Sprawy dotyczące cyberprzestępczości

Fałszywe strony internetowe

Fałszywe strony internetowe stają się coraz bardziej wszechobecne i godne zaufania, generując miliardy dolarów w nieuczciwych przychodach kosztem niczego niepodejrzewających użytkowników Internetu. Abbasi i inni stwierdzili, że wzrost dochodowych fałszywych stron internetowych można przypisać kilku czynnikom, w tym ich autentycznemu wyglądowi, braku świadomości użytkowników na ich temat oraz zdolności oszustów do podważania wielu istniejących mechanizmów ochrony przed nimi. Projekt i wygląd tych stron utrudnia użytkownikom ręczną identyfikację ich jako fałszywych. Można dokonać rozróżnienia między fałszywymi witrynami a wymyślonymi witrynami. Fałszywa witryna to imitacja istniejącej komercyjnej witryny internetowej, takiej jak eBay czy PayPal. Wymyślona witryna to zwodnicza witryna, która próbuje stworzyć wrażenie legalnego, unikalnego i godnego zaufania podmiotu. Wykrywanie fałszywych stron internetowych jest trudne. Potrzebne są zarówno wskazówki dotyczące oszustw, jak i wiedza dotycząca konkretnego problemu. Wskazówki dotyczące oszustw są ważnymi elementami projektu fałszywych stron internetowych, które mogą służyć jako wskaźniki ich braku autentyczności. Po pierwsze, fałszywe strony internetowe często wykorzystują techniki automatycznego generowania treści do masowej produkcji fałszywych stron internetowych. Następnie sygnały oszustwa obejmują informacje, nawigację i projekt graficzny. Informacje w postaci tekstu na stronie internetowej często zawierają oznaki oszustwa wynikające z elementów projektu informacji. Nawigacja pod względem informacji o linkach i nazwach adresów URL witryny internetowej może dostarczyć odpowiednich wskazówek dotyczących oszustw związanych z cechami projektu nawigacji. Na przykład twierdzi się, że 70 procent stron w domenie „.biz" to fałszywe witryny. Fałszywe strony internetowe często wykorzystują obrazy z istniejących legalnych lub wcześniejszych fałszywych stron internetowych. Na przykład fałszywe witryny kopiują logo firmy z witryn, które naśladują. Fakt, że jest kopiowany, można wykryć w systemie . Oprócz wskazówek dotyczących oszustw potrzebna jest wiedza na temat konkretnego problemu. Specyficzna wiedza problemowa dotycząca unikalnych właściwości fałszywych stron internetowych obejmuje podobieństwa stylistyczne i powielanie treści Abbasi i inni opracowali prototypowy system wykrywania fałszywych stron internetowych. System oparty jest na statystycznej teorii uczenia się. Statystyczna teoria uczenia się to teoria uczenia się obliczeniowego, która próbuje wyjaśnić proces uczenia się ze statystycznego punktu widzenia. Naukowcy przeprowadzili serię eksperymentów, porównując prototypowy system z kilkoma istniejącymi systemami wykrywania fałszywych witryn na próbie testowej obejmującej 900 witryn. Wyniki wskazują, że systemy oparte na teorii statystycznego uczenia się mogą dokładniej wykrywać różne kategorie fałszywych stron internetowych, wykorzystując bogatsze zestawy wskazówek dotyczących oszustw w połączeniu z wiedzą dotyczącą konkretnego problemu. Odmianą fałszywych stron internetowych są fałszywe wiadomości e-mail, w przypadku których nadawca wiadomości e-mail twierdzi, że stowarzyszenie ze znanymi i renomowanymi korporacjami lub jednostkami organizacyjnymi. Na przykład jeden e-mail od „Microsoft/AOL Award Team" powiadomił zwycięzców o loterii, stwierdzając: „Prestiżowe firmy Microsoft i AOL zorganizowały i pomyślnie zorganizowały loterię z okazji końca roku, w którym wprowadziliśmy ponad 100 000 000,00 z okazji naszej noworocznej losowania rocznicowego". E-mail zaczął prosić o dane osobowe potencjalnej ofiary. Nhan i inni zbadali 476 oszukańczych ofert e-mailowych i stwierdzili, że trzema najczęściej domniemanymi stowarzyszeniami organizacyjnymi były Microsoft, America Online i PayPal. Oszuści próbują również zbudować zaufanie poprzez kontakty z korporacjami finansowymi emitującymi kredyty oraz autorytatywnymi organizacjami i grupami.

Pranie pieniędzy

Pranie brudnych pieniędzy jest ważną działalnością w większości działalności przestępczej. Pranie pieniędzy oznacza zabezpieczenie dochodów z przestępstwa. Dochody muszą zostać włączone do gospodarki prawnej, zanim sprawcy będą mogli je wykorzystać. Celem prania jest sprawienie, by dochody zostały nabyte legalnie, a także ukrycie ich nielegalnego pochodzenia. Pranie pieniędzy ma miejsce w ramach wszystkich rodzajów przestępstw motywowanych zyskiem, takich jak defraudacja, oszustwo, przywłaszczenie, korupcja, rabunek, dystrybucja środków odurzających i handel ludźmi Pranie brudnych pieniędzy często charakteryzuje się jako trzyetapowy proces, który wymaga (1) przeniesienia środków pochodzących z bezpośredniego związku z przestępstwem, (2) zamaskowanie tropu w celu udaremnienia pościgu oraz (3) ponowne udostępnienie ich przestępcy z ukryciem ich zawodowego i geograficznego pochodzenia. Pierwszy etap jest najbardziej ryzykowny dla przestępców, ponieważ pieniądze pochodzące z przestępstwa są wprowadzane do systemu finansowego. Etap 1 jest często nazywany etapem umieszczania. Etap 2 jest często nazywany etapem nakładania warstw, w którym pieniądze są przenoszone w celu ukrycia lub usunięcia bezpośrednich powiązań z popełnionym przestępstwem. Pieniądze mogą być przekazywane za pośrednictwem kilku transakcji, które mogą obejmować wiele kont, instytucji finansowych, firm i funduszy, a także korzystać z usług profesjonalistów, takich jak prawnicy, brokerzy i konsultanci jako pośrednicy. Etap 3 jest często nazywany etapem integracji, w którym stworzono uzasadnioną podstawę do powstania aktywów. Pieniądze są udostępniane przestępcy i mogą być swobodnie wykorzystywane do konsumpcji prywatnej, zakupów luksusowych, inwestycji w nieruchomości lub inwestycji w legalne firmy. Pranie pieniędzy zostało również opisane jako proces pięcioetapowy: umieszczanie, nakładanie warstw, integracja, uzasadnianie i osadzanie. Sugerowano również, że pranie pieniędzy nie należy do kategorii przestępstw finansowych. Ponieważ pranie pieniędzy może wykorzystywać ten sam system finansowy, który jest wykorzystywany do popełniania najpoważniejszych przestępstw finansowych, oczywiste jest, że pokrywa się on z tym ostatnim. Według Joyce'a, pieniądze pochodzące z przestępstwa są często usuwane z kraju, w którym doszło do przestępstwa, są przekazywane przez międzynarodowy system płatniczy w celu zatarcia wszelkich śladów audytu. Trzeci etap prania pieniędzy odbywa się na różne sposoby. Na przykład karta kredytowa może być wydana przez banki zagraniczne, „wygrane" w kasynie mogą zostać wypłacone, mogą wystąpić zyski kapitałowe z obrotu opcjami i akcjami, a sprzedaż nieruchomości może przynieść zysk. Dochody z czynów karalnych mogą pochodzić z przestępczości zorganizowanej, takiej jak handel narkotykami, przemyt ludzi, handel ludźmi, dochody z rabunków lub pieniądze uzyskane w wyniku defraudacji, uchylania się od płacenia podatków, oszustwa, nadużywania struktur firmy, wykorzystywania informacji poufnych lub korupcji. Jednostka analityki finansowej w Norwegii twierdzi, że większość czynów przestępczych jest motywowana zyskiem. Gdy przestępstwo generuje znaczne dochody, sprawcy muszą znaleźć sposób na kontrolowanie majątku bez zwracania na siebie uwagi lub popełnionego przestępstwa. Tak więc proces prania pieniędzy jest decydujący, aby cieszyć się dochodami bez wzbudzania podejrzeń. Dochody z przestępstw trafiają do różnych sektorów gospodarki. Badanie przeprowadzone w Kanadzie wskazuje, że instytucje depozytowe są największym odbiorcą, ponieważ zostały zidentyfikowane w 114 ze 149 spraw dotyczących dochodów z przestępstwa (POC). Podczas gdy sektor ubezpieczeniowy był zamieszany w prawie 65 procent wszystkich przypadków, w zdecydowanej większości sprawca nie szukał wyraźnie sektora ubezpieczeniowego jako narzędzia do prania. Zamiast tego, ponieważ pojazdy silnikowe, domy, firmy i statki morskie były kupowane za dochody z przestępstwa, często konieczne było wykupienie ubezpieczenia tych aktywów. Kiedy banki są zamieszane w pranie pieniędzy, przestępstwa komputerowe są popełniane w zakresie transakcji finansowych. Dochody z przestępstwa są deponowane w banku, a następnie przekazywane w taki sposób, że ślady są ukrywane, zanim pieniądze zostaną ponownie udostępnione przestępcy. Chociaż ujawnienie, że obsługuje on pieniądze pochodzące z przestępstwa, może zaszkodzić reputacji banku, jak zobaczymy w dalszej części tej książki, pieniądze pochodzące z przestępstwa mogą stanowić dobry interes dla banku

Oszustwo bankowe

Fisher opisuje przypadek oszustwa bankowego w USA. Dotyczył on Jeffreya Bretta Goodina z Azusa w Kalifornii, który został skazany na 70 miesięcy więzienia w wyniku swoich oszukańczych działań. Goodin wysłał do użytkowników America Online (AOL) tysiące e-maili, które wyglądały, jakby pochodziły z działu rozliczeniowego AOL, i zachęcały klientów do przesłania danych osobowych i danych karty kredytowej, których następnie używał do dokonywania nieautoryzowanych zakupów. Wiadomości e-mail odsyłały klientów AOL do jednej z kilku stron internetowych, na których ofiary mogły wprowadzić swoje dane osobowe i informacje kredytowe. Goodin kontrolował te strony internetowe, umożliwiając mu zbieranie informacji, które umożliwiły mu i innym dokonywanie nieautoryzowanych obciążeń na kartach kredytowych lub debetowych użytkowników AOL. Oszustwo bankowe to przestępstwo polegające na świadomej realizacji programu mającego na celu oszukanie instytucji finansowej. Na przykład w Chinach oczekuje się, że oszustwa bankowe będą rosły zarówno pod względem złożoności, jak i ilości, ponieważ przestępcy wciąż ulepszają swoje metody i techniki oszustw. Ze względu na silny nacisk w chińskim prawie karnym, surowe kary, w tym kara śmierci i dożywocie, są często stosowane w przypadku poważnych oszustw bankowych i korupcji. Cheng i Ma stwierdzili jednak, że surowość prawa nie przełożyła się na skuteczniejszą walkę z przestępcami. Niepewne prawo i niespójne praktyki egzekwowania prawa sprawiły, że przestępcy są bardziej fatalistyczni w tej sprawie, mając po prostu nadzieję, że nie będą pechowcami, którzy zostaną złapani. Oszustwa finansowe w sektorze bankowym to czyny przestępcze często powiązane z instrumentami finansowymi, ponieważ inwestorzy są oszukiwani w celu zainwestowania pieniędzy w instrument finansowy, o którym mówi się, że przynosi wysoki zysk. Inwestorzy tracą pieniądze, ponieważ w rzeczywistości nie ma inwestycji, instrumentu nie ma, inwestycja nie może przynieść obiecanego zysku lub jest to inwestycja o bardzo wysokim ryzyku, nieznana inwestorowi. Pieniądze są zwykle dzielone między osobę, która namówiła inwestora na transakcję, a różnych pośredników, którzy brali udział w transakcji. Picard stwierdził, że systemy informatyczne w bankach ułatwiają popełnianie oszustw, a jednocześnie komplikują dochodzenie. Dlatego istnieje atrakcyjna okazja do oszustwa związanego z niskim ryzykiem. To, co z kryminalnego punktu widzenia wygląda na szansę, stanowi nieodłączne ryzyko wewnątrz organizacji. Jedna kwestia dotycząca możliwości dotyczy wewnętrznych operacji banku. Oszustwo ma na celu operacje wewnętrzne i wykorzystuje wiele słabości lub pozwala uniknąć istniejących ograniczonych kontroli. Fisher twierdzi, że system z jednodniową odprawą czekową w Wielkiej Brytanii zwiększyłby narażenie na cyberprzestępczość. Przeprowadził analizę porównawczą systemów rozliczania czeków w Wielkiej Brytanii i USA, zbadał zwiększoną podatność na oszustwa powodowaną przez system rozliczania czeków jednodniowych i przeanalizował wynikające z tego trudności dowodowe napotykane podczas ścigania oszustw związanych z czekiem w USA. Wprowadzenie jednodniowych czeków w USA zapowiadało wzrost cyberprzestępczości oszustw bankowych i ograniczenie możliwości wnoszenia spraw do sądu przez prokuraturę z powodu braku dokumentów dowodowych.

Oszustwo związane z zaliczką

Jak wspomniano we wstępie, przestępczość finansowa związana z Nigerią jest szeroko rozpowszechniona, a 122 ze 138 krajów na spotkaniu Interpolu skarżyło się na udział Nigerii w oszustwach finansowych w ich krajach. Najbardziej znanym rodzajem ataków na pracowników biurowych na całym świecie jest tak zwane oszustwo z zaliczką. Nadawca będzie starał się zaangażować odbiorcę w plan zarabiania milionów dolarów, jeśli odbiorca zapłaci zaliczkę. Oszustwo można zdefiniować jako celowe wprowadzenie w błąd w celu osiągnięcia zysku. Jest to typowe przestępstwo finansowe, często popełniane przez przestępców umysłowych. Oszustwo istnieje od początku zapisanej historii. Charakter oszustw rozszerzył się wraz z wprowadzeniem komunikacji internetowej, handlu elektronicznego (e-commerce) i elektronicznego biznesu (e-biznes). Wiele dowodów wskazuje

na to, że mimo wysiłków organów ścigania coraz częściej dochodzi do oszustw opartych na technologii. Nigeryjscy przestępcy kontaktują się e-mailem z potencjalnymi ofiarami oszustwa polegającego na pobieraniu zaliczek bez wcześniejszego kontaktu. Adresy ofiar pozyskiwane są z książek telefonicznych i e-mailowych, dzienników biznesowych, magazynów i gazet. Typowy list o oszustwie z wyprzedzeniem opisuje potrzebę przeniesienia funduszy z Nigerii lub innego kraju Afryki Subsaharyjskiej, zwykle odzyskania funduszy kontraktowych, dostaw ropy naftowej lub spadku po zmarłych królach lub gubernatorach. Jest to zewnętrzny rodzaj oszustwa, w którym oszuści pobierający zaliczki próbują uzyskać przedpłaconą prowizję za porozumienie, które nigdy nie zostało faktycznie zrealizowane, lub za pracę, która nigdy nie została wykonana. Ofiary są często naiwne i chciwe, a w najgorszym razie przygotowane do podżegania do poważnych przestępstw kryminalnych, takich jak grabież publicznych pieniędzy z biednego państwa afrykańskiego. Oszustwo polegające na pobieraniu zaliczki istnieje od wieków, najsłynniejsze w postaci oszustwa z hiszpańskimi więźniami:

W tym przypadku z bogatym kupcem skontaktowałby się nieznajomy, który szukał pomocy w przemyceniu fikcyjnego członka rodziny z hiszpańskiego więzienia. W zamian za ufundowanie „ratunku" kupcowi obiecano nagrodę, która oczywiście nigdy się nie zmaterializowała.

Oszustwa związane z opłatami zaliczkowymi szybko rozwijają się w Internecie. Chang stwierdza, że tego rodzaju oszustwa są obecną epidemią, która przynosi setki milionów dolarów rocznie. Pojawienie się Internetu i rozpowszechnienie jego wykorzystania w ostatnich dziesięcioleciach sprawia, że jest on atrakcyjnym medium do informowania o oszustwach, umożliwiającym zasięg ogólnoświatowy. Oszuści pobierający zaliczki zwykle stosują określone metody, które wykorzystują ograniczoną racjonalność i automatyczne zachowanie ofiar. Metody obejmują zapewnianie autorytetu i władzy eksperckiej, odwoływanie się do szanowanych osób i organizacji, dostarczanie częściowego dowodu legalności, tworzenie pilności oraz sugerowanie niedostatku i przywilejów. Holt i Graves zbadali schematy stosowane w wiadomościach e-mail o oszustwach związanych z opłatami z góry. W ich badaniu zbadano mechanizmy stosowane przez oszustów poprzez analizę jakościową 412 fałszywych wiadomości e-mail. Ich odkrycia pokazują, że do generowania odpowiedzi i informacji od ofiar używa się wielu technik pisania. Połowa wiadomości wymagała również, aby odbiorca przekazał swoje dane osobowe nadawcy, umożliwiając w ten sposób również kradzież tożsamości. Odkrycia Holta i Gravesa sugerują, że oszuści wykorzystują zwodniczo proste wiadomości w celu identyfikacji i prześladowania osób. Oszuści wykorzystują unikalne frazy w każdym e-mailu, aby zwiększyć wiarygodność swoich wiadomości i prawdopodobieństwo odpowiedzi. Na przykład większość wiadomości ma kuszący wiersz tematu, który może zmusić daną osobę do otwarcia wiadomości e-mail. Częste wiersze tematu to „Uwaga pilna", „Przeczytaj i odpowiedz tak szybko, jak to możliwe", „Przyjaciół uwagi" i „Od dr Mariam Abacha". Powiadomienia o loterii zazwyczaj zawierają wyrażenia takie jak „Gratulacje" lub „Zwycięzca uwagi", podczas gdy wiadomości biznesowe używają wyrażeń takich jak „Potrzebny agent płatności". Treść wiadomości e-mail umożliwia oszustowi stworzenie fałszywego wrażenia profesjonalizmu poprzez podanie referencji biznesowych i oświadczeń o potrzebie zaufania i poufności. Oszuści mogą również zwiększyć wiarygodność swoich twierdzeń, wiążąc historię z bieżącymi wydarzeniami lub używając w wiadomościach zwrotów religijnych lub języka emocjonalnego. Oprócz zachowania poufności nadawcy proszą o jak najszybszy kontakt z nimi. Połowa e-maili zbadanych przez Holta i Gravesa prosiła odbiorcę o podanie nadawcy danych osobowych. Nhan i in. badał nieuczciwe namawianie do wiadomości e-mail. Przeanalizowali charakter nagabywania, charakter adwokata oraz informacje, o które proszono adresata. Ich badanie opierało się na dwóch kontach e-mail, które przechwyciły w sumie 476 niechcianych wiadomości e-mail zidentyfikowanych jako podejrzane w zamiarze w ciągu trzech miesięcy. Zdecydowana większość e-maili pochodziła z Wielkiej Brytanii (37%) Nigerii (33%). E-maile docierały również z Tajwanu, Rosji, Chin, Wybrzeża Kości Słoniowej i Francji. Wielu prawników podało się za urzędnika bankowego (29%), prawnika (27%) i polityka (17%). Aby

wzbudzić zaufanie docelowych ofiar, prawnicy zazwyczaj przygotowują i zawierają prezentację, która, jak się oczekuje, będzie odwoływać się do troski ofiary o innych. Dlatego wielu przestępców umieszcza w swoich e-mailach rzekome dane osobowe. Najczęściej adwokaci wskazywali, że są w związku małżeńskim (32%) lub chorują (23%). Inni zgłaszali, że byli ofiarą jakiegoś wydarzenia społecznego lub politycznego (15%), posiadali dzieci (12%), byli w jakiś sposób spokrewnieni z ofiarą tragicznego zdarzenia (10%) lub byli spadkobiercą (7%), który wkrótce zbierze dużą sumę pieniędzy, którymi rzekomo się podzielą.

Złośliwi agenci

Główna motywacja złośliwych agentów atakujących systemy informatyczne z biegiem czasu zmieniła się z dumy i prestiżu na korzyść finansową. Złośliwy agent to program komputerowy, który działa w imieniu potencjalnego intruza, aby pomóc w zaatakowaniu systemu lub sieci. Podczas gdy wirus komputerowy tradycyjnie był najwybitniejszym przedstawicielem gatunku złośliwych agentów, agenci szpiegujący stają się coraz bardziej powszechni. Agenci szpiegujący przekazują poufne informacje z organizacji do autora agenta. Innym rodzajem agenta są agenci zdalnie sterowani, którzy zapewniają atakującemu pełną kontrolę nad maszyną ofiary. Oprogramowanie jest klasyfikowane jako złośliwe oprogramowanie (złośliwe oprogramowanie) na podstawie postrzeganej intencji twórcy, a nie konkretnych funkcji. Złośliwe oprogramowanie dla zysku obejmuje oprogramowanie szpiegujące, botnety, rejestratory naciśnięć klawiszy i dialery. W botnecie złośliwe oprogramowanie loguje się do systemu czatu, podczas gdy keylogger przechwytuje naciśnięcia klawiszy użytkownika podczas wprowadzania hasła, numeru karty kredytowej lub innych informacji, które mogą zostać wykorzystane. Złośliwe oprogramowanie może zautomatyzować różne ataki na przestępców i jest częściowo odpowiedzialne za globalny wzrost cyberprzestępczości. Bossler i Holt zastosowali teorię rutynowych działań do badania złośliwych agentów. Zgodnie z teorią działań rutynowych, wiktymizacja drapieżna w kontakcie bezpośrednim występuje ze zbieżnością w przestrzeni i czasie trzech elementów: zmotywowanego sprawcy, braku zdolnego opiekuna i odpowiedniego celu. W przeciwieństwie do świata fizycznego, świat wirtualny często pomija czasy działalności przestępczej. Dlatego ważniejsze niż czasy takich działań są działania potencjalnych ofiar oraz strony internetowe lub pliki, z którymi się stykają.

Manipulacja robotem magazynowym

Program komputerowy był w stanie manipulować robotem giełdowym powiązanym z Giełdą Papierów Wartościowych w Oslo w Norwegii. Program generował fałszywe zlecenia kupna i sprzedaży, które kończyły się nawzajem, jednocześnie wpływając na ceny akcji. Następnie program wykonuje realne zlecenia kupna i sprzedaży, w których akcje były kupowane po niskich cenach i sprzedawane po wysokich cenach. Ten rodzaj manipulacji wartością akcji jest nielegalny w Norwegii, a w 2010 roku złapano dwóch maklerów giełdowych.

Kradzież tożsamości

Miri-Lavassani i inni odkryli, że oszustwa związane z tożsamością to najszybciej rozwijająca się przestępczość w białych kołnierzykach w wielu krajach, zwłaszcza w krajach rozwiniętych. W 2008 r. liczba ofiar oszustw związanych z tożsamością wzrosła o 22 procent do 9,9 miliona ofiar. Wywiad jest ważnym źródłem informacji do analizy przestępczości. Przykładem analizy przestępczości jest model pomiaru oszustw tożsamościowych opracowany przez Miri-Lavassani. Pięciowymiarowy model pomiarowy dotyczy: (i) rodzajów oszustw związanych z tożsamością, (ii) skutków oszustw związanych z tożsamością, (iii) metod oszustw związanych z tożsamością, (iv) oszustw dotyczących tożsamości międzynarodowej oraz (v) ryzyka oszustw związanych z tożsamością biznesową. Instytucje finansowe w Kanadzie zostały przebadane pod kątem gromadzenia danych empirycznych. Analiza czynnikowa

została zastosowana na danych do oceny wymiarów i zawartości każdego wymiaru w modelu, co dało czterowymiarowy, a nie pięciowymiarowy model pomiarowy, w którym metody oszustwa tożsamości obejmują oszustwa dotyczące tożsamości transnarodowej.

Rodzaje oszustw związanych z tożsamością odzwierciedlają sposób, w jaki złodzieje tożsamości wykorzystują skradzione lub sfałszowane tożsamości innych osób do popełniania czynów bezprawnych bez wiedzy ofiar. Rodzaje oszustw związanych z tożsamością można zmierzyć liczbą oszustw związanych z kartami kredytowymi; nieautoryzowane korzystanie z narzędzi lub usług; oszustwo ubezpieczeniowe; oszustwa inwestycyjne; oszukańcze pożyczki i kredyty hipoteczne; oszustwa bankowe; wnioski o nowe karty kredytowe i media (internet, telefon itp.), wystawione polisy ubezpieczeniowe, rachunki bankowe otwarte przez złodziei tożsamości; nadużywanie istniejących kart kredytowych, polis ubezpieczeniowych i rachunków bankowych przez złodziei tożsamości.

Wpływ oszustwa dotyczącego tożsamości można zmierzyć w kategoriach bezpośrednich kosztów oszustwa tożsamości dla firmy; bezpośrednie koszty oszustwa dla klientów; bezpośredni niefinansowy wpływ oszustwa na biznes (np. nadszarpnięcie reputacji); bezpośredni niefinansowy wpływ oszustw na klientów (takich jak uszkodzona dokumentacja kredytowa i historia dokumentacji); ilość czasu, jaką poszczególne ofiary oszustwa poświęcają na rozwiązywanie problemów; ilość czasu, jaki firma poświęca na rozwiązanie problemów związanych z oszustwami; emocjonalny i psychologiczny wpływ oszustwa na ofiary; oraz emocjonalny i psychologiczny wpływ oszustwa na rodziny ofiar.

Metody oszustwa tożsamości odnoszą się do metod, które zostały użyte przez złodziei tożsamości w celu uzyskania identyfikatorów ofiar oszustwa tożsamości. Metody obejmują główną kradzież; wypełnianie fałszywych zmian adresu; kradzież lub utrata portfela lub torebki; wyłudzanie informacji; vising; rejestry zatrudnienia; kradzież przez włamanie i wejście; kradzież przez Internet, wirusy komputerowe, oprogramowanie szpiegowskie i robaki; nagabywanie telefoniczne; wymuszenie lub sabotaż przez osobę z wewnątrz; oraz wymuszenie lub sabotaż przez osobę postronną. Metody transnarodowe obejmują pomiar przypadków oszustw związanych z tożsamością w kraju, podczas gdy złodzieje tożsamości znajdują się w innych krajach; oraz pomiar oszustw związanych z tożsamością na całym świecie pochodzących z Kanady.Ryzyko oszustwa związanego z tożsamością biznesową obejmuje samą firmę; pracownika organizacji; oraz inne organizacje i klienci współpracujący z organizacją. Badanie Miri-Lavassani i in. zaowocował modelem pomiaru, który obejmuje 27 wskaźników i cztery czynniki. Twierdzą, że przy braku szeroko rozwiniętego i stosowanego modelu pomiaru kradzieży tożsamości pojawiło się wiele nieporozumień na temat problemu oszustw związanych z tożsamością. Jednym z przykładów jest nieobiektywne przekonanie, że korzystanie z Internetu w biznesie elektronicznym zwiększa ryzyko narażenia na oszustwa związane z tożsamością.

Piractwo cyfrowe

Piractwo cyfrowe definiuje się jako nielegalne kopiowanie towarów cyfrowych, oprogramowania, dokumentów cyfrowych, cyfrowego dźwięku (w tym muzyki i głosu) oraz cyfrowego wideo z jakiegokolwiek innego powodu niż tworzenie kopii zapasowych bez wyraźnej zgody właściciela praw autorskich i rekompensaty dla niego. Internet sprzyja piractwu cyfrowemu, ponieważ sieć umożliwia popełnienie przestępstwa w oderwaniu od właściciela. Na przykład, piractwo w muzyce cyfrowej jest popełniane w wielu modus operandi. Kwestia piractwa cyfrowego stała się tematem ogromnego zaniepokojenia, do tego stopnia, że przyciągnęła uwagę ustawodawców, naukowców, a także biznesmenów . Higgins badał powiązania między niską samokontrolą, racjonalnym wyborem, wartością i piractwem cyfrowym. Jego wyniki pokazują, że niska samokontrola ma bezpośredni i pośredni wpływ na zamiary związane z piractwem cyfrowym. Co więcej, jego badanie pokazuje, że niska samokontrola ma pośrednie powiązania ze zmodyfikowaną wersją czynników sytuacyjnych,

takich jak wartość. Wyniki te wskazują, że teoria niskiej samokontroli i racjonalnego wyboru może być zgodnymi teoriami, które mogą wyjaśnić piractwo cyfrowe. Dla uznanej branży nagrań i dystrybucji muzyki pojawienie się Napstera, pierwszego peer-to-oprogramowanie sieci peer (P2P) było przełomowym wydarzeniem o znaczącym wpływie. Napster został stworzony w 1999 roku przez 18-letniego Shawna Fanninga jako aplikacja mająca na celu uproszczenie procesu wyszukiwania i udostępniania plików muzycznych online. Aplikacja umożliwiła bezpłatne powielanie i rozpowszechnianie wysoce skompresowanych plików muzycznych. Sieć Napster zyskała ogromną popularność i wygenerowała ogromny wybór muzyki do pobrania. Miliony użytkowników podłączonych do sieci w celu udostępniania i wymiany muzyki chronionej prawem autorskim bez wyraźnej zgody.W 2003 roku przemysł nagraniowy w USA wszczął szereg procesów sądowych przeciwko użytkownikom sieci P2P, aby powstrzymać ich przed nielegalnym udostępnianiem plików muzycznych. Pozew został również złożony przeciwko Napsterowi. Oskarżenia pod adresem Napster, Inc. opierały się na architekturze systemu. Napster korzystał z centralnie zlokalizowanych i należących do firmy serwerów do generowania i utrzymywania list podłączonych użytkowników oraz dostarczonych przez nich plików muzycznych.

Chociaż rzeczywiste transakcje plikami były przeprowadzane bezpośrednio między użytkownikami, te centralne serwery ułatwiały również połączenia między użytkownikami i inicjowały pobieranie plików muzycznych. Ze względu na scentralizowaną architekturę przemysł nagraniowy zdefiniował Napstera jako usługę z listami, która oferowała wyszukiwarkę, katalog, indeks i linki, a zatem była postrzegana jako ostatecznie odpowiedzialna za transakcje na plikach muzycznych i powodowane przez nie naruszenia praw autorskich.

W empirycznym badaniu piratów muzycznych online Bachmann odkrył, że udostępnianie plików i pobieranie muzyki należy analizować oddzielnie, badając wpływ egzekwowania praw autorskich na społeczności udostępniające pliki i osoby pobierające muzykę. Wyniki pokazują, że internauci w USA doskonale zdają sobie sprawę z tego, że ściganie prawne dotyczy jedynie udostępniania plików muzycznych. W innym badaniu dotyczącym piratów muzycznych online Higgins i in. odkryli, że trajektorie piractwa cyfrowego są powiązane z neutralizacją w kierunku piractwa cyfrowego. Neutralizacja obejmuje zaprzeczenie odpowiedzialności, zaprzeczenie zranienia, zaprzeczenie ofierze, potępienie skazańców i odwołanie się do większej lojalności. Wyniki ich badań wskazują, że wiele osób przejmie dewiacyjne zachowanie spod kontroli społecznej, aby pozwolić sobie na piracką muzykę bez rozwijania pirackiej tożsamości. Jednostki stosują różne formy neutralizacji w celach egoistycznych, odcinając się od przestępczości zachowania. Podczas gdy Higgins i in. badali neutralizację w odniesieniu do kontroli społecznej, Moore i McMullan badali neutralizację w bezpośrednim związku z piractwem cyfrowym. Okazało się, że wszyscy uczestnicy ich badania wskazali na poparcie, choć w różnym stopniu, technik neutralizacji. Jedną ze znalezionych technik neutralizacji było to, że wszyscy to robią. Jednak tylko szesnaście procent uczestników badania wskazało tę technikę, co zaskoczyło jednego z autorów badania, ponieważ spodziewali się, że więcej osób będzie kojarzyć się z tym przekonaniem.

Przestępstwa dotyczące własności intelektualnej

Przestępstwa przeciwko własności intelektualnej są poważnym problemem finansowym dla producentów samochodów, producentów dóbr luksusowych, firm medialnych i farmaceutycznych. Według Interpolu najbardziej niepokojące jest to, że podrabianie stanowi zagrożenie dla zdrowia publicznego, zwłaszcza w krajach rozwijających się, gdzie Światowa Organizacja Zdrowia szacuje, że ponad 60 procent farmaceutyków to towary podrabiane. Interpol uruchomił nową bazę danych na temat międzynarodowej przestępczości przeciwko własności intelektualnej, która została stworzona w celu wypełnienia luki w danych dotyczących konfiskat gromadzonych przez różne organy międzynarodowe i sektor prywatny. Spośród 1710 podmiotów znajdujących się w bazie, kontrole w

innych bazach danych Interpolu ujawniły powiązania z fałszowaniem kart kredytowych i walut, oszustwami, praniem pieniędzy, kradzieżą, brutalnymi przestępstwami oraz handlem ludźmi, bronią i narkotykami. Świadczy to o roli przestępczości zorganizowanej w podrabianiu i piractwu na dużą skalę. Rosnąca wartość własności intelektualnej w wytwarzaniu bogactwa została odzwierciedlona przez jej wzrost podatności na przestępczość. Snyder i Crescenzi stwierdzili, że przestępczość własności intelektualnej jest często powiązana z cyberprzestępczością, i zbadali ryzyko przestępczości nieodłącznie związane z kapitałem intelektualnym i rozproszoną cyberprzestępczością środowiska, aby wykazać, że tradycyjne środki prawne są w dużej mierze nieskuteczne w ochronie praw własności. W przeciwieństwie na przykład do gotówki lub obrazów, które wymagają od przestępcy wejścia do skarbca lub muzeum, a następnie zabrania skradzionych przedmiotów, przestępstwo przeciwko własności intelektualnej wymaga jedynie, aby przestępca wykonał kopię elektroniczną. Klasycznym środkiem zaradczym w przypadku kradzieży jest zwrot nieruchomości pierwotnemu właścicielowi. Dziś pobrane filmy i pliki muzyczne są tak samo przydatne, jak oryginały.

Hazard internetowy

Hazard internetowy to problem globalny, który ma wpływ na wszystkie kraje, niezależnie od ich lokalnych przepisów zakazujących lub zezwalających na uprawianie hazardu. Fidelie zadało pytanie, czy hazard internetowy jest niewinną działalnością, czy cyberprzestępczością. Znalazła bardzo niejasny status prawny hazardu internetowego. Hazard to branża, która w ciągu swojego istnienia przeszła wiele zmian. Hazard jest na ogół kontrolowany przez rządy stanowe w ramach wykonywania swoich uprawnień policyjnych. Jednak zasięg międzystanowy i międzynarodowy hazardu internetowego wymaga zarządzania przez prawo międzynarodowe. Pontell i inni zbadał przypadek Antigui dotyczący nielegalnego hazardu internetowego na morzu. Antigua to mała karaibska wyspa, która uzyskała niepodległość od Wielkiej Brytanii w 1981 roku. W 1997 roku uruchomiono internetowy serwis hazardowy o nazwie World Sports Enterprise (WSE) i znajduje się na wyspie. Klienci musieli przekazać 300 dolarów, zanim mogli grać, a GPW pobierała dziesięć procent od górnej części każdego zakładu. W pierwszych piętnastu miesiącach działalności firma pozyskała 3,5 miliona dolarów. Twierdzi się, że przestępczość zorganizowana przeniknęła do gier hazardowych w Antigua i że nieletni uczestnicy mogą grać. Ze względu na duże trudności w zakazie hazardu internetowego Fidelie zaleca rządom na całym świecie regulowanie i opodatkowanie internetowych przedsięwzięć biznesowych. Sugeruje, że ze względu na niejasny status prawny hazardu internetowego, musi istnieć ustawodawstwo wyraźnie określające, co jest, a co nie jest dozwolone, a także nacisk na regulacje rządów światowych i samoregulację przez internetowe firmy hazardowe.