczna ułatwia nam życie, ale może być również śmiertelna. Jeśli nie będziemy przestrzegać zasad korzystania z Internetu, możemy stać się ofiarami zachowań przestępczych, które różnią się stopniem surowości i niebezpieczeństwem. Ludzie muszą zrozumieć, że dziś przestępczość zmieniła się z tradycyjnej na elektroniczną. Smutne jest to, że na całym świecie prawodawstwo nie dogoniło tej mutacji. W rezultacie w sądach toczą się obecnie tysiące spraw karnych i cywilnych, które są przestępstwami czysto elektronicznymi lub zawierają elementy wymagające dochodzenia w sprawie cyberprzestępczości. Należy zauważyć, że stopniowo każde przestępstwo będzie wymagało dochodzenia elektronicznego. Wszystkie dochodzenia policyjne w sprawie poważnych przestępstw (terroryzm, zabójstwo, szantaż, porwanie, zapobieganie samobójstwom, zaginięcia itp.) Obejmują element elektroniczny. W rezultacie rozpaczliwie potrzebna jest nowa rasa śledczych policji. W związku z tym wszyscy kuratorzy sądowi, śledczy, prokuratorzy, a także sędziowie zajmujący się sprawami, które posiadają dowody na istnienie elementów elektronicznych, muszą znać podstawowe zasady przestępczości elektronicznej. Od 1995 roku, jako policyjny śledczy cyberprzestępczy, obsłużyłem ponad dziesięć tysięcy spraw z łącznej liczby około dwudziestu tysięcy spraw mojego Departamentu. Jak pamiętam, w 1995 r. Mieliśmy od dwóch do trzech spraw miesięcznie. Obecnie w 2017 r. Skargi dotyczące cyberprzestrzeni wynoszą średnio osiemdziesiąt dziennie. Typowym cyberprzestępczością jest oprogramowanie ransomware, w którym wirus instaluje się na komputerze ofiary. Blokuje wszystkie funkcje, wyświetlając na ekranie komunikat żądający okupu w zamian za odblokowanie komputera. Poniżej znajdują się dwa typowe przypadki ransomware, z jakimi często spotykają się władze.

Przypadek pierwszy: Wirus ransomware uderza w komputery ofiar, blokując wszystkie funkcje i wyświetlając komunikat o wymuszeniu. Wiadomość ma logo jednostki ds. w alki z cyberprzestępczością w policji danego kraju, twierdząc, że ten komputer - komputer ofiary - odwiedził witryny o

zabronionych treściach i że został ukarany grzywną w wysokości X euro. Wiadomość o wymuszeniu zawiera także instrukcje i linki do stron internetowych, na których ofiara może kupić e-gotówkę i zapłacić okup.

Przypadek drugi: Podobny wirus ransomware, który uderzył w wiele komputerów, szyfruje wszystkie pliki komputera, wyświetlając wiadomość o wymuszeniu wymagającą kwoty X euro, którą można zapłacić w e-walucie BitCoin. W obecnych okolicznościach transakcje BitCoin są niemożliwe do wykrycia.

Faktem jest, że niewykrywalne e-waluty uniemożliwiły władzom na całym świecie właściwe prowadzenie dochodzeń i ściganie przestępstw. Warto przeczytać oficjalne dokumenty przedstawiające cyberprzestrzeń w przyszłości. Jednym z takich dokumentów jest biała księga: prognoza i metodologia Cisco VNI, 2015-2020 , która przewiduje i analizuje rozwój i trendy w Internecie. W przeciwieństwie do tej wykładniczej ewolucji, która ma miejsce w cyberprzestrzeni, opracowanie nowych ram prawnych dotyczących przestępczości elektronicznej jest znacznie opóźnione. Prognozy Cisco są ogólnie konserwatywne i niezwykle dokładne, pokazując światową tendencję do szybkiego dostosowywania się do nowych technologii. Smutne jest to, że dostępność zaawansowanych technologii zwiększa stopień zaawansowania przestępczości.

Przestępczość elektroniczna

Najpierw zdefiniujmy, co rozumiemy przez przestępczość elektroniczną, której cyberprzestępczość jest w przeważającej części. Zasadniczo przestępczość elektroniczna to przestępstwa popełnione przy użyciu technologii

• W przypadku samodzielnych komputerów, fałszowanie pieniędzy lub tworzenie fałszywych dokumentów. Lub,

• Z wykorzystaniem niepewności w cyberprzestrzeni, gdzie istnieje szerokie spektrum przestępstw, od piractwa własności intelektualnej po cybernękanie.

Przypadek trzeci: Przestępcy elektroniczni posiadający wysokiej jakości sprzęt do produkcji kart kredytowych we współpracy z kasą sklepu „zgromadzili" dane paska magnetycznego ważnych kart i następnie osadzili je na fałszywych kartach noszących nazwy użytkowników. W związku z tym wyświetlanie ważnego dowodu tożsamości ze zdjęciem dawało wiarygodność karcie kredytowej, ponieważ obie miały tę samą nazwę. Jednak natychmiastowe powiadomienie o użyciu podrobionej karty doprowadziło policję do sklepu, w którym była używana, i do aresztowania przestępcy elektronicznego.

Cyberprzestępczość jest szybka, popełniana w milisekundach i często nie jest rozpoznawana przez ofiary. Szybkość i łatwość przeprowadzania cyberprzestępczości przyciągnęła wykwalifikowanych cyberprzestępców, co stanowi poważną wadę i niepokój dla organów ścigania na całym świecie. Powody rozpowszechnienia się cyberprzestępczości mogą być następujące:

• Specjalistyczna wiedza nie zawsze jest wymagana.

• Można popełnić na odległość i anonimowo.

• Umożliwia przestępcom szybkie i niedrogie komunikowanie się z osobami o podobnych poglądach, nawet w czasie rzeczywistym, bez konieczności przeprowadzki.

• Trudno jest ustalić rzeczywiste pochodzenie cyberprzestępczości.

• Jest bez granic. Bardzo często wymaga wielonarodowej współpracy w celu prowadzenia dochodzeń i prześladowań.

• Ścigane i ścigane cyberprzestępstwa stanowią wierzchołek góry lodowej.

• Dochodzenie policyjne jest stosunkowo trudne i wymaga doskonałego szkolenia i specjalistycznej wiedzy.

Dla osób zaangażowanych w funkcjonariuszy policji, prokuratorów okręgowych, sędziów i prawników zajmujących się przestępczością elektroniczną wymagana jest specjalistyczna wiedza, doświadczenie i umiejętności. Ponieważ jednak wszystkie przestrzegają litery prawa, nie mogą skutecznie wykonywać swoich obowiązków, jeżeli nie są wspierane przez odpowiednią infrastrukturę prawną.

Formy cyberprzestępczości

Według sondażu przeprowadzonego przez McConnell International w 52 krajach przestępstwa popełnione w cyberprzestrzeni są w większości następujące:

• Utrudnianie ruchu (cyber)

• Modyfikacja i kradzież danych

• Inwazja i sabotaż w sieci

• Nieautoryzowany dostęp

• Zastrzyki wirusa

• Traktowanie przestępstw

• Plagiat i oszustwo

Najczęstsze cyberprzestępstwa, które utrzymują organy zajmujące się zwalczaniem cyberprzestępczości, są następujące:

• Oszustwa przez Internet

• Przestępstwa związane z moralnością

• Pękanie i hackowanie

• Przejmowanie oprogramowania i piractwo

• Karty kredytowe

• Handel narkotykami

• Przestępstwa za pośrednictwem czatów

• Naruszenie - wprowadzenie w błąd danych osobowych (media społecznościowe itp.)

Badanie przestępstw elektronicznych

Podczas nawigacji w cyberprzestrzeni wszyscy użytkownicy Internetu pozostawiają unikalne ślady swojej tożsamości elektronicznej. Każdy ślad elektroniczny składa się co najmniej z trzech części, które zapewniają wyjątkowość tożsamości:

• Adres IP (adres połączenia internetowego przyznany dla tej konkretnej komunikacji)

• Data (na podstawie położenia geograficznego używanego urządzenia)

• Strefa czasowa lokalizacji urządzenia.

• Prawdopodobnie numer seryjny podłączonego urządzenia (komputer, telefon itp.)

• Prawdopodobnie numer seryjny używanej aplikacji (przeglądarka, serwer itp.)

W każdym dochodzeniu online podejmowana jest próba zlokalizowania elektronicznego śladu przestępcy, który jest unikalny dla każdej wymiany danych i jest bardzo ważnym dowodem w każdym postępowaniu sądowym. Oprócz korzystania z ich prawdziwej tożsamości można uzyskać dostęp do Internetu, publikując i podpisując jako anonimowe lub nawet używając pseudonimu. Ten stan domniemanej anonimowości w Internecie ułatwia i motywuje sprawców, którzy myślą, że zawsze pozostaną anonimowi, aby popełniać przestępstwa online. Anonimowość utrudnia ich zlokalizowanie, ale gdy organy ścigania dysponują odpowiednimi narzędziami i doświadczeniem, sprawcy nie będą w stanie uniknąć prawa. Jeśli anonimowa osoba popełni cyberprzestępczość, organy ścigania, w drodze postanowienia sądu, mogą otrzymać cyber ślady od dostawcy usług internetowych (ISP). Często proces ten wymaga czasu, co utrudnia proces ścigania. Podsumowując, w Internecie nie ma anonimowości, ale zdarzają się przypadki, w których aktor online korzystał z różnych elektronicznych programów unikania śledzenia lub bezpłatnych sieci bezprzewodowych. Jednak w takich przypadkach przestępstwa są badane za pomocą specjalnych technik prowadzących do identyfikacji sprawcy.

Przypadek czwarty: odrzucony kochanek opublikował anonimowo zdjęcia byłego partnera z numerem telefonu i zaproszeniami erotycznymi. Jednak z powodu braku doświadczenia w protokołach internetowych kochanek pozostawił wiele śladów, które doprowadziły do udanego ścigania.

Przypadek piąty: śledczy policji stwierdzili istnienie cyberprzestępcy, który handlował nielegalnymi / niemoralnymi materiałami online działającymi w kafejkach internetowych, które zapewniały anonimowość użytkownika. Jednak za pomocą specjalnych programów policja była w stanie rozpoznać ślady własności intelektualnej, które doprowadziły do aresztowania podejrzanego.

Hakerzy i crackerzy

„Zabójców cyberprzestrzeni" można podzielić na dwie kategorie, w zależności od ich intencji, sposobu ich penetracji i pożądanego rezultatu.

Hakerzy: zwykle hakerzy „atakują" komputer bez wyrządzania jakichkolwiek szkód lub pozostawiania śladów. Ich motywem może być przyjemność lub ciekawość, bez szukania korzyści ekonomicznych. W niektórych przypadkach hakerzy identyfikują słabość cyberbezpieczeństwa i zgłaszają ją właścicielowi komputera w nadziei na uznanie lub inną korzyść.

Crackerzy: Zwykle crackerzy „atakują" komputer, próbując zidentyfikować słabość cyberbezpieczeństwa i wykorzystać ją. Oznacza to, że szukają korzyści finansowych lub powodują cyfrowy wandalizm. Mówiąc prościej, crackerzy to cyberprzestępcy, którzy „atakują" swój system, aby uczyć się lub zdobywać coś w celu późniejszego popełnienia czynu niezgodnego z prawem.

Przypadek szósty: muły finansowe. Właściciele dużych sum pieniędzy, którzy chcą przenieść je z konta na konto, anonimowo zabiegają o posiadaczy rachunków, którzy mogą „przenieść" swoje pieniądze za bardzo wysoką „opłatą". W ten sposób tacy właściciele działają w sposób niewidoczny dla władz.

Dochodzenie w sprawie cyberprzestępczości

Dochodzenie w sprawie cyberprzestępstw jest dość trudnym i bardzo czasochłonnym zadaniem. Śledczy działają na zasadzie, że „przestępca zawsze pozostawia ślady. " Dochodzenia w sprawie

cyberprzestępczości obejmują identyfikację śladów elektronicznych. Dochodzenie może potrwać kilka minut do lat. Może to być czasochłonne, ponieważ cyberprzestępcy czerpią korzyści z braku ustawodawstwa, które zapewnia śledczym szybki dostęp do historycznych danych z komunikacji cybernetycznej. W każdej ankiecie internetowej próbuje się zidentyfikować ślady online przestępcy, które są unikalne, gdy każdy użytkownik Internetu porusza się po Internecie. Każdy rekord śladu może zawierać kilka parametrów, takich jak data, znacznik czasu i numery seryjne powiązanych aplikacji (przeglądarka, edytor tekstu, procesor obrazu itp.). Zbiór takich parametrów faktycznych służy jako ważny i niepodważalny dowód sądowy w ściganiu podejrzanego przestępstwa.

Cyberoszustwa finansowe

Podstawową zasadą oszustwa internetowego jest przekonanie ofiary, że płacąc teraz niewielką kwotę, czeka znacznie większa kwota. Oszustwa internetowe rosną wykładniczo, a jednocześnie wyrafinowanie oszustów. Zakres cyberprzestępstw finansowych osiągnął punkt, w którym powstały takie kategorie, jak opisano poniżej.

<u>List Nigeryjski</u>

Jest to wiadomość e-mail, która informuje potencjalną ofiarę, że ktoś, prawdopodobnie „były wysoki urzędnik wysokiego szczebla" w rządzie Nigerii, potrzebuje pomocy w przekazaniu - pod przykryciem - dużej kwoty (np. 30 mln USD) i jest skłonny uiścić „wysoką" opłatę w zamian za taką usługę. Odbiorca tego listu proszony jest o pomoc, działając jako „muł pieniężny", tymczasowo otrzymujący tę kwotę na swoim koncie. W liście podkreślono poufność, której należy przestrzegać. W pierwszej kolejności cyberprzestępcy proszą kandydata będącego ofiarą o zgodę i podanie informacji dotyczących jego kont bankowych oraz wszelkich informacji „uznanych za niezbędne" do przeprowadzenia transakcji. Wiele razy i na prośbę niczego niepodejrzewającej ofiary przedstawiane są dokumenty, które wydają się autentyczne i oficjalne, w celu wyeliminowania wszelkich wątpliwości, jakie mogła mieć naiwna ofiara. Gdy ofiara odpowiada, niekończący się proces wymiany maili, e-maili i połączeń telefonicznych zaczyna sprawiać, że potencjalna ofiara uważa, że proces otrzymywania dużych pieniędzy jest bliski. Tuż przed domniemanym „ostatecznym transferem pieniędzy" cyberprzestępcy informują ofiarę o nieoczekiwanym problemie. Takim problemem może być zapłata podatku, nieoczekiwana opłata lub potrzeba przekupienia pracownika banku, który autoryzuje przekaz pieniężny. Tutaj zaczyna się „haczyk". Cyberprzestępcy twierdzą, że nie są w stanie pokryć tych nieoczekiwanych kosztów, ponieważ duże pieniądze są zablokowane w transferze, i proszą potencjalną ofiarę o zapłatę tej kwoty, która, jak powiada ofierze, zostanie zwrócona po zakończeniu transakcja. Niektóre ofiary przekonuje się nawet do udania się do Nigerii, aby zapłacić kwotę w celu „sfinalizowania" transakcji. Co więcej, ofiara jest wprowadzana w błąd, że nie potrzebuje wizy, trafia nielegalnie do kraju, wpadając głębiej w sieć nigeryjskich przestępców. Takie przestępstwa nie są nowe. Odbywały się one za pośrednictwem listów i faksów. Dzisiaj kontynuują, z tą różnicą, że Internet jest infrastrukturą przestępców.

Przypadek siódmy. Pani o najwyższym poziomie wykształcenia została przekonana do wyjazdu do europejskiej stolicy w celu otrzymania „nagrodzonych" funduszy. Po przybyciu została potraktowana poważnie, prawdopodobnie w oczekiwaniu na transfer środków nastąpi. Pani została zabrana do banku, gdzie spotkała ją na korytarzu, prawdopodobnie wysokiego „urzędnika bankowego", który zapewnił ją o swoich funduszach. „Urzędnik" zwrócił uwagę, że bank natychmiast zwolni „nagrodę" w wysokości 12 milionów euro, jak tylko zostanie zapłacony podatek w wysokości 0,5 miliona euro. Pani przekazała swoje środki „urzędnikowi bankowemu". Przestępcy zostali w końcu złapani, ale fundusze zostały utracone na zawsze.

Hiszpańskie Lotto

Ta forma oszustwa odbywa się poprzez masowe wysyłanie e-maili do losowych użytkowników Internetu. Te wiadomości informują ich, że w loterii internetowej zarobili dużą ilość pieniędzy, rzędu milionów dolarów. Jednak odbiorcy nigdy nie brali udziału w lotto. Sprawcy, aby uwierzyć, używają nazwisk od dużych firm (np. Microsoft, Yahoo itp.) I towarzysząc wiadomościom wysyłają fałszywe certyfikaty dotyczące rzekomego losowania elektronicznego. Oszustwo polega na tym, że prosi domniemanych zwycięzców o dokonanie przedpłaty niektórych podatków, zwykle w wysokości kilku tysięcy dolarów. Co zaskakujące, ta kategoria cyberprzestępstw pochłania setki ofiar.

Phishing danych

Wyłudzanie informacji jest zwykle przeprowadzane przez wysyłanie masowych wiadomości e-mail ze spamem, które powinny być wysyłane przez istniejącą i legalną korporację (bank, sklep internetowy, usługa płatności elektronicznych itp.) W celu wprowadzenia odbiorcy w błąd i pobrania prywatnych danych osobowych i dane finansowe. Następnie sprawcy tego rodzaju oszustwa wykorzystują te dane do popełnienia przestępstwa. Zazwyczaj proszą o numery kart kredytowych z terminem płatności i numerem zabezpieczającym. Dzięki tym informacjom powstają fałszywe karty bankowe do nieuczciwego użytku.

Piractwo oprogramowania

Piractwo komputerowe oznacza nieautoryzowane powielanie i / lub usuwanie programów komputerowych chronionych prawem autorskim. Dystrybucja odtwarzanego materiału rozpoczęła się od obsługi płyt CD lub dyskietek. Jednak rozprzestrzenianie się Internetu otworzyło drogę do nowej formy przestępczości, w której materiał jest sprzedawany za pośrednictwem poczty e-mail, czatu lub aplikacji peer-to-peer.

Przypadek ósmy. Pakiet oprogramowania - własność intelektualna International Welding Corporation (IWC) - został nielegalnie wprowadzony na rynek i rozpowszechniany w Europie za pośrednictwem Internetu, co spowodowało stratę wielu milionów euro dla twórców oprogramowania. Nielegalne reklamy przyciągnęły uwagę IWC, a w ciągu kilku minut przestępcy zostali zlokalizowani i postawieni przed sądem.

Karty kredytowe

Zjawiska oszustw związane z używaniem kart kredytowych na rynkach internetowych rosną w szybkim tempie. Szacuje się, że banki liczą miliony euro strat poniesionych przez osoby, które robią podróbki, przechwytują numery kart kredytowych lub inne osoby, które dokonują zakupów online przy użyciu numerów kart znalezionych na przykład przez phishing lub wyprodukowanych za pomocą analogicznych algorytmów komputerowych.

Przypadek dziewiąty. Przestępca reklamuje dostępność określonego produktu w bardzo atrakcyjnej cenie, prosząc o niewielki procent zamówienia za pomocą karty kredytowej - z góry, a resztę należy zapłacić po otrzymaniu produktu. Wielu się na to zgadza, podając wszystkie dane swojej karty, aby zapłacić za niską „zaliczkę". Na podstawie tych informacji przestępcy dokonują nieuczciwych zakupów, a następnie sprzedają je za gotówkę.

Pokoje czatowe

Współczesny styl życia nie pozwala rodzicom poświęcać niezbędnego czasu na nadzór i prowadzenie dzieci, co prowadzi do stopniowego braku komunikacji. Ze swojej strony dzieci uwielbiają wysyłać i odbierać wiadomości oraz korzystać z czatów. W pokojach czatowych dzieci szukają ciepła, towarzystwa i wygody, których nie znajdują w rodzinie. Jednak nie ma czatu bez drapieżnika, który

będzie próbował wykorzystać niewinność młodzieży. Niestety, drapieżniki, udając nastolatków, korzystają z czatów, serwisów społecznościowych i innych witryn komunikacji online, aby przyciągać i wykorzystywać dzieci. Zaskakujące jest to, że drapieżnikami są zwykle ludzie podejrzani, społecznie szanowani, wykształceni - naukowcy, nauczyciele, przedsiębiorcy i tak często wybitni, zamożni ekonomicznie i zwykle mający własną rodzinę. Takie osoby rozpoczynają rozmowy z potencjalnymi ofiarami dzieci w celu nawiązania przyjaznego związku i uzyskania jak największej ilości informacji o ich życiu osobistym - miejscu zamieszkania, zainteresowaniach, hobby itp. Dyskusje mogą trwać kilka dni, tygodni, a nawet miesięcy, do drapieżnik zyskuje zaufanie dziecka. Następnie drapieżnik powoli angażuje się w rozmowy w nadziei, że doprowadzą do znęcania się nad dzieckiem-ofiarą.

Trendy w cyberprzestępczości

Cybernękanie

Są to działania, które mają miejsce przez Internet i mają na celu zastraszenie i poniżenie osoby od jednej lub więcej osób. Cybernękanie zwykle występuje wśród nieletnich, odbywa się za pośrednictwem wszystkich nowoczesnych mediów komunikacji internetowej - e-maili, mediów społecznościowych, czatu, wiadomości błyskawiczne itp. Zasadniczo jest to mutacja tradycyjnego szykanowania. Niestety, wersja cybernetyczna przeżywa ostatnio światowy wzrost, a incydenty mają miejsce głównie w środowiskach szkolnych. Cybernękanie może przybierać różne formy, z których większość jest następująca:

• Wysyłanie SMS-ów, wiadomości e-mail lub komunikatorów internetowych z obraźliwymi treściami (w komunikatorach internetowych lub na czatach)

• Złośliwe publikowanie zdjęć w serwisach społecznościowych, blogach lub innych witrynach wyłącznie w celu nękania

• Rozpowszechnianie plotek i fałszywych faktów w celu

zniesławianie osób trzecich w mediach społecznościowych, blogach, witrynach internetowych itp.

• Anonimowe zastraszające rozmowy i wiadomości.

Cybernękanie nie powinno być postrzegane jako niewinny żart dzieci, ale jako poważny negatywny wpływ na życie dziecka. Takie konsekwencje, które powinny ostrzec rodziców i nauczycieli obejmują

• Nieobecność w szkole

• Nagły spadek wyników w nauce

• Wykonanie czynu niezgodnego z poprzednim zachowaniem

• Zaangażowanie w działania niezgodne z prawem

• Chęć dziecka do zmiany własnego imienia

• depresja psychiczna

• Myśli lub próby samobójcze.

Przypadek dziesiąty: w szkole podstawowej uczennica pierwszej klasy, A, była zastraszana przez kolegę z klasy, B, który groził opublikowaniem w Internecie nagiego zdjęcia ucznia A. Poważnie wpłynęło to na wyniki akademickie ofiary, przyciągając uwagę władz szkolnych, które zbadały incydent i odpowiednio ukarały ucznia B.

Badanie przeprowadzone przez organizację non-profit N.EO.I na próbie 422 dzieci w wieku 13–18 lat (275 chłopców i 147 dziewcząt) wykazało, że:

• 16% chłopców i 22% dziewcząt w wieku 13–18 lat twierdziło, że padło ofiarą cybernękania.

• 32% twierdziło, że zastraszyło ich publikacja osobistych zdjęć w Internecie.

• 10% chłopców odpowiedziało pozytywnie na pytanie, czy byli zastraszani przez kolegę z klasy, przyjaciela lub znajomego za pośrednictwem Internetu lub innych nowych technologii.

• 42% odpowiedziało, że wie lub słyszało o kimś, kto padł ofiarą prześladowania przez Internet i / lub nowe technologie.

Chociaż powyższe statystyki odzwierciedlają środowisko młodzieżowe Grecji, gdzie te dane były dostępne, światowa rzeczywistość jest znacznie gorsza.

Samobójstwa i zaginięcia

Ogólny niepokój związany z rolą Internetu w życiu jego użytkowników wynika z przypadków samobójczych, w których Internet działał jako czynnik. Typowe przypadki to samobójstwa związane z uzależnieniami od hazardu online.

Przypadek jedenasty: W Grecji znaleziono 18-letniego studenta martwego obok jego komputer, gdy komputer był online na czacie. Na ekranie w e-mailu znajdował się przepis na śmierć od osoby o imieniu żeńskim, który zawierał szczegółowe instrukcje na temat tego, jakiego leku użyć, aby zakończyć życie.

Na szczęście istnieje całodobowy internetowy czat służący zapobieganiu samobójstwom, który w ostatnich latach najwyraźniej zapobiegł ponad tysiącowi możliwych samobójstw. Warto wspomnieć, że dzięki Internetowi i pozostawionym śladom rozwiązano liczne przypadki zniknięć.

Wniosek

W ostatnich dziesięcioleciach technologia poczyniła duże postępy, wprowadzając nowe urządzenia, nowe techniki i nowe funkcje. Do tej pory komputery i Internet stały się integralną częścią naszego codziennego życia, ulepszyły nasze życie w nieskończony sposób i sprawiły, że nasze działania były znacznie szybsze i łatwiejsze. To samo dotyczy działań przestępczych - stały się one znacznie szybsze i łatwiejsze. Ponieważ Internet stał się cenną i niezbędną częścią naszego codziennego życia, błędem byłoby demonizowanie go pod pretekstem, że ułatwia on działania przestępcze. Dzięki szkoleniom uświadamiającym w zakresie cyberbezpieczeństwa możemy chronić się przed pułapkami kryminalnymi i być dodatkowymi podejrzliwy wobec wspaniałych ofert. Faktem jest, że uniknęlibyśmy wielu hacków internetowych, gdybyśmy wiedzieli kilka podstawowych rzeczy na temat korzystania z nich. Na zakończenie nawigacja w zakresie bezpieczeństwa cybernetycznego jest jak nawigacja na otwartym morzu, gdzie wymagane są specjalistyczne umiejętności. Podobnie wszyscy musimy przeprowadzić pewną formę szkolenia w zakresie cyberbezpieczeństwa, aby mieć bezpieczną i przyjemną nawigację w sieci.