**ZASADY KORZYSTANIA Z POCZTY I INTERNETU**

**WPROWADZANIE**

Internet oferuje każdemu przedsiębiorstwu ekscytujące możliwości znalezienia aktualnych informacji i dotarcia do potencjalnych klientów. Ta właśnie moc niesie ze sobą ryzyko zniszczenia reputacji firmowej i zawodowej. Problemy nietechniczne w cyberprzestrzeni to złe informacje, oszustwa, utrata produktywności, łamanie prawa cywilnego i karnego oraz łamanie przyjętych przez zwyczaj w cyberprzestrzeni konwencji prawidłowego zachowania. Ponadto powszechne nadużywanie dostępu do Internetu w pracy wymusza uznanie, że jasne zasady są niezbędne, aby pracownicy mogli właściwie korzystać z zasobów firmy. Konsensus w naszym zawodzie – pomimo strasznego braku twardych statystyk – jest taki, że około dwie trzecie wszystkich szkód wyrządzonych naszym systemom informacyjnym pochodzi od słabo wyszkolonych, nieostrożnych lub złośliwych osób z wewnątrz. Na przykład badanie opublikowane pod koniec 2005 r. wykazało, że, 69% ze 110 dyrektorów wyższego szczebla w firmach z listy Fortune 1000 twierdzi, że są „bardzo zaniepokojeni" atakami sieciowymi lub kradzieżą danych. mówią, że są tak zaniepokojeni, że nie mogą spać w nocy, powiedział eSecurityPlanet Sanjay Uppal, wiceprezes Caymas Systems. Badanie sponsorowane przez McAfee w Europie wykazało, że (według słów Departamentu Bezpieczeństwa Wewnętrznego Daily Open Source Infrastructure Report):

Pracownicy w całej Europie nadal narażają własne firmy na ryzyko ataków na bezpieczeństwo informacji. Według badania przeprowadzonego przez firmę McAfee zajmującą się bezpieczeństwem, to „zagrożenie od wewnątrz" podważa inwestycje, jakie organizacje podejmują w celu obrony przed zagrożeniami bezpieczeństwa. Ankieta przeprowadzona przez ICM Research dostarczyła dowodów zarówno ignorancji, jak i zaniedbań w korzystaniu z zasobów IT firmy. Jeden na pięciu pracowników pozwala rodzinie i przyjaciołom korzystać z firmowych laptopów i komputerów PC w celu uzyskania dostępu do Internetu. Ponad połowa podłącza własne urządzenia lub gadżety do służbowego komputera, a jedna czwarta robi to codziennie. Około 60 procent przyznaje, że przechowuje osobiste treści na swoim służbowym komputerze. Jeden na dziesięciu przyznał się do pobierania treści w pracy, których nie powinien. Większość zbłąkanych pracowników naraża swoje firmy na ryzyko przez samozadowolenie lub ignorancję, ale uważa się, że niewielka mniejszość aktywnie stara się zaszkodzić firmie od wewnątrz. Pięć procent ankietowanych twierdzi, że uzyskało dostęp do obszarów swojego systemu informatycznego, których nie powinni mieć, podczas gdy bardzo niewielka liczba przyznała się do kradzieży informacji z serwerów firmowych.

Innym tematem o coraz większym znaczeniu jest nasycenie maili wysyłanych przez pracowników o dobrych intencjach, którzy nie wiedzą, jak efektywnie korzystać z poczty elektronicznej. Na koniec, niektóre informacje zawarte w tym rozdziale mogą pomóc administratorom bezpieczeństwa zaangażować swoich użytkowników w bardziej aktywną rolę, przekazując im wiadomości, które pomogą im chronić własne rodziny i przyjaciół. Sprawienie, by pracownicy dbali o bezpieczeństwo swoich rodzin, to dobry krok do zaangażowania ich w bezpieczeństwo korporacyjne.

**NARUSZENIE REPUTACJI PRZEDSIĘBIORSTWA**

Gdy ktoś publikuje informacje w sieci, nagłówek wiadomości zwykle wskazuje, kto jest nadawcą. W szczególności wszyscy pracownicy korzystający z firmowego konta e-mail identyfikują swojego pracodawcę w każdym ogłoszeniu. Wynika z tego, że gdy pracownik - na przykład joe@acme.com - zachowuje się niewłaściwie w sieci, jest prawdopodobne, że każdy, kto je zobaczy, skojarzy je z pracodawcą, niezależnie od daremnych prób oddzielenia pracownika od pracodawcy za pomocą oświadczeń np. „Powyższe opinie niekoniecznie są opiniami mojego pracodawcy". Pracownicy mogą

zawstydzić swoich pracodawców, używając swoich firmowych identyfikatorów e-mail w następujący sposób:

* Płonący. Wyprowadzanie niegrzecznych ataków słownych na innych.

* Spamowanie. Wysyłanie wiadomości-śmieci (spamu), niechcianych reklam i promocji sprzedaży do wielu, często niepowiązanych grup Usenet i list mailingowych oraz na adresy e-mail osób bez ich zgody.

* Bombardowanie pocztą. Wysyłanie wielu wiadomości e-mail na jeden adres e-mail w celu zdenerwowania użytkownika lub w skrajnych przypadkach, aby spowodować odmowę usługi.

Ponadto pracownicy mogą łamać prawo, wysyłać zawstydzające treści pocztą elektroniczną, wplątać pracodawców w sprawy osobiste i rozpowszechniać nieprawdę z możliwymi konsekwencjami.

**Naruszenie prawa**

Pracownicy mogą angażować się w nielegalne działania, które mogą poważnie zagrozić ich pracodawcy; przykłady zawierają:

* Szpiegostwo przemysłowe

* Manipulacja zapasami

* Kryminalne hakowanie, nieuprawniona penetracja innych systemów

* Sabotaż, ataki typu „odmowa usługi”

* Wandalizm, niszczenie stron internetowych

* Tworzenie, przesyłanie lub przechowywanie pornografii dziecięcej

* Wysyłanie gróźb (np. wyrządzenia krzywdy prezydentowi Stanów Zjednoczonych)

* Oszustwa związane z kartami kredytowymi, używanie skradzionych lub nieuczciwie wygenerowanych numerów kart kredytowych do zakupów dokonywanych przy użyciu zasobów firmy

Korporacyjne zasady korzystania z Internetu powinny wyraźnie zabraniać wykonywania jakichkolwiek z tych działań.

**III – Polecana poczta e-mail**

W ostatnich latach było zbyt wiele przypadków nierozsądnego korzystania z poczty e-mail. Pracownicy stworzyli nieprzyjazne środowisko pracy, wysyłając wewnętrzne wiadomości e-mail z lubieżnymi lub nienawistnymi żartami i obrazami; członkowie personelu obrażali swoich szefów lub pracowników w wiadomościach e-mail, które później stały się publiczne; ludzie wysuwają oszczercze oskarżenia pod adresem innych pracowników lub konkurencyjnych firm. Wszystkie te zastosowania są całkowicie nieodpowiednie dla medium, które przejmuje kontrolę nad dystrybucją z dala od twórców i tworzy zapisy, które mogą być archiwizowane i archiwizowane przez nieokreślony czas możliwego wyszukiwania. Zdrowy rozsądek podpowiada, że wszystko, co zostanie wysłane pocztą elektroniczną, nie powinno być nielegalne ani nawet krępujące, jeśli zostało opublikowane w gazecie. Użytkownicy powinni również mieć świadomość, że obrażanie ludzi za pomocą poczty elektronicznej jest kiepskim pomysłem. Wysyłanie płomieni, które umniejszają, wyśmiewają i poniżają innych ludzi, prawdopodobnie wywoła więcej tego samego w odpowiedzi, a podpalanie jest brzydką praktyką, która zniekształca standardy dyskursu publicznego i prywatnego. Jeśli użytkownik lub pracownik zdecyduje się odpowiedzieć na niegrzeczną lub poniżającą wiadomość e-mail, powinien powstrzymać się od odpowiadania tym samym niegrzecznym lub poniżającym tonem. W jednym przypadku zgłoszonym na

zajęciach z zarządzania bezpieczeństwem autorowi Kabay w 2013 r., pracownik zauważył, że młody stażysta odpowiedział na memorandum e-mail, naciskając ODPOWIEDZ WSZYSTKO i wysyłając pogardliwą, arogancką, poniżającą i niegramatyczną krytykę wiadomości. Wiadomość ta została wysłana do wszystkich pracowników przez prezesa. Tego dnia stażystę wyrzucono. Pracownicy powinni pracować nad utrzymaniem wyżyn moralnych, powstrzymując się od nieprzyzwoitości, wulgaryzmów i wulgaryzmów zarówno w dyskursie pisemnym, jak i ustnym. Jest to nie tylko ogólnie dobry nawyk, ale także pozwala uniknąć rozwścieczenia zupełnie obcych ludzi, którzy mogą być niebezpieczni fizycznie lub elektronicznie. Te najlepsze praktyki dotyczą również życia domowego i rodzinnego. Hakerzy kryminalni są znani z tego, że niszczą ratingi kredytowe, uczestniczą w kradzieży tożsamości, aby gromadzić duże rachunki na nazwiska ofiar, a nawet manipulują kontami firm telekomunikacyjnych. W jednym znanym dowcipie hakerzy przekierowali wszystkie przychodzące połączenia telefoniczne do słynnego eksperta ds. bezpieczeństwa Donna Parkera, który jest dość łysy, do firmy zajmującej się regeneracją włosów. Anonimizatory to usługi, które usuwają informacje identyfikujące z wiadomości e-mail, a następnie przesyłają tekst do wskazanych celów. Jednak nawet anonimizatorzy odpowiadają na wezwania do sądu, żądając tożsamości osób zamieszanych w zniesławienie lub groźby. Witryna o nazwie annoy.com stale publikuje wiadomości, które mogą irytować znaczną liczbę osób w związku z korzystaniem z praw wynikających z Pierwszej Poprawki Stanów Zjednoczonych; jednak nawet ta służba miała kiedyś szczególnie jasny przekaz dotyczący odmowy tolerowania nadużyć:

**OSTRZEŻENIE**

Zwróciliśmy uwagę, że niektórzy ludzie używają annoy.com do dostarczania czegoś, co niektórzy mogą uznać za groźby przemocy fizycznej lub krzywdzenia innych. Nie myl naszego zaangażowania na rzecz wolności słowa z licencją na nadużywanie naszych usług w ten sposób. Planujemy w pełni współpracować z organami ścigania we wszelkich staraniach, jakie podejmą, aby cię znaleźć i ukarać – nawet jeśli jest to jakaś zbuntowana autorytarna dyktatura… Wolność słowa i annoy.com nie dotyczą nękania i zdecydowanie nie dotyczą krzywdy ani przemocy. Jeśli pomyślisz przez chwilę, że pozwolimy tchórzliwym idiotom zepsuć naszą imprezę wolności słowa, popełniasz błąd. Ogromny błąd.

Zarówno dla USENETu, globalnego internetowego systemu dyskusyjnego, jak i dla grup dyskusyjnych w sieci, wiadomość może trwać wiecznie. Istnieją archiwa wiadomości USENET sięgające dziesięcioleci, a Wayback Machine (nazwany tak od wehikułu czasu prowadzonego przez pana Peabody [psa naukowego] w kreskówce telewizyjnej Hanna-Barbara's Rocky [latająca wiewiórka] i Bullwinkle [ujmujący łoś]. show of the 1960s) w sieci ma zapisy wstecz do 1996 roku. Wysyłanie obraźliwych lub poniżających wiadomości online może nie zaszkodzić trwale reputacji nadawcy, ale prawdopodobnie nie poprawi czyichkolwiek perspektyw na zdobycie lub utrzymanie dobrej pracy, zwłaszcza jeśli adres e-mail nadawcy adres zawiera przynależność do firmy.

**Niewłaściwe użycie identyfikatorów korporacyjnych**

Istnieje wiele kontrowersji dotyczących tego, czy polityka firmy powinna zakazywać identyfikatorów firmowych do użytku osobistego w Internecie. Nie ma powodu, aby publikować wiadomości na grupach dyskusyjnych w hierarchii .alt, a zwłaszcza na grupach zainteresowanych lub sympatyzujących z działalnością przestępczą. Jeśli pracownicy organizacji chcą uczestniczyć w ożywionych dyskusjach politycznych, rozmowach na temat aktywności seksualnej i wszelkich innych tematach niezwiązanych z ich pracą, mogą to zrobić, korzystając z własnych tożsamości internetowych. Pracodawcy płacą za firmowe tożsamości e-mail; ludzie, którzy chcą publikować opinie – zwłaszcza poglądy polityczne – na temat, powiedzmy, technik wyplatania koszyków, powinni zapłacić za własny dostęp i pozostawić swojego pracodawcę z dala od postów. Ryzyko zaszkodzenia reputacji organizacji poprzez naruszenie

netykiety jest wysokie. Niektórzy sprawcy sami byli maltretowani przez wściekłych i pozbawionych skrupułów internautów. W jednym znanym wczesnym przypadku, w 1994 r., naiwny dyrektor spamował „Net" – umieścił wiadomości w kilkudziesięciu grupach dyskusyjnych. W odwecie 800-numer jego firmy został opublikowany na telefonicznych grupach dyskusyjnych w hierarchii .alt, co spowodowało tysiące zirytowanych i kosztownych rozmów telefonicznych przez osoby poszukujące seksu słuchowego. Stali klienci nie mogli się dodzwonić, a część pracowników zrezygnowała z powodu obraźliwych telefonów. Dyrektor prawie stracił pracę. Dodatkowym ryzykiem jest to, że pracownicy niechcący opublikują poufne informacje firmy w grupie, którą błędnie postrzegają jako zamknięte, prywatne grupy. Konkurenci lub osoby sprawiające kłopoty mogą następnie wykorzystać te informacje w celu uzyskania przewagi konkurencyjnej lub opublikować je, aby zaszkodzić przedsiębiorstwu. Nawet jeśli grupa dyskusyjna lub korespondencja są naprawdę zamknięte, nic nie stoi na przeszkodzie, aby uczestnik mógł używać lub rozpowszechniać poufnych informacji bez pozwolenia. Do czasu wykrycia naruszenia bezpieczeństwa może być za późno na naprawę.

**Blogi, osobiste strony internetowe i serwisy społecznościowe**

Czy pracodawcy powinni być zaniepokojeni tworzeniem przez pracowników blogów, osobistych stron internetowych i stron społecznościowych? Zdarzały się przypadki, w których pracownicy wygłaszali niemądre lub szczerze obraźliwe komentarze na temat swoich obecnych pracodawców, z możliwymi do przewidzenia konsekwencjami. O wiele lepiej jest zapobiegać takim konfliktom, ustanawiając jasne zasady dla pracowników, które wyraźnie zabraniają wymieniania nazwy pracodawcy w publikacjach osobistych i mediach, takich jak blogi i strony internetowe. Odmiana może wymagać zatwierdzenia korporacyjnego przez działy public relations lub komunikacji przed opublikowaniem materiału. Takie zasady są powszechne w celu kontrolowania tego, co pracownicy publikują w wywiadach, biuletynach i innych publikacjach. Niektórzy pracownicy prawdopodobnie mają osobiste strony w serwisach społecznościowych, takich jak Facebook, Twitter i Tumblr. Te same problemy pojawiają się, gdy pracownicy odwołują się do swojego pracodawcy po imieniu w swoim profilu: Co czułby pracodawca, widząc nieprzyzwoicie ubrane zdjęcie na swojej stronie na Facebooku z profilem osoby wyświetlającym nazwę firmy? Umowy o pracę mogą i powinny określać ograniczenia w korzystaniu z tożsamości korporacyjnej. Nie ma nic złego w zastrzeganiu, że strony społecznościowe nie zawierają nazwy pracodawcy. Sprawę dodatkowo komplikuje rozwój profesjonalnych serwisów społecznościowych, takich jak LinkedIn. Witryny te zachęcają do publikowania cyfrowego CV, które zawiera podstawowe informacje o historii zatrudnienia danej osoby. Podobnie jak osobiste witryny sieciowe, firmy muszą określić jasne oczekiwania dotyczące użytkowania i okresowo monitorować zgodność poprzez wyszukiwanie i kontrolę wizualną. Jednak w przeciwieństwie do Facebooka, LinkedIn zwykle nie ma wielu użytkowników, którzy publikują nieprofesjonalne informacje i komentarze na swoich stronach.

**Rozpowszechnianie i wykorzystywanie nieprawidłowych informacji**

Internet, a w szczególności sieć World Wide Web, są pod pewnymi względami równie wielką zmianą w dystrybucji informacji, jak wynalezienie pisma 6000 lat temu i wynalezienie ruchomej czcionki 600 lat temu. We wszystkich tych przypadkach wynalazki obejmowały dezpośrednictwo: eliminację pośredników w przekazywaniu wiedzy. Pisanie wyeliminowało historyków ustnych; można było czytać informacje z daleka i dawno temu bez konieczności rozmowy z osobą, która osobiście tę wiedzę zapamiętała. Druk pozwalał na znacznie większą dystrybucję wiedzy niż ręcznie pisane księgi i zwoje, eliminując całą klasę skrybów, którzy kontrolowali dostęp do cennych i rzadkich zapisów. „Sieć i sieć kontynuują ten trend, z radykalnym wzrostem" w liczbie osób zdolnych do bycia wydawcami. Tam, gdzie kiedyś wydawanie wymagało pras drukarskich, kapitału i rozbudowanej infrastruktury administracyjnej, a przynajmniej stosunkowo drogich powielaczy (lata 50.), kserokopiarek (lata 60.) i drukarek (lata 70.), dziś jednostka może publikować materiały stosunkowo niedrogo, jeśli nie za darmo.

Wielu dostawców usług internetowych (ISP) oferuje bezpłatne usługi hostingowe i miejsca, w których ludzie mogą dołączać do elektronicznych społeczności wszelkiego rodzaju. Nawet jeśli osoba to robi , nie ma dostępu do Internetu w domu i postępują zgodnie z regulaminem pracy, bezpłatny dostęp można uzyskać w lokalnych bibliotekach lub w rosnącej liczbie bezpłatnych punktów dostępu do Internetu. Strony internetowe mogą prowadzić do widoczności niespotykanej nawet dekadę temu. Na przykład pewna młoda ekshibicjonistka, Jennifer Kaye Ringley, utworzyła stronę internetową, aby wyświetlić zdjęcia jej domu wykonane za pomocą kamer internetowych (kamer internetowych); ta strona „jennycam.org" otrzymywała do pół miliona odsłon dziennie, gdy działała. W połowie lat 90. inna młoda kobieta postanowiła założyć stronę internetową poświęconą jednej z jej ulubionych postaci literackich, NeroWolfe. W ciągu kilku lat jej witryna zyskała tak wielki szacunek, że została zatrudniona przez hollywoodzkiego filmowca jako konsultant techniczny przy serialu filmów NeroWolfe. Opłaty, które otrzymywała, mimo że oferowała pomoc za darmo, pomogły jej w zdobyciu doktoratu. studia z psychologii społecznej. Byłoby dla niej praktycznie niemożliwe osiągnięcie tego uznania, próbując publikować swój własny, drukowany magazyn dla fanów; gazeta mogła dotrzeć do kilkuset osób, ale strona internetowa dotarła do wielu tysięcy. Niestety, cała ta dezintermediat ma implikacje zarówno negatywne, jak i pozytywne. Wolność od wydawców wyzwoliła niezależnego myśliciela od wpływu korporacji, ograniczeń redakcyjnych i standardów stylu domowego. Jednak wolność ta wyzwoliła również wiele osób od odpowiedzialnego raportowania, odpowiednich badań, a nawet podstawowych zasad ortografii i gramatyki. Powiedzenie „Nie wierz we wszystko, co czytasz" jest jeszcze ważniejsze podczas czytania informacji internetowych. Osoby fizyczne mogą publikować nieprawidłowe wersje informacji technicznych (np. witryny zdrowia, które twierdzą, że masowanie części małżowiny usznej może wyleczyć wiele znanych chorób), nieuzasadnione teorie dotyczące wydarzeń historycznych i naturalnych (np. Uderzenie Tungska w 1908 zostało spowodowane przez meteoryt z antymaterii). i niekonwencjonalną historię rewizjonistyczną (np. niewolnictwo w Stanach Zjednoczonych było dobre dla Czarnych, a Hitler nigdy nie prześladował Żydów). Wikipedia, mimo że stała się pierwszą linią informacji dla niektórych użytkowników, cierpi z powodu możliwości czasowych lub nawet długotrwałych modyfikacji treści w celach żartów lub w innych celach. Na przykład uważa się, że zwolennicy nieudanej prawicowej kandydatki Sarah Palin próbowali zmienić wpis w Wikipedii na temat Paula Revere, aby zmusić go do dostosowania się do jej błędnych stwierdzeń na temat jego słynnej jazdy5. Ponieważ nie ma gwarancji, że treść odniesienie do Wikipedii jest uzasadnione lub będzie uzasadnione, a nawet takie samo przy następnym odwołaniu, instytucje akademickie mają tendencję do odrzucania odniesień do Wikipedii w pracach semestralnych.

**Oszustwa**

Dowcipnisie od lat używają e-maili do oszukiwania naiwnych ludzi, używając szczególnego rodzaju błędnych informacji: celowych oszustw. Oszustwo to złośliwa sztuczka oparta na zmyślonej historii. W Internecie krążą dwa główne rodzaje oszustw: miejskie mity i fałszywe informacje o wirusach. Archiwa mitów miejskich Strony internetowe są pełne zabawnych oszustw, z których część krąży od lat. Dlaczego nie wymierają? Problemem jest natura Internetu. Informacje nie są rozpowszechniane wyłącznie z centralnie kontrolowanej witryny; wręcz przeciwnie, każdy może nadawać lub retransmitować dowolny rodzaj danych w dowolnym momencie. W plikach nie ma wiarygodnych dat utworzenia ani obowiązkowych dat ważności, więc osoby, które otrzymują pięcioletni dokument, mogą nie mieć oczywistego sposobu rozpoznania jego wieku i prawie na pewno nie mają prostego sposobu na zidentyfikowanie przestarzałych lub niepoprawnych informacji. Widzą tylko, że dokument został im wysłany niedawno, często przez kogoś, kogo znają osobiście.

**Miejskie mity**

Oto kilka znanych przykładów dziwacznych, a czasem niepokojących mitów miejskich, które są dokładnie obalane na stronie Snopes.com:

* Drogie ciasteczka. Ktoś twierdzi, że pracownik Neiman-Marcus obciążył kartę kredytową kwotą 250 dolarów za przepis na dobre ciasteczka z kawałkami czekolady. Historia ta została sprowadzona do fałszywego roszczenia z 1948 roku, w którym sklep został oskarżony o pobieranie 25 dolarów za przepis na ciasto krówkowe.

* Nie zapalaj świateł samochodowych. W rytuale inicjacji gangów chuligani jadą autostradą z wyłączonymi światłami samochodów. Niewinni kierowcy, migający światłami jako przypomnienie, staliby się nowymi ofiarami, zwykle skutkując śmiercią przez gang.

* Uważaj na zatrute igły. Obłąkani, mściwi narkomani zostawiają igły zakończone krwią HIV+ w fotelach kinowych, rączkach pomp benzynowych i w miejscach powrotów wymiany telefonu.

*Pozbądź się nerek. Ofiara odwiedza obce miasto, pije z nieznajomymi i budzi się rano w lodowej wannie z dwoma zgrabnymi nacięciami, przez które usunięto obie nerki. Wydaje się, że nikt nigdy nie wyjaśnia, dlaczego przestępcy, którzy usuwają nerki, zawracają sobie głowę pakowaniem ofiary w lód.

* Biedny mały facet chce pocztówki. Craig Shegold jest tylko jednym z wielu prawdziwych lub wyimaginowanych dzieci, o których ludzie mający dobre intencje krążą łańcuszkami z prośbą o pocztówki, wizytówki, modlitwy, a nawet pieniądze. Shegold urodził się w 1980 roku; kiedy miał dziewięć lat, zdiagnozowano u niego raka mózgu, a przyjaciele rozpoczęli projekt, aby go pocieszyć – rozpowszechniali wiadomości z prośbą o wysłanie mu pocztówek, aby mógł zostać wpisany do Księgi Rekordów Guinnessa. Do 1991 roku otrzymał 30 milionów kart, a amerykański filantrop zaaranżował operację mózgu, która poskutkowała: Shegold przeszedł w stan remisji. Potop pocztówkowy nie. Do 1997 r. miejscowa poczta otrzymała dla niego ponad 250 milionów pocztówek i już dawno miał dość całego projektu.

* Chciałbym, żebyś przestała składać życzenie. Mniej więcej w połowie lat 90. jakiś dowcipniś umieścił fałszywe informacje o fundacji Make-a-Wish w przestarzałych łańcuszkach dotyczących Shegolda. Ta nieszczęsna organizacja została natychmiast zasypana e-mailami i pocztą, z których żadna nie była w żaden sposób przydatna ani istotna dla jej pracy. Musieli publikować zastrzeżenia na stronie internetowej, aby spróbować odciąć się od nieaktualnych informacji.

**Mity o wirusach**

Jedna kategoria oszustw stała się wiecznym problemem w sieci: mity o wirusach. Jest coś wspaniałego w chęci łatwowiernych ludzi o dobrych intencjach do przekazywania niedorzecznych wiadomości o nieistniejących wirusach o niemożliwych skutkach. Jednym z najbardziej znanych jest „wirus Good Times", który pojawił się około 1994 roku. Mit i liczne warianty krążą nieprzerwanie od lat. Co kilka lat następuje nowy wybuch, ponieważ niektórzy nowicjusze w Internecie napotykają starą kopię ostrzeżeń i wysyłają ją do wszystkich, których znają. Pierwotne bardzo krótkie ostrzeżenie brzmiało następująco, łącznie z nieprawidłową interpunkcją:

Oto kilka ważnych informacji. Uważaj na plik o nazwie Goodtimes. Szczęśliwej Chanuki wszystkim i bądźcie ostrożni. Na America Online jest wirus wysyłany pocztą e-mail. Jeśli otrzymasz coś, co nazywa się „Dobre czasy", NIE czytaj go ani nie pobieraj. Jest to wirus, który wymaże twój dysk twardy. Przekaż to wszystkim swoim znajomym. Może im to bardzo pomóc.

Wirus Good Times twierdził, że pobranie dokumentu lub przeczytanie dokumentu może spowodować szkody; w tamtym czasie takie roszczenie było niemożliwe. Jak na ironię, w ciągu kilku lat rzeczywiście

stało się możliwe wyrządzenie szkód za pośrednictwem dokumentów, ze względu na możliwości makrojęzyka programu Microsoft Word i innych programów obsługujących skrypty. Przez resztę lat 90. głupcy modyfikowali nazwę wyimaginowanego wirusa i dodawali więcej szczegółów, czasami twierdząc, że są niemożliwe skutki, takie jak zniszczenie sprzętu komputerowego. Do 1997 roku ostrzeżenia były tak absurdalne, że anonimowy autor rozpowszechniał następującą satyrę Monty Pythonesque:

Okazuje się, że ten tak zwany wirus oszustwa jest mimo wszystko bardzo niebezpieczny. Goodtimes ponownie zapisze Twój dysk twardy. Co więcej, zaszyfruje wszystkie dyski, które są nawet blisko twojego komputera. Ponownie skalibruje ustawienie chłodzenia lodówki, aby wszystkie lody się rozpuściły. Rozmagnesuje paski na wszystkich twoich kartach kredytowych, zepsuje śledzenie w telewizorze i użyje harmonicznych pól podprzestrzennych do zarysowania wszelkich płyt CD, które próbujesz odtworzyć. To da twojej byłej dziewczynie twój nowy numer telefonu. Wmiesza Kool-aid do twojego akwarium. Wypije całe twoje piwo i zostawi brudne skarpetki na stoliku do kawy, gdy przyjdzie towarzystwo. Umieści martwego kotka w tylnej kieszeni twoich dobrych spodni od garnituru i ukryje kluczyki do samochodu, gdy spóźnisz się do pracy. Goodtimes sprawi, że zakochasz się w pingwinu. Przyniesie ci koszmary o karłach cyrkowych. Wleje cukier do zbiornika paliwa i ogoli obie brwi podczas umawiania się z dziewczyną za plecami i obciążania karty Discover za kolację i pokój w hotelu. Uwiedzie twoją babcię. Nie ma znaczenia, czy ona nie żyje, taka jest moc Goodtimes, sięga poza grób, aby zbrukać to, co jest nam najdroższe. Przemieszcza Twój samochód losowo po parkingach, więc nie możesz go znaleźć. Kopie twojego psa. Pozostawi pożądliwe wiadomości na poczcie głosowej twojego szefa w twoim głosie! Jest podstępny i subtelny. To niebezpieczne i przerażające. To także dość ciekawy odcień fioletu. Goodtimes da ci holenderską chorobę wiązów. Pozostawi podniesioną deskę sedesową. Wyprodukuje porcję metamfetaminy w twojej wannie, a następnie pozostawi gotujący się bekon na kuchence, podczas gdy wyjdzie, by gonić uczniów w wieku szkolnym z twoją nową odśnieżarką.

Nieświadomi ludzie rozpowszechniają oszustwa wirusowe, ponieważ otrzymują oszustwo od kogoś, kogo znają. Niestety osobista przyjaźń z nadawcą nie gwarantuje prawdziwości jego wiadomości. Niektórzy strasznie mili ludzie są naiwnymi naiwniakami inżynierów społecznych, którzy mają dobre intencje. Przesyłanie informacji technicznych o wirusach (lub jakiekolwiek zauważone niebezpieczeństwo) bez sprawdzania, czy zasadność i dokładność informacji jest zła przysługą dla wszystkich. Utrudnia to ekspertom dotarcie do opinii publicznej z ostrzeżeniami o rzeczywistych zagrożeniach i zaśmieca skrzynki pocztowe odbiorców niepokojącymi informacjami o ograniczonym lub bezużytecznym charakterze. Naucz pracowników, rodzinę i znajomych, aby skonsultowali się ze snopes.com lub jego odpowiednikiem przed przesłaniem alarmujących wiadomości – i nie przesyłaj żadnych wiadomości o złośliwym oprogramowaniu: upewnij się, że wszyscy, których znasz, używają aktualnego oprogramowania chroniącego przed złośliwym oprogramowaniem.

**Wiadomości-śmieci**

Niezamawiana komercyjna poczta e-mail (UCE) jest szyderczo nazywana wiadomością-śmiecią, a także spamem. Wiadomości-śmieci są tworzone przez głupich (na początku) lub przestępczych (dzisiaj) ludzi, którzy wysyłają tysiące lub miliony identycznych wiadomości do niechętnych odbiorców. Wiadomości-śmieci zapychają kosze ofiar i marnują ich czas, otwierając niechciane wiadomości i poświęcając kilka sekund na uświadomienie sobie, że są to śmieci. Wiadomości-śmieci zawierające obrazy pornograficzne lub pornografię reklamową mogą być bardzo obraźliwe dla odbiorców. Śmieci mogą nawet przesuwać systemy poczty e-mail ludzi ponad limity ich serwerów, jeśli nie odbierają regularnie swoich wiadomości; w takich przypadkach poszukiwany e-mail może zostać odrzucony, ponieważ skrzynka pocztowa jest pełna. Dzisiaj wiadomości-śmieci są głównym wektorem ataków socjotechnicznych, takich jak phishing, którego celem jest nakłonienie odbiorców do naruszenia ich

prywatności lub kodów identyfikacyjnych i uwierzytelniających. (Więcej informacji na temat spamu, phishingu i innych sztuczek można znaleźć w rozdziale 20 tego podręcznika.) Większość wiadomości-śmieci wykorzystuje sfałszowane nagłówki; oznacza to, że nadawcy celowo umieszczają wprowadzające w błąd informacje w polach OD i ODPOWIEDŹ, aby uniknąć otrzymywania gniewnych odpowiedzi od ofiar ich przestępczego zachowania. Fałszowanie nagłówków wiadomości e-mail jest nielegalne w stanach Massachusetts, Wirginii i Waszyngtonie. W tych stanach zidentyfikowanie sprawców może prowadzić do spraw sądowych i kar finansowych za każdą wiadomość związaną z oszustwem. W jednym ze słynnych, przełomowych przypadków student Craig Nowak wysłał kilka tysięcy wiadomości-śmieci i postępował zgodnie z instrukcjami w swoim zestawie spamowym, umieszczając zmyślony adres ODPOWIEDZI za pomocą „@flowers.com" bez sprawdzania, czy rzeczywiście istnieje taką domenę. Rzeczywiście tak było, a właścicielka tej renomowanej usługi dostarczania kwiatów, Tracy LaQuey Parker, nie była zbyt zadowolona, gdy jej system został zalany ponad 5000 wiadomości o odesłaniu i gniewnych listach od klientów, którzy mówili, że nigdy więcej nie będą z nią robić interesów. Pozwała studentkę o odszkodowanie i otrzymała ponad 18 000 dolarów od sędziego, który powiedział, że żałuje, że nie mógł być jeszcze bardziej karny. Ogólnie rzecz biorąc, spam stał się mechanizmem nakłaniania nieświadomych dostawców do płacenia za iluzoryczne usługi marketingowe. To smutne, gdy do profesorów uniwersytetów w Ameryce Północnej wysyła się e-maile z reklamami chińskich rurociągów przemysłowych; ofiarami są ciężko pracujący chińscy przemysłowcy, którzy zostali oszukani przez zapewnienia przestępców obiecujących wysyłanie swoich reklam do chętnych i dobrze wykwalifikowanych odbiorców. Większość pozostałych śmieci wysyłana jest w nadziei, że niewielka część odbiorców błędnie napisanych, absurdalnych oświadczeń zostanie zmuszona do wysyłania pieniędzy – lub ich adresów e-mail – w celu wyrzucenia skrzynek. Więcej informacji na temat takich ataków socjotechnicznych można znaleźć w rozdziałach 19 i 20 tego podręcznika. Jeśli uczestniczysz w e-mailowej grupie dyskusyjnej, zwłaszcza w grupie niemoderowanej, dotyczącej określonego tematu, nie wysyłaj wiadomości e-mail do członków listy na temat, który wykracza poza obszar tematyczny. Typową klasą nieodpowiedniego publikowania jest apel o wsparcie wartościowej sprawy, która nie ma lub ma tylko wątły związek z tematem. Na przykład ktoś może zaapelować o wsparcie w ratowaniu wielorybów w grupie dyskusyjnej poświęconej ogrodnictwu: zły pomysł. Rozumowanie brzmi: „Oni lubią rośliny; prawdopodobnie wrażliwy na środowisko; prawdopodobnie zainteresowany konserwacją; dlatego chętnie usłyszą o wielorybach". Problem polega na tym, że takie rozumowanie można rozszerzyć na praktycznie każdy temat, zakłócając koncentrację grupy. Takie wiadomości często powodują gniewne riposty, które są zazwyczaj wysyłane przez naiwnych członków do całej listy, a nie tylko do nadawcy nieodpowiedniej poczty. Następnie gniewne riposty powodują dalsze gniewne reakcje na obciążenie listy bezużytecznymi wiadomościami i wkrótce grupa ogrodnicza pogrąża się w niezgodzie i zmarnowanym wysiłku, generując złe przeczucia i nieufność. Jak zasugerowano w poprzednim akapicie, jeśli zobaczysz nieodpowiednie wiadomości na liście e-mailowej, na której Ci zależy, nie odpowiadaj na całą listę; odpowiedz ładnie i tylko do nadawcy, ewentualnie z kopią dla moderatora, jeśli taki istnieje. Odpowiedź powinna być umiarkowana i uprzejma. Listy łańcuchowe i schematy Ponzi.

Szczególnie irytującą formą wiadomości-śmieci jest list łańcuszkowy. Niektóre łańcuszki zawierają śmieszne historie o strasznych chorobach i wypadkach, które przytrafiły się ludziom, którzy odmówili przekazania wiadomości (śmieszne na pierwszy rzut oka, ale najwyraźniej przemawiające do osób na tyle irracjonalnych, by utrzymać w obiegu nonsensy). Inni skupiają się na tym, aby ofiary wysyłały pieniądze komuś znajdującemu się na szczycie listy nazwisk, dodając swoje imiona na dole listy, zanim wyślą je do określonej liczby odbiorców. W zależności od długości listy i kwoty, którą należy wysłać osobie na górze, teoretyczny zwrot może wynosić setki tysięcy dolarów. W praktyce zyskują tylko pomysłodawcy programu. Po pewnym czasie wszyscy możliwi uczestnicy zostali zaproszeni z

rozczarowującymi wynikami, a kajdany w wielu miejscach zostały zerwane. Inny rodzaj piramidy znany jest jako schemat Ponzi, czyli oszustwo inwestycyjne, w którym obiecuje się wysokie zyski, a pierwsi inwestorzy spłacają środkami zebranymi od późniejszych. Oszustwo nosi imię Charlesa Ponziego (1882-1949), spekulanta, który zorganizował taki program w 1919 i 1920 roku. Program Ponziego oszukał tysiące ludzi w Bostonie, kiedy Ponzi zagwarantował 50-procentowy zysk ze składek w ciągu 45 dni i podwojenie wartość za 90 dni. Oszust twierdził, że wymienia 1-centowe hiszpańskie certyfikaty pocztowe na 6-centowe znaczki amerykańskie – twierdzenie to wyśmiewali wówczas analitycy finansowi. Niemniej jednak Ponzi zarobił około 15 milionów dolarów w 1920 dolarów i ukradł około 8 milionów dolarów, wypłacając resztę wczesnym uczestnikom w celu zwiększenia wiarygodności. Sześć banków upadło, ponieważ zainwestowały w ten program środki swoich deponentów. Ponzi ostatecznie odsiedział ponad trzy lata w więzieniu, ale uciekł w 1925 roku. Współczesny program Ponzi e-mail zazwyczaj zawiera pełne pasji zapewnienia od niejasno zidentyfikowanych osób o tym, jak sceptycznie podchodzili do tego programu, ale jak ulegli ciekawości, uczestniczyli w programie i zarobili ogromne kwoty pieniędzy (np. 50 000 USD) w ciągu kilku tygodni. Pisma często zawierają zapewnienia, że wszystko jest zgodne z prawem i wskazują na nieistniejące pocztowe linie informacyjne lub w różnych miejscach listu twierdzą, że „jak widziano w telewizji". Listy te instruują ofiarę, aby wysłała niewielką sumę pieniędzy (zazwyczaj 1 lub 2 dolary) na krótką listę około czterech osób, aby otrzymać „raporty". Ofiara jest następnie proszona o dodanie swojego nazwiska i adresu do listy, usuwając pierwszy przed wysłaniem kopii nowego listu do jak największej liczby osób. Niektóre listy przechodzą obliczenia oparte na takich założeniach, jak „Wyobraź sobie, że wysyłasz sto, tysiąc lub dziesięć tysięcy wiadomości i otrzymujesz zaledwie 1%, 2% lub 10% odpowiedzi", a następnie obiecujesz ogromne zwroty. W rzeczywistości „raporty" to nic innego jak jednostronicowe, bezsensowne notki o łańcuszkach. Oszuści próbują ominąć przepisy, takie jak list przewozowy U.S. Post Office przeciwko nieuczciwemu wykorzystaniu poczty. Oto dokładny tekst listu wysłanego 1 grudnia 2000 r. przez V.J. Bellingera z Grupy Wsparcia Operacyjnego Służby Inspekcji Pocztowej Stanów Zjednoczonych w Newark, New Jersey. Zawiera kilka interesujących informacji, które powinny być pomocne dla czytelników próbujących przekonać pracowników (lub rodzinę i przyjaciół), że takie łańcuszki e-mail zawierające adresy pocztowe są nielegalne.

List łańcuszkowy lub wielopoziomowy program marketingowy mogą być przedmiotem działań w ramach Statutu Loterii Pocztowej, Fałszywego Reprezentowania i/lub Oszustwa Pocztowego, jeśli zawierają trzy elementy: nagrodę, uwagę i szansę. Nagroda jest zwykle w formie pieniędzy, prowizji lub innej wartości, którą otrzymasz, zgodnie z nagabywaniem. Wynagrodzenie to wymagana wpłata na rzecz sponsora w celu uzyskania nagrody. O szansie decydują działania uczestników, nad którymi mailer nie ma kontroli. Tego typu schematy stanowią loterie, których nie można przesyłać pocztą elektroniczną, ponieważ naruszają one następujące przepisy: Tytuł 18, Kodeks Stanów Zjednoczonych, sekcje 1302 i 1341 oraz Tytuł 39, Kodeks Stanów Zjednoczonych, sekcja 3005. Próbując wyglądać legalnie, wiele listów łańcuszkowych lub wielopoziomowe mailingi marketingowe oferują za opłatą produkt lub „raport". Ponieważ jednak sukces programu zależy od liczby chętnych do udziału, wszystkie trzy elementy stanowiące naruszenie są nadal obecne. Promotor tego programu został poinformowany o potencjalnych naruszeniach i został poproszony o zaprzestanie tego rodzaju działalności wysyłkowej.…

Pozornie podobnym zjawiskiem jest marketing wielopoziomowy. W tym nieoszukańczym, legalnym systemie sprzedaży produktów i usług, ludzie są zachęcani do rekrutowania dystrybutorów spośród swoich przyjaciół i znajomych, ale nacisk kładzie się na wartość produktów. Nikt nie twierdzi, że bez pracy ktoś się wzbogaci, a na inwestycje nie ma popytu. Produkty mają ugruntowany rynek, a firma zarabia na sprzedaży, a nie na rekrutacji. Oto kilka praktycznych wskazówek dla pracowników i osób fizycznych:

* Nie uczestnicz w żadnym programie polegającym na przesyłaniu dużej liczby listów lub wiadomości e-mail do wszystkich znajomych lub nieznajomych.

* Rozróżnij oszustwa piramidowe i legalne systemy marketingu wielopoziomowego: te pierwsze kładą nacisk na rejestrowanie uczestników, podczas gdy te drugie podkreślają wartość produktów i usług.

* Nie bierz udziału w rzekomych systemach marketingu wielopoziomowego, jeśli wymagają one znacznych inwestycji.

* Jeśli jesteś zainteresowany wielopoziomowym działaniem marketingowym:

* Sprawdź właścicieli i funkcjonariuszy.

* Porozmawiaj z ludźmi, którzy kupili produkty, aby sprawdzić, czy są zadowoleni ze swoich zakupów.

* Skontaktuj się z lokalnym biurem Better Business Bureau, aby sprawdzić, czy były jakieś skargi.

* Nie wysyłaj pieniędzy do podejrzanych oszustw piramidowych.

* Współpracuj z kolegami, aby zademonstrować, w jaki sposób oszustwo piramidowe zabiera pieniądze rosnącej liczbie późniejszych ofiar i przekazuje je osobom, które wcześniej uczestniczyły w oszustwie. Podkreśl fakt, że oszustwo jest nielegalne, nawet jeśli perspektywa wczesnego uczestnictwa może wydawać się skuteczna.

**Schematy szybkiego wzbogacenia się**

Inne programy szybkiego wzbogacenia się w sieci wykorzystują myślenie życzeniowe ofiar, ich brak sceptycyzmu i zwykle brak zdrowego rozsądku. Pojawiły się twierdzenia, że możesz zarobić ćwierć miliona dolarów rocznie, pielęgnując pudle w swoim domu. Albo że możesz zostać milionerem, pracując cztery godziny tygodniowo, wysyłając materiały promocyjne produktów, których nawet nie musisz sprzedawać. Często niebezpieczni ludzie ogłaszają takie plany; na przykład niektóre ekstremistyczne grupy milicji żądają od ludzi setek dolarów, aby nauczyli się oszukiwać rząd, żądając zastawów na własności rządowej, a następnie zastawiając bezsensowne zastawy jako zabezpieczenie pożyczek. Inni przestępcy rozpowszechniają programy do generowania fałszywych numerów kart kredytowych i wykorzystywania ich do kradzieży towarów. W innych przypadkach przestępcy pobierają pieniądze, aby nauczyć ofiary, jak sfałszować ich złą historię kredytową, aby mogły uzyskać jeszcze bardziej oszukańczy kredyt, cały czas twierdząc, że ich metody przestępcze są w 100 procentach legalne. Z korporacyjnego punktu widzenia takie łańcuszki i schematy powodują marnotrawstwo przepustowości i stwarzają możliwość poważnego zakłopotania, gdy zasoby przedsiębiorstwa są wykorzystywane do rozpowszechniania bezsensownych materiałów. Jednak bezpieczeństwo korporacyjne może zyskać przychylność użytkowników, pomagając im uniknąć pułapek związanych z takimi oszustwami, nawet jeśli korzystają z własnych systemów komputerowych. Korzyści są szczególnie duże, gdy pomaga się pracownikom uczyć własne dzieci, jak unikać tego rodzaju kłopotów. Aby zilustrować kłopoty, w jakie mogą wpaść dzieci, stosując te techniki, rozważmy przypadek Drew Henry'ego Maddena. W 1996 roku ten 16-letni Australijczyk z Brisbane tuż po ukończeniu szkoły zaczął oszukiwać firmy przy użyciu skradzionych i sfałszowanych numerów kart kredytowych. Ukradł towary o wartości 18 000 dolarów, a w lutym 1997 roku przyznał się do 104 oszustw i został skazany na rok więzienia. Jednak śledczy odkryli dodatkowe oszustwo i okazało się, że ukradł dodatkowe 100 000 dolarów w towarach i usługach. W październiku 1997 roku przyznał się do kolejnych 294 zarzutów oszustwa i otrzymał dodatkowy wyrok w zawieszeniu. Jego obrońca za straty obwiniał słabe zabezpieczenia: „Madden zaczął od bardzo drobnych oszustw związanych z kartami kredytowymi, ale sytuacja zaczęła się niepokojąco eskalować, ponieważ zabezpieczenia były tak niewystarczające”.

Pomimo niezwykłego strumienia dochodów młodzieńca, jego matka wydawała się akceptować jego podróże po świecie i masowe zakupy losów na loterię bez komentarza. W pewnym momencie powiedziała dziennikarzom: „Gdybyśmy byli zamożną rodziną, byłby w prywatnej szkole, gdzie jego talenty mogłyby być odpowiednio ukierunkowane". Stosunkowo nowym rodzajem oszustwa w Internecie jest młyn dyplomowy. Organizacje te udają instytucje edukacyjne; w rzeczywistości jest to jedna lub więcej oszukańczych osób, które sprzedają fałszywe dyplomy rzekomo reprezentujące uznane stopnie naukowe, ale nie oszukują nikogo poza nabywcą. Chociaż zakłady dyplomowe nie są akredytowane, brak akredytacji nie oznacza automatycznie, że szkoła jest podmiotem oszukańczym.

**ZAGROŻENIA DLA LUDZI I SYSTEMÓW**

Na szczególną uwagę zasługuje jedna szczególna klasa wiadomości e-mail: groźby. E-maile z pogróżkami mogą być skierowane do osób, systemów, organizacji lub procesów, na których polegają te podmioty. Podobnie jak inne rodzaje nielegalnej działalności w Internecie, odpowiednia edukacja, świadomość i reagowanie mogą ograniczyć liczbę przyszłych ofiar.

**Groźby obrażeń fizycznych.**

Każdy, kto otrzymuje groźby pocztą elektroniczną, ma prawo, a być może obowiązek, poinformowania lokalnych organów ścigania. W dzisiejszym klimacie strachu i przemocy każde zagrożenie zasługuje na uwagę. Oprócz niepokoju, jaki mogą wywołać takie wiadomości, mogą one być sygnałami ostrzegawczymi poważnych problemów. Wczesne ostrzeżenie, które pozwala władzom na interwencję w celu rozładowania potencjalnie wybuchowej sytuacji, może stanowić w szczególności groźby przemocy w pracy, w szkole lub wobec jakiejkolwiek określonej grupy. Wysyłanie wiadomości e-mail z pogróżkami nie jest akceptowalnym żartem ani drobnym żartem, zwłaszcza jeśli groźba obejmuje przemoc. Niektórzy ludzie, wierząc, że mogą ukryć swoją prawdziwą tożsamość, niemądrze wysyłali groźby śmierci do Białego Domu; Ponieważ Secret Service jest prawnie zobowiązane do zbadania wszelkich gróźb pod adresem prezydenta i pierwszej rodziny, agenci pojawiają się w ciągu kilku godzin, aby przesłuchać złoczyńców. Na przykład młodzież z dziesiątej klasy w Profile High School w Bethlehem w stanie New Hampshire wysyłała groźby śmierci na stronę internetową Białego Domu ze swoich szkolnych komputerów. Wiadomości zostały namierzone przez Secret Service w ciągu kilku minut, dzieci zostały zawieszone w szkole i straciły przywileje korzystania z Internetu na następne dwa lata.

**Pedofile w Internecie**

Ta sekcja dotyczy przede wszystkim szkolenia użytkowników w zakresie ochrony ich dzieci. Pedofilię definiuje się jako podniecenie seksualne w odpowiedzi na kontakt z dziećmi przed okresem dojrzewania lub obrazy przedstawiające je. Niektórzy pedofile fałszywie przedstawiają się jako młodzi ludzie na czatach lub za pośrednictwem poczty elektronicznej i nakłaniają dzieci do nawiązania przyjaźni z rówieśnikami. W jednym głośnym przypadku Paul Brown Jr., 47-letni mężczyzna, w e-mailu do 12-letniej dziewczynki z New Jersey podał się za 15-letniego chłopca. Matka ofiary natknęła się na związek na odległość, gdy znalazła na swoim progu paczkę od córki do nieznanego mężczyzny; dziecko umieściło na nim niewłaściwą opłatę pocztową i poczta odesłała go. Otwierając paczkę, znalazła kasetę wideo, na której jej córka bawiła się nago przed kamerą rodziny. Zrozpaczona matka przeszukała pokój córki i znalazła parę męskich majtek w rozmiarze 44 w jednej z szuflad dziecięcego biurka. Brown został aresztowany w lutym 1997 roku. Policja znalazła korespondencję z co najmniej 10 innymi nastolatkami w całym kraju, dzięki której Brown przekonał swoje młode ofiary, niektóre w wieku zaledwie 12 lat, do wykonywania różnych czynności seksualnych przed kamerami i wysyłania mu zdjęć i kasety wideo. W czerwcu przyznał się do nakłaniania nieletniego do robienia pornografii. W sierpniu 1997 r., podczas rozprawy skazującej, jedna z jego licznych ofiar powiedziała sądowi, że doznała wyśmiewania i upokorzenia w wyniku uwięzienia i opuściła szkołę, aby uciec od traumy. Oskarżyła Browna o gwałt

emocjonalny. Przedstawiając zdumiewającą interpretację własnego zachowania, Brown powiedział na rozprawie skazującej: „To był po prostu zły osąd z mojej strony". Kierując się zdrowym rozsądkiem, sąd skazał go na pięć lat więzienia. W marcu 2000 roku Patrick Naughton, były dyrektor firmy internetowej INFOSEEK, przyznał się do przekroczenia granic stanu w celu popełnienia ustawowego gwałtu na dziecku. W sierpniu urzędnicy FBI powiedzieli, że Naughton udzielał pomocy w dochodzeniach organów ścigania w sprawie pedofilii w sieci. W zamian za jego współpracę prokuratorzy zażądali od sądu 5 lat w zawieszeniu (zamiast ewentualnych 15 lat więzienia), pomocy psychologicznej, grzywny w wysokości 20 tys. trzymać się z dala od czatów erotycznych online. Problem prześladowania pedofilów za pośrednictwem Internetu osiągnął wymiar międzynarodowy. W styczniu 1999 roku siły policyjne na całym świecie współpracowały w celu wyśledzenia i zamknięcia ogólnoświatowej siatki pedofilów handlujących dziecięcą pornografią za pośrednictwem sieci. Eksperci ds. bezpieczeństwa dzieci ostrzegli komisję Kongresu USA ds. ochrony dzieci w Internecie, że wraz ze spadkiem średniego wieku użytkowników sieci (dzieci w wieku od dwóch do siedmiu lat należą do najszybciej rosnących kohort użytkowników Internetu), dzieci są coraz bardziej narażone na ryzyko przez ich nieostrożne lub ignoranckie działania w Internecie.

**Wirusy i inny złośliwy kod**

Według stanu na rok 2008, WildList (www.wildlist.org) zgłasza ponad 2000 różnych form kodu złośliwego oprogramowania powszechnie krążącego w cyberprzestrzeni. Badacze oprogramowania antywirusowego zarejestrowali o wiele więcej typów, ale nie zaobserwowano, aby infekowały one znaczną liczbę komputerów użytkowników. Większość tych szkodliwych programów ogranicza się do laboratoriów antywirusowych i komputerów hobbystów wirusów — ludzi, którzy czerpią przyjemność z igrania z niebezpieczeństwem. Więcej informacji na temat wirusów i innego złośliwego oprogramowania można znaleźć w rozdziałach 16, 17, 18 i 41 tego podręcznika. Pracodawcy powinni mieć zasady wyraźnie zabraniające tworzenia, wymiany i przechowywania złośliwego oprogramowania w systemach korporacyjnych.

**Oprogramowanie szpiegujące i reklamowe**

W grudniu 1999 roku informatyk, badacz cyberprzestępczości i pisarz Richard Smith zainteresował się programem o nazwie zBubbles, który zainstalował w swoim systemie w celu usprawnienia zakupów online. Stworzony przez Alexę, spółkę zależną e-tailera Amazon.com, program dostarczał konkurencyjnych informacji o alternatywnych i możliwie tańszych źródłach poszczególnych produktów. Jednak Smith odkrył, że dzieje się coś więcej niż na pierwszy rzut oka. Smith monitorował własny ruch internetowy podczas korzystania z zBubbles za pomocą sniffera pakietów, narzędzia, które wyświetla szczegóły każdej informacji przesyłanej przez połączenie sieciowe. Odkrył, że zBubbles wysyła do Alexy ciągły strumień informacji o nim i jego zwyczajach związanych z surfowaniem, w tym jego adres domowy, tytuły płyt DVD, które przeglądał na Buy.com, oraz szczegóły biletu lotniczego, który zweryfikował online. Ponadto program regularnie wysyłał informacje na serwery Alexy, nawet gdy Smith nie korzystał z przeglądarki. Okazało się, że zBubbles nie był jedynym programem wysyłającym informacje z powrotem do swoich twórców. Dostępnych jest wiele programów, które po zainstalowaniu informują o odwiedzanych witrynach internetowych, klikanych banerach reklamowych, wyszukiwanych produktach oraz wszelkich innych informacjach, do których pozyskiwania zostały zaprojektowane programy. Wykazano, że nawet szeroko stosowane oprogramowanie do pobierania, takie jak NetZip, zgłasza swoim dostawcom nazwy każdego pliku pobranego przez każdego użytkownika.

Czasami programy te są nieformalnie znane jako aplikacje E.T. , w nawiązaniu do filmu Stevena Spielberga o tym tytule, w którym istota pozaziemska stara się „zadzwonić do domu" – dokładnie to,

co robią programy spyware. Termin spyware odnosi się do każdej technologii, która przesyła informacje bez wiedzy jej użytkownika. Kilka programów dystrybuowanych bezpłatnie za pośrednictwem Internetu potajemnie zbiera informacje o użytkowniku, monitoruje zachowanie użytkownika, a następnie wysyła te dane do reklamodawców. Bardziej ogólna klasa oprogramowania monitorującego, które zbiera informacje do wykorzystania przez reklamodawców, jest znana jako oprogramowanie wspierane przez reklamy lub oprogramowanie reklamowe. Programy te pozwalają freeware zarabiać pieniądze dla swoich twórców, generując przychody w oparciu o liczbę użytkowników, którzy przekazują reklamodawcom informacje o swoich zwyczajach. Chociaż obrońcy programów wspieranych przez reklamy twierdzą, że są one nieszkodliwe, obrońcy prywatności argumentują, że problemem jest kontrola: czy użytkownicy wiedzą, co robią te programy, czy też potajemnie zbierają i przesyłają informacje? Niektóre adware są dostarczane ze skomplikowanymi umowami zawierającymi skomplikowany język prawniczy, aby ukryć fakt, że będą monitorować i zgłaszać zachowanie użytkowników. Co gorsza, wiele takich umów wyraźnie upoważnia dostawcę oprogramowania do zmiany warunków prywatności bez powiadomienia i niedorzecznie instruuje użytkownika, aby często sprawdzał umowy w sieci. Nikt nie ma czasu na monitorowanie niezliczonych dostawców, aby zobaczyć, czy warunki prywatności zostały zmienione, zwłaszcza jeśli nie podejmuje się prób podkreślenia zmian. Innym problemem jest to, że niektóre moduły spyware wykorzystują technologię stealth charakterystyczną dla wirusów, koni trojańskich i innego złośliwego oprogramowania. Na przykład niektóre adware (np. TSADBOT) instalują się jako proces systemowy i nie są wymienione na liście zadań systemu Windows. Dlatego nie można go łatwo przerwać przez użytkownika. TSADBOT jest również odporny na usunięcie; nawet jeśli produkt przewoźnika zostanie odinstalowany, TSADBOT będzie nadal działać. Jeśli zapora sieciowa użytkownika blokuje transmisję wychodzącą przez proces TSADBOT, oprogramowanie szpiegujące inicjuje próby dotarcia do celu z szybkością 10 na sekundę, co potencjalnie prowadzi do przeciążenia jednostki centralnej (CPU) i zasobów sieciowych. Oprogramowanie szpiegujące, jak każde oprogramowanie, może zawierać błędy powodujące problemy z systemem. W szczególności wykazano, że składniki oprogramowania szpiegującego Aureate/Radiate powodują niestabilność i awarie systemu. Jeden z najbardziej rażących przypadków spyware wybuchł w 1999 roku, kiedy odkryto, że CometCursor, dostawca kursorów z uroczymi postaciami z kreskówek skierowanych do dzieci, wysyłał z powrotem na swoje serwery informacje o tym, co dzieci przeglądają w sieci. Według niektórych prawników tego rodzaju potajemne gromadzenie danych o dzieciach może stanowić naruszenie amerykańskiej federalnej ustawy o ochronie prywatności dzieci w Internecie. Napisano kilka bezpłatnych programów, które pomagają użytkownikom identyfikować i usuwać programy szpiegujące. Ponadto zapory osobiste mogą zwykle identyfikować i blokować nieautoryzowaną komunikację wychodzącą; na przykład bezpłatna wersja ZoneAlarm robi to skutecznie. Dzisiejsze programy chroniące przed złośliwym oprogramowaniem (np. Bitdefender) zawierają funkcje antyszpiegowskie. Dostępnych jest również wiele specjalistycznych programów (np. Ad-Aware firmy Lavasoft), które działają w tle w celu monitorowania i udaremniania prób instalacji oprogramowania szpiegującego i reklamowego.

**ZAGROŻENIA DLA WYDAJNOŚCI**

Niektóre działania i zjawiska są uciążliwe dla pracodawców głównie ze względu na ich szkodliwy wpływ na produktywność i nadużywanie zasobów korporacyjnych. Na przykład niechciane wiadomości e-mail i burze pocztowe stanowią problem, ponieważ wyczerpują zasoby, a nie dlatego, że wyrządzają określone szkody organizacji lub jej pracownikom. Jednak łańcuszki, programy szybkiego wzbogacenia się, aukcje online, hazard online, nadmierne zakupy online i uzależnienie od Internetu mogą być bezpośrednio szkodliwe dla pracowników i innych osób.

**Nieefektywne wykorzystanie firmowej poczty e-mail**

Kolejne sekcje koncentrują się na problemach spowodowanych błędami w korzystaniu z poczty elektronicznej — błędami, które mogą powodować irytację, nieefektywność i potencjalne zakłócenia krytycznych procesów biznesowych.

**Przekazywanie wiadomości e-mail na konta osobiste**

Pracownicy mogą ulec pokusie przekierowywania firmowego ruchu e-mail na osobiste adresy e-mail dla wygody lub gdy nie mają wygodnego sposobu uzyskania dostępu do firmowego systemu poczty e-mail spoza biura. Takie przekazywanie powinno być zabronione przez politykę, chyba że do prywatnych wiadomości e-mail pracownika wykorzystywane są wirtualne sieci prywatne (VPN) lub inne silnie zaszyfrowane kanały. Poczta elektroniczna i inny ruch w Internecie nie są objęte żadną zasadą poufności. Teoretycznie każdy, kto jest w stanie przechwycić pakiety TCP/IP w dowolnym miejscu podczas transmisji, może naruszyć poufność. Tak więc, ponownie w teorii, każdy, kto ma dostęp do sprzętu dostawców usług internetowych, szkieletowych linii transmisyjnych Internetu, a nawet publicznej komutowanej sieci telefonicznej, może przechwytywać pakiety. Przy łączu w dół z przekaźników satelitarnych wynoszącym mile kwadratowe praktycznie wszystko może zostać przechwycone ze znacznej części ruchu krążącego w Internecie. W praktyce jednak prawie wszystkie zgłoszone przypadki naruszenia poufności wynikały z dostępu do danych w punktach końcowych, a nie podczas ich przesyłania. Ataki wewnętrzne i naruszenia bezpieczeństwa serwerów były odpowiedzialne za większość przechwyceń danych, które dotarły do prasy i sądów. Praktyczną przeszkodą w skutecznym przechwytywaniu ważnych danych w tranzycie jest routing datagramów, który leży u podstaw Internetu: datagramy to pakiety informacji z informacjami o pochodzeniu i miejscu docelowym; transmisja typu store-and-forward umożliwia przesyłanie tych datagramów przez Internet innymi trasami niż inne pakiety w strumieniu wiadomości. Tablice routingu mogą być aktualizowane w czasie rzeczywistym, aby odzwierciedlić zmiany w natężeniu ruchu lub dostępności określonych łączy do innych miejsc docelowych w Internecie, więc nie ma gwarancji, że pakiety z tej samej wiadomości będą podróżować tą samą trasą lub dotrą we właściwej kolejności (kolejność numery pozwalają na ponowne złożenie oryginalnej wiadomości). Dlatego jest mało prawdopodobne, aby losowe przejmowanie pojedynczych pakietów w miejscu innym niż źródło i miejsce docelowe pakietów przyniosło wiele rezultatów. Niemniej jednak najlepsze praktyki zalecają stosowanie szyfrowania do przekazywania wrażliwych danych; dlatego wiele organizacji instaluje wirtualne sieci prywatne (VPN) do komunikacji z uznanymi partnerami handlowymi. Oprogramowanie VPN jest również dostępne do tunelowania przez Internet ze zdalnej stacji roboczej przez niezabezpieczone linie komunikacyjne. Prostym przykładem takiej funkcji szyfrowania łącza są internetowe usługi poczty elektronicznej, które używają protokołu SSL do ustanowienia bezpiecznego łącza do serwera poczty e-mail (tj. używają protokołu https zamiast zwykłego http). Użytkownik może odbierać wiadomości e-mail z serwera korporacyjnego bez konieczności przekazywania ich do niezabezpieczonej zewnętrznej usługi poczty e-mail. Niektóre produkty poczty e-mail zawierają narzędzia do bezpośredniej komunikacji między bezpiecznym serwerem poczty e-mail a klientem poczty e-mail użytkownika. Używanie oprogramowania do tunelowania VPN jako ciągu wyszukiwania w wyszukiwarce Google przynosi prawie pół miliona trafień (stan na maj 2013 r.), z których wiele dotyczy określonych produktów i kart katalogowych, dzięki czemu czytelnicy będą mogli znaleźć rozwiązanie odpowiadające ich potrzebom.

**Błędne oznaczenie wiersza tematu**

Wiele osób popełnia błąd polegający na tworzeniu nowych wiadomości do korespondenta, znajdując starą wiadomość od tej osoby i odpowiadając na nią. Problem polega na tym, że osoby te zwykle

pozostawiają stary temat nietknięty, co prowadzi do absurdalnych sytuacji, takich jak znalezienie niezwykle ważnej wiadomości w lipcu w e-mailu oznaczonym jako „Przyjęcie urodzinowe 12 maja". Nie wszystkie wiadomości e-mail są sobie równe; niektóre są przeznaczone na śmietnik, jeśli nie historii, to przynajmniej systemu poczty elektronicznej. Ta decyzja jest czasami podejmowana automatycznie w zależności od tematu. Na przykład użytkownik dodaje wiersz tematu żartu do filtra wiadomości e-mail, co powoduje, że przyszłe wiadomości z tym tematem będą lądować w folderze wiadomości-śmieci. Ktoś odpowiada na żartobliwą wiadomość, podając ważne informacje, a filtr poczty widzi temat i automatycznie przenosi wiadomość do folderu wiadomości-śmieci odbiorcy. Odbiorca może nigdy nie zobaczyć ważnych informacji, ponieważ większość ludzi nie monitoruje aktywnie swoich folderów-śmieci. Inny problem z błędnie oznaczonymi tematami pojawia się, gdy ktoś umieszcza więcej niż jeden odrębny temat w wiadomości e-mail, której temat sugeruje co innego. Załóżmy na przykład, że temat wiadomości e-mail brzmi „Spotkanie w przyszłym tygodniu", ale nadawca zawiera pilną prośbę o podjęcie działań w dniu dzisiejszym w jakiejś krytycznej sprawie; istnieje duża szansa, że odbiorca może nie otworzyć wiadomości od razu, jeśli inne wiadomości wydają się ważniejsze. Pracownicy powinni, aby ich temat był jak najbardziej opisowy, bez przekształcania go w akapit. Niektóre systemy poczty e-mail obcinają wiersze tematu w wyświetlanych wiadomościach, które widzi użytkownik; sensowne jest umieszczanie słów kluczowych na początku tematu. Zachęcaj pracowników do używania prefiksów, takich jak „MISA:" lub „ABCv2.0.1:", aby ułatwić organizowanie wiadomości. Pomocne może być również stosowanie standardowych formatów w tematach. Na przykład wykładowcy i pracownicy programu MISA na Norwich University odnoszą się do problemu na konkretnym seminarium, używając formularza „MISA c.s" w temacie, gdzie c oznacza klasę (np. 40 dla studentów rozpoczynających się w grudniu 2013 r.) a s oznacza numer seminarium (np. od 1 do 6). Te proste sugestie mogą sprawić, że poczta e-mail będzie skuteczniejsza jako narzędzie komunikacji.

**Pierwsze e-Wrażenia**

Kiedy otrzymujesz wiadomość e-mail od nieznajomego, czy obchodzi cię, czy zawiera ona błędy ortograficzne i gramatyczne? A co z obraźliwym językiem i obraźliwym humorem? Czy kontekst ma znaczenie? Na przykład, czy stosujesz te same standardy w przypadku wiadomości e-mail odnoszących się do spraw biznesowych, jak w przypadku nieformalnej komunikacji dotyczącej hobby? Naukowcy z University of Chicago badali wpływ wiadomości e-mail na postrzeganie charakteru. Psycholog Nicholas Epley i współpracownicy zbadali rozmowy telefoniczne na tematy rozmów między losowo wybranymi osobami za pomocą sześciu przypisanych pytań. Następnie dokonali transkrypcji rozmów ustnych i użyli dokładnie tych samych odpowiedzi w pisemnej, e-mailowej wersji sesji pytań i odpowiedzi. Ich wyniki były interesujące. Pytający otrzymali fałszywe szkice biograficzne ludzi, z którymi się komunikowali, wskazujące na inteligencję poniżej normy lub inteligencję normalną, a także różne zdjęcia przedstawiające schludnych ludzi lub niechlujów. Badani, którzy słuchali przez telefon zalecanych odpowiedzi, mieli pozytywne wrażenia na temat inteligencji rozmówcy, niezależnie od biogramu i zdjęć. W przeciwieństwie do tego, „Jednak za pośrednictwem poczty elektronicznej uczniowie trzymali się swojego pierwszego wrażenia, nadal zakładając, że ich partnerzy mają na przykład inteligencję poniżej standardów, jeśli tak wskazywał szkic biograficzny". Jeśli te badania zostaną potwierdzone, lekcja jest taka, że podczas korzystania z poczty e-mail pierwsze wrażenie naprawdę się liczy. Specjaliści powinni uważnie przeglądać wiadomości e-mail pod kątem akceptowalnego tekstu, w tym doboru słów, interpunkcji, wielkich liter i pisowni.

**Zastrzeżenia dotyczące wiadomości e-mail**

Autor Kabay otrzymał kiedyś 30-wyrazową wiadomość e-mail od bardzo miłego czytelnika z Wielkiej Brytanii i zauważył, że jego system poczty elektronicznej dodał następujące zdumiewające

zastrzeżenie, które jest cytowane w całości, łącznie z brytyjską pisownią, po oczyszczeniu go ze szczegółów identyfikacyjnych:

Ta wiadomość e-mail, jej zawartość oraz wszelkie przesłane z nią pliki lub załączniki są przeznaczone wyłącznie dla adresata (adresatów) i mogą być prawnie uprzywilejowane i/lub poufne. Dostęp jakiejkolwiek innej strony jest nieautoryzowany bez wyraźnej pisemnej zgody nadawcy. Jeśli otrzymałeś ten e-mail przez pomyłkę, nie możesz kopiować ani wykorzystywać treści, plików, załączników lub informacji w żaden sposób ani ujawniać ich innym osobom. Proszę go zniszczyć i skontaktować się z nadawcą pod numerem wydrukowanym powyżej, za pośrednictwem centrali <Nazwa banku> pod numerem +44 (0) nnnn nnnnnn dla <miejsce1> i +44 (0) nnnn nnnnnn dla <miejsce2> lub e-mailem zwrotnym . Komunikacja internetowa nie jest bezpieczna, jeśli nie jest chroniona za pomocą silnej kryptografii. Ta wiadomość e-mail została przygotowana na podstawie informacji, które autor uważa za rzetelne i dokładne, ale <Nazwa banku> nie udziela żadnych gwarancji ani oświadczeń, wyraźnych ani dorozumianych, co do ich dokładności lub kompletności i nie ponosi odpowiedzialności wobec Ciebie ani nikogo innego za wszelkie straty lub szkody w związku z jakąkolwiek transmisją wysyłaną przez Bank do Ciebie przez Internet. <Nazwa Banku> nie gwarantuje, że jakiekolwiek informacje lub materiały są wolne od wad lub wirusów. W szczególności <Nazwa Banku> nie ponosi odpowiedzialności za zmiany dokonane w niniejszym e-mailu po jego wysłaniu. Jeśli podejrzewasz, że ta wiadomość e-mail mogła zostać zmieniona lub przechwycona, skontaktuj się z nadawcą w sposób podany powyżej. Jeśli ta transmisja zawiera pliki lub załączniki, upewnij się, że zostały one otwarte w odpowiedniej aplikacji, aby zapewnić pełny odbiór. Jeśli napotkasz trudności, skontaktuj się ponownie z nadawcą w sposób podany powyżej. Wszelkie opinie wyrażone w tej transmisji są opiniami autora i niekoniecznie odzwierciedlają opinie Banku i mogą ulec zmianie bez powiadomienia. Należy pamiętać, że dla celów niniejszego dokumentu wszelkie odniesienia do <Nazwa Banku> lub Banku należy rozumieć jako <Nazwa Banku> (miejsce) Limited lub dowolnego innego członka Grupy Banków <Większy>. Nic w tej transmisji nie stanowi ani nie będzie uważane za ofertę lub przyjęcie oferty ani w inny sposób nie ma skutku w postaci zawarcia umowy za pośrednictwem komunikacji elektronicznej.

Kabay skomentował w swojej odpowiedzi: „Czy wiesz, że twoja wiadomość ma 30 słów (152 bajty ze spacjami), podczas gdy twoje wyłączenie odpowiedzialności ma 367 słów (2177 bajtów)? To najniższy stosunek sygnału do szumu (6,5 procent użytecznych informacji z całości i stosunek sygnału do szumu 1:73), jaki kiedykolwiek widziałem poza łańcuchem kopia-kopia-kopia. Proszę pogratulować swoim prawnikom wykorzystania maksymalnej przepustowości przy minimalnej zawartości!” Zaśmiecanie wiadomości e-mail w ten sposób to marnowanie przepustowości. Gorzej jest w biurach, gdzie ludzie kopiują całe wiadomości bez redagowania ich treści, co skutkuje łańcuchami kopiowania kopii, kopiowania kopii, które rozprzestrzeniają się jak rakowate erupcje poprzez kosze odbiorcze w całej organizacji. Niektórzy ludzie, którzy mają dobre intencje, umieszczają nawet szczegółowe nagłówki w swoich kopiach. Ze względu na grzeczność i zdrowy rozsądek, kiedy odpowiada się na wiadomość, łatwo jest usunąć z kopii oryginału nieistotne elementy. Nadawcy mogą używać wielokropków (…w przypadku fragmentów w zdaniu,… w przypadku fragmentów przekraczających granice zdania), aby zasygnalizować luki, ale zazwyczaj jeden lub dwa wycinki wystarczą, aby wyczyścić kopię, aby czytelnik mógł zrozumieć istotę rozmowy bez konieczności przedzierać się przez stosy zbędnych rzeczy. Niestety, zalecenie to nie wydaje się być często stosowane w praktyce.

**Scentralizowane listy dystrybucyjne**

Organizacje mogą rozrosnąć się na tyle, że wśród personelu występuje znaczna rotacja. Nie tylko nowi członkowie personelu okresowo dołączają do grupy, ale także pracownicy przechodzą z jednej grupy funkcjonalnej do drugiej; na przykład pracownik może zmienić stanowisko z asystenta dyrektora w

jednym programie na dyrektora administracyjnego w innym. Czasami członkowie personelu mogą całkowicie opuścić grupę. Prymitywnym sposobem utrzymywania list dystrybucyjnych jest wyznaczenie „Keeper-of-the-Lists" do utrzymywania listy wszystkich członków personelu; jednak nie ma powiązania między plikiem a listami adresowymi, które każdy członek grupy musi utrzymywać, aby móc dystrybuować wiadomości e-mail do odpowiednich osób lub grup. Niezależne pliki prawie na pewno odbiegają od scentralizowanej i dokładnej listy. Na przykład w wiadomości, która powinna zostać wysłana do wszystkich obecnych pracowników, może brakować kilku nowych członków, w tym pracowników, którzy już nie pracują w grupie docelowej. Próba zmuszenia wielu ludzi do utrzymywania własnych kopii kilku list dystrybucyjnych jest beznadziejną przyczyną: nawet przy najlepszej woli ludzie nieuchronnie zapomną zaktualizować swoje listy, a zatem:

* Niektóre przesyłki nie trafią do uprawnionych odbiorców.

* Niektóre osoby otrzymają wiadomości, których nie czytają w interesach.

Istnieją co najmniej cztery rozwiązania, które rozwiązałyby taki problem

1. Można wdrożyć centralny serwer poczty e-mail (np. Microsoft Exchange Server), przełączyć wszystkich użytkowników do centralnie kontrolowanego klienta poczty e-mail (np. Microsoft Outlook) i zdefiniować korporacyjne listy dystrybucyjne utrzymywane przez Keeper-of-the-Lists. Wszyscy użytkownicy automatycznie uzyskają dostęp do jedynej listy dystrybucyjnej dla każdej grupy bez ręcznej interwencji.

2. Można zainstalować szeroko dostępne oprogramowanie serwera list, aby umożliwić scentralizowane tworzenie i utrzymywanie określonych list; na przykład SGS-ALL, SGS-DIRECTORS, MSIA-STAFF, MSIA-INSTRUCTORS i tym podobne tworzą listy, których wszyscy pracownicy mogą używać do adresowania poczty elektronicznej.

3. Można przełączyć wszystkich użytkowników na dowolnego klienta poczty e-mail, który obsługuje eksportowalne listy mailingowe. Zaktualizowane korporacyjne listy dystrybucyjne można następnie wysłać do wszystkich użytkowników. Jednak to rozwiązanie nadal wymaga ręcznej interwencji ze strony użytkowników: każdy musi zastąpić starą listę nową listą.

4. Można utworzyć grupę dyskusyjną na serwerze publicznym (np. Yahoo Groups) w celu zdefiniowania grup zamkniętych. Te grupy zapewniają automatyczny dostęp do list mailingowych. Niestety takie podejście ma poważne problemy:

* Istnieją obawy dotyczące bezpieczeństwa związane z używaniem takich grup do komunikacji korporacyjnej.

* Niewłaściwe wydaje się umieszczanie niezbędnej aplikacji produkcyjnej na darmowym zasobie całkowicie poza kontrolą organizacji.

**E-mail w formacie HTML**

Jednym z sześciu podstawowych atrybutów informacji, które chronimy, jest integralność, której jednym z aspektów jest zgodność z pierwotnie przechowywanymi danymi (patrz rozdział 3 niniejszego podręcznika). Kiedy ktoś zada sobie trud stworzenia elegancko sformatowanego memorandum lub innego dokumentu i wyśle go do odbiorców, każdy chciałby zachować integralność danych, widząc ten sam wygląd na wszystkich systemach udostępniających ten dokument. Niestety wysyłanie sformatowanych wiadomości jako wiadomości e-mail (w odróżnieniu od załączników) nie gwarantuje

zachowania dokładnego wyglądu materiału źródłowego. Atrakcyjne, dobrze sformatowane wiadomości e-mail z pogrubioną czcionką, kursywą, różnymi rozmiarami punktów itp. są zwykle przesyłane w formacie HTML (hipertekstowy język znaczników) do skrzynek pocztowych odbiorców, na co zezwalają klienci poczty większości użytkowników (Eudora, Netscape, Outlook itp.). zabawnie wyglądający kod, który ma zostać odtworzony w coś podobnego do oryginału. Słowo podobne jest wymieniane, a nie dokładnie takie, ponieważ HTML niekoniecznie kontroluje ostateczny wygląd tekstu w systemie odbiorcy. Kody odnoszą się do typów, a nie dokładnych dopasowań czcionek; w związku z tym nadawca może chcieć użyć, powiedzmy, 24-punktowego Arial jako wyświetlacza nagłówka 1, ale konkretny odbiorca mógł zdefiniować nagłówek 1 jako, powiedzmy, Times Roman 14 pkt. Dwustronicowy dokument oryginalny może wydawać się dokumentem trzystronicowym dla jednego odbiorcy, a dokumentem jednostronicowym dla innego. Co ważniejsze, wiele osób wyłącza pocztę e-mail w formacie HTML ze względów bezpieczeństwa. Wszystkie takie sformatowane wiadomości e-mail są automatycznie konwertowane na zwykły tekst ASCII. Korespondent wysłał kiedyś autorowi Kabayowi wiadomość, która brzmiała: „Uwaga: system oceny kursu on-line może być używany w pokoju, laboratorium i domu — wszędzie tam, gdzie jest dostępny dostęp do Internetu. / Przegląd:…. Nieukończenie oceny kursu spowoduje „wstrzymanie" końcowych ocen ucznia". Poniższy fragment wiadomości przedstawia wynik autokonwersji MS-Outlook oryginalnie sformatowanej wiadomości HTML do ASCII: „Uwaga: Z systemu oceny kursów on-line można korzystać z sali, laboratorium i domu ? wszędzie tam, gdzie jest dostęp do Internetu./Przegląd:…. Nieukończenie oceny kursu spowoduje ?wstrzymanie? umieszczane na końcowych ocenach ucznia".

* W procesie konwersji oryginalne apostrofy zamieniły się w znaki zapytania („?hold?"), ponieważ nadawca używał „krzywych" cudzysłowów zamiast prostych w edytorze tekstu lub edytorze wiadomości e-mail. Jeśli ktoś chce uniknąć tej osobliwości podczas korzystania z wcześniejszych wersji Microsoft Word, musi wyłączyć opcję w {Narzędzia | Autokorekta | Autoformatowanie podczas pisania}, usuwając zaznaczenie pola oznaczonego {„Cytaty proste" z „cytatami inteligentnymi"}. W późniejszych wersjach wyłącz tę opcję, klikając {Opcje programu Word} w menu głównym, wybierając {Sprawdzanie}, a następnie klikając przycisk {Opcje autokorekty} u góry okna. {Autoformatowanie podczas pisania} to jedna z dostępnych kart, po której możesz odznaczyć pole {„Cytaty proste" z „cytatami inteligentnymi"}.

* Ponadto wygląda na to, że w tekście w pierwszej sekcji (oznaczonej jako „Uwaga") mogła znajdować się kreska. Można wyłączyć tę konwersję w tych samych menu, odznaczając {Myślniki (–) z myślnikiem (—)}.

Znacznie prostszym rozwiązaniem, aby zapobiec bałaganowi, jest po prostu wysłanie niesformatowanego tekstu ASCII we wszystkich wiadomościach wychodzących poprzez wybranie tej opcji w swoim pakiecie e-mail. Niektóre osoby próbują wysyłać pliki, które powinny wyglądać tak samo w systemie odbiorcy i systemie źródłowym, załączając dokumenty edytora tekstu: na przykład pliki Word (DOC), pliki WordPerfect (WPD) lub pliki Rich Text Format (RTF) (i wkrótce). Niestety, nawet te próby nie zawsze działają zgodnie z planem, ponieważ brak wspólnych czcionek, różne domyślne rozmiary papieru (w różnych krajach mogą być używane różne rozmiary) oraz różne marginesy drukowania (wynikające z instalacji różnych drukarek) mogą powodować, że dokumenty nie będą wyglądać dokładnie to samo we wszystkich systemach. Jeśli więc dokładny wygląd wiadomości wysyłanej przez e-mail jest niezwykle ważny, należy wysłać treść i jej format w sposób (w dużej mierze) niezależny od platformy; na przykład pliki Acrobat PDF (Portable Document Format). Chociaż nawet one niekoniecznie prowadzą do idealnego odwzorowania intencji autora w różnych systemach, pliki PDF mają znacznie większe szanse powodzenia niż inne wymienione metody. Pliki PDF można tworzyć na wiele sposobów; niektóre systemy mają zainstalowany Adobe Acrobat, dzięki czemu można albo

wysłać do sterownika Acrobat, aby utworzyć pliki PDF, albo nawet po prostu kliknąć przycisk paska narzędzi, aby to zrobić z poziomu edytora tekstu. Na przykład Microsoft Office 2007 i nowsze wersje zapewniają możliwość zapisywania jako PDF we wszystkich swoich głównych komponentach. Istnieją inne pakiety, które są tańsze (i generalnie mniej bogate w funkcje) niż pełne oprogramowanie Adobe Acrobat, ale mimo to umożliwiają użytkownikom łatwe tworzenie plików PDF. Można wpisać „utwórz PDF" w wyszukiwarce internetowej, aby znaleźć wiele opcji.

**Listy dystrybucyjne w wiadomościach e-mail**

Jeśli chodzi o poufność, należy wziąć pod uwagę, że użycie pól Do i DW w wiadomości e-mail powoduje, że wszystkie adresy odbiorców są widoczne dla wszystkich odbiorców. Ta sytuacja jest zwykle pomocna w wewnętrznej poczcie e-mail, ponieważ członkowie zespołu mogą zobaczyć, kto otrzymał wiadomość, ale może to być irytujące w zewnętrznej poczcie e-mail. Dlaczego lista dziesiątek, a nawet setek nazwisk nieznajomych miałaby być swobodnie rozpowszechniana wśród nich, bez wyraźnej zgody wszystkich zainteresowanych? Kto wie, gdzie trafią te informacje? Użycie pola BCC (ślepa kopia) eliminuje możliwość zobaczenia przez odbiorców wszystkich zamierzonych odbiorców oryginalnej wiadomości. Ten dodatkowy krok jest dobrym elementem etykiety e-mailowej, niezależnie od tego, czy wiadomość jest biznesowa, czy osobista. Pole BCC jest również przydatne w wewnętrznej poczcie e-mail, gdy lista odbiorców jest bardzo duża, ale nie jest ważne, aby ludzie dokładnie wiedzieli, kto otrzymał wiadomość. W jednym przypadku miła pani z działu kadr (HR) na uniwersytecie wysłała wiadomość do tuzina osób, przypominając odbiorcom, że nie zakończyli jeszcze rejestracji w celu uzyskania nowego ubezpieczenia medycznego. Niestety umieściła wszystkie adresy e-mail w wierszu CC (kopia), gdzie były widoczne dla wszystkich na liście. Jak było do przewidzenia, ktoś z listy ułożył jej odpowiedź, nacisnął ODPOWIEDZ WSZYSTKIM i wysłał nieco osobiste informacje o stanie jej problemów medycznych do wszystkich odbiorców z pierwotnej listy, z których żaden nie był zainteresowany jej problemami. Na szczęście w tej wiadomości nie było wielu prywatnych informacji, ale uświadomiło to, że wiele osób bezmyślnie używa linii CC do adresowania do listy dystrybucyjnej i że wiele osób bezmyślnie używa ODPOWIEDZ WSZYSTKIM do odpowiedzi na każdą wiadomość e-mail. Połączenie może prowadzić do żenujących naruszeń poufności; kiedy pracownicy działu HR używają CC zamiast BCC (funkcja Blind Carbon Copy, która ukrywa listę dystrybucyjną), funkcja ODPOWIEDZ WSZYSTKIM może nieumyślnie naruszyć prywatność. W tym przypadku nie ujawniono szczególnie wrażliwych materiałów, ale inny przypadek mógłby z łatwością naruszyć ustawę HIPAA (Health Information Portability and Accountability Act) oraz uniwersyteckie zasady dotyczące poufności pracowników. Gdy pracownicy zrozumieją problem, nauczą się nie używać CC do list dystrybucyjnych, gdy intencją jest komunikowanie się z poszczególnymi osobami; domyślnie wszyscy powinni korzystać z listy UDW, chyba że istnieje potrzeba stymulowania dyskusji w grupie lub ważne jest, aby członkowie grupy wiedzieli, kto otrzymał wiadomość. Ważne jest, aby nie lekceważyć tego problemu jako zbyt łatwego lub zbyt oczywistego, aby się nim przejmować. „Z głupotą sami bogowie walczą na próżno" — napisał Friedrich von Schiller w swojej Dziewicy Orleańskiej (Die Jungfrau von Orleans) w 1801 r. Niemniej jednak zwyczaj CC + REPLY ALL staje się tajnym kanałem udostępniania poufnych informacji osobom, które odmówić prowadzenia książki adresowej i po prostu wyszukać starą wiadomość e-mail i ODPOWIEDZIEĆ na nią jako leniwy sposób na wysłanie nowej wiadomości. Jeśli wątpisz w powagę problemu, poświęć trochę czasu na przejrzenie własnych archiwów e-maili i policz, ile oczywistych przypadków e-maili z nieodpowiednimi tematami i nieodpowiednimi listami dystrybucyjnymi znajduje się w otrzymanych folderach. Niestety, możesz być przerażony wynikami swoich badań. Jeśli zajrzysz do własnego folderu SENT, możesz być jeszcze bardziej przerażony.

**Efektywne wykorzystanie BCC**

Jak wspomniano, problemy powodowane przez CC są gorsze, gdy odbiorcy się nie znają. Często otrzymuje się wiadomości od nieskomplikowanych technicznie korespondentów, którzy w polu DW umieszczają dziesiątki adresów e-mail, mimo że wielu odbiorców jest dla siebie zupełnie obcych. Takie ujawnienie adresów e-mail zawsze denerwuje pracowników ochrony; kto wie, czy wszyscy na liście są godni zaufania? Nawet jeśli lista nie jest niewłaściwie wykorzystywana do jawnego spamu, ludzie często ODPOWIADAJĄ WSZYSTKIM, podając bezużyteczne informacje, skutecznie dodając osoby do list dyskusyjnych, na których nigdy nie chcieli się znaleźć. Szczególnie irytującym nawykiem jest ODPOWIADANIE WSZYSTKIM komentarzem wynikającym z jakiejś początkowej wiadomości. Następnie ludzie generują serię coraz dłuższych wiadomości, w tym kopie wszystkich poprzednich kopii pozornie sprytnej odpowiedzi, zmuszając niektórych użytkowników do generowania dodatku do filtrów wiadomości-śmieci. Nawyk używania opcji REPLY ALL jest wystarczająco irytujący, gdy odpowiedź w rzeczywistości nie musi trafić do wszystkich z oryginalnej listy dystrybucyjnej. Jednak funkcja REPLY ALL jest pozytywnym zagrożeniem, jeśli jest połączona z odrażającą praktyką wykorzystywania istniejącej wiadomości e-mail jako skrótu do tworzenia nowej wiadomości na zupełnie inny temat.

**Zarządzanie prywatną pocztą e-mail w pracy**

Co jest złego w używaniu firmowej poczty e-mail do żartów, zaproszeń i tym podobnych? Jednym z problemów jest marnowanie przepustowości. Niektórzy ludzie uważają, że jakość żartów, mistyfikacji i sesji wiwatujących jest na tyle niska, że może być irytująca. Co najgorsze, poziom tolerancji dla tego, co jest uważane za właściwe w miejscu pracy, może się różnić w zależności od osoby, co wymaga najwyższej staranności i rozwagi dla wszystkich. Inny problem pojawia się w przypadku wiadomości wrażliwych politycznie, takich jak ogłoszenia lub poglądy, które niektórzy członkowie grupy mogą uznać za obraźliwe. Czemu wszyscy w grupie powinni być narażeni na zalew niechcianych wiadomości e-mail tylko dlatego, że gdzieś pracują? W pytaniu poruszono również kilka cennych i pouczających kwestii dotyczących zasad właściwego korzystania z poczty e-mail. Korporacje muszą mieć formalną pisemną politykę dotyczącą właściwego korzystania z oficjalnej poczty e-mail. Kierownicy powinni sformułować jasne, pisemne zasady, z którymi każdy członek personelu może łatwo zapoznać się w celu uzyskania wskazówek dotyczących odpowiednich i nieodpowiednich treści wiadomości osobistych wysyłanych za pomocą korporacyjnych adresów pocztowych. Taka polityka zmniejszy możliwe rozczarowania i niechęć wynikające z decyzji opartych na niepisanych oczekiwaniach. Ponadto wszelkie przejawy dyskryminacji ze względu na określone uprzedzenia polityczne lub religijne będą musiały zostać zbadane, aby upewnić się, że organizacja nie podlega reperkusjom prawnym. Łatwym narzędziem, które pracownicy mogą opracować, jest dobrowolna lista adresów e-mail poza pracą dla e-maili poza pracą. Yahoo! na przykład grupa (http://groups.yahoo.com/) oferuje wiele korzyści w porównaniu z nieformalną listą w polu DW: lub Do:. Żarty i tym podobne mogą być rozpowszechniane tylko wśród chętnych odbiorców, ponieważ dołączenie może być całkowicie opcjonalne. Jednak pracownicy muszą zawsze pamiętać, że wszelkie działania wykonywane na firmowym sprzęcie lub przy użyciu firmowych zasobów komputerowych mogą być przeglądane przez upoważnione osoby i mogą potencjalnie zaszkodzić ich reputacji lub, co gorsza, narazić ich na problemy prawne.

**Burze pocztowe**

Osobliwy rodzaj wiadomości-śmieci jest wysyłany przez przypadek. Te lawiny niechcianych wiadomości nazywane są burzami pocztowymi. Większość z nas należy do list mailingowych; wielu z nas ma więcej niż jeden adres e-mail; niektórzy z nas używają automatycznego przekazywania, aby automatycznie przenosić wiadomości e-mail z jednego adresu na inny; a niektórzy z nas używają automatycznych odpowiedzi na naszych kontach e-mail, aby informować korespondentów, kiedy jesteśmy poza biurem lub nie możemy szybko odpowiedzieć. Wszystkie te czynniki mogą przyczynić się do burz pocztowych.

**Automatyczne przekazywanie**

Burza pocztowa ma miejsce, gdy komputery zaczynają wysyłać do siebie pocztę bez interwencji człowieka. Czasami burze pocztowe mogą stać się odmową usługi poprzez nasycenie kanałów komunikacyjnych i innych zasobów. Robaki obsługujące pocztę e-mail, takie jak Melissa, komunikat I-love-you i inne, to przykłady złośliwego oprogramowania, którego autorzy celowo napisali je w celu wywoływania burz pocztowych. Prosta sytuacja miała miejsce w latach 90.:

* Pracownik wyjeżdżający na urlop postanowił otrzymywać firmową pocztę e-mail za pomocą konta osobistego u dostawcy usług internetowych o zasięgu globalnym. Po ustawieniu polecenia automatycznego przekazywania na koncie firmowym cała przychodząca poczta była wysyłana na osobiste konto e-mail.

* Niestety, na odległej tropikalnej wyspie, na której wczasowicz spędził dwa tygodnie, nie można było uzyskać dostępu do ogólnoświatowego dostawcy usług internetowych bez dopłaty w wysokości 6 dolarów za minutę połączenia międzymiastowego z najbliższym węzłem telefonicznym. Okazało się to zbyt kosztowne i nie otrzymano ani nie wysłano żadnych e-maili.

* W międzyczasie konto firmowe sumiennie przekazywało każdą otrzymaną wiadomość na właściwe konto osobiste - które miało niewielki limit przechowywania wynoszący 250 wiadomości. Limit ten został osiągnięty w ciągu kilku dni. W tym momencie każda wiadomość przychodząca generowała odesłanie informujące nadawcę, że skrzynka pocztowa odbiorcy jest pełna.

* Pierwsza wiadomość z zapełnioną skrzynką pocztową wysłana na konto firmowe została automatycznie przekazana z powrotem do osobistej skrzynki pocztowej wczasowicza.

* Ta kopia wiadomości o pełnej skrzynce pocztowej wygenerowała drugą wiadomość o pełnej skrzynce pocztowej, która następnie została odesłana z powrotem na konto firmowe i tak dalej bez przerwy.

* W końcu nawet firmowa skrzynka pocztowa się zapełniła, a potem dwa systemy pocztowe nadal rozmawiały ze sobą w nieskończoność. W tym konkretnym przypadku administratorzy systemu zauważyli problem, gdy skrzynka pocztowa użytkownika osiągnęła 20 000 wiadomości i spowodowała awarię serwera pocztowego.

Liczba wiadomości e-mail, które mogą zostać wygenerowane przez tego rodzaju nieskończoną pętlę, jest funkcją opóźnienia systemu pozytywnego sprzężenia zwrotnego, który przypadkowo utworzył użytkownik. Na przykład, jeśli zwrot odesłanej wiadomości do witryny, z której pochodzi, zajmuje dokładnie jedną minutę, to każda wiadomość powodująca początkowy błąd może utworzyć 60 dodatkowych wiadomości na godzinę. Jednak każda nowa wiadomość od innego nadawcy, która dotrze do pierwotnej skrzynki pocztowej, wygeneruje własny nowy zestaw odrzucanych wiadomości w nieskończonych pętlach. Nierzadko zdarza się, że dziesiątki tysięcy wiadomości gromadzą się w skrzynce pocztowej odbiorcy, jeśli nikt nie zauważy pętli z ruchem stale rosnącym do setek lub tysięcy wiadomości na godzinę przeskakujących między kontami, potencjalnie generujących odmowę usługi w firmowej poczcie e-mail z powodu nasycenia przepustowości sam. Serwery pocztowe mogą również ulec awarii z powodu przytłaczającego ruchu. Wiadomość o nieobecności może również przypadkowo wywołać burzę pocztową w wyniku wyścigu. Na przykład dwóch pracowników (Albert i Bob) włącza wiadomości o nieobecności w biurze, a Albert wysyła wiadomość e-mail do Boba. Usługa e-mail Boba odsyła Albertowi wiadomość o nieobecności, co z kolei generuje kolejną wiadomość o nieobecności od Alberta do Boba. Skutki burzy pocztowej.

**Źle skonfigurowane serwery list**

Użytkownik autorespondera może należeć do listy, gdzie adres OD jest w rzeczywistości adresem rozgłoszeniowym wysyłającym odpowiedź na całą listę. Pierwsza zautomatyzowana odpowiedź „poza biurem" na listę wygeneruje wiadomość do wszystkich osób na tej liście, generując nieskończoną sekwencję wiadomości „do i z". Ta sytuacja jest bardzo krępująca dla administratora listy i bardzo irytująca dla wszystkich innych.

**Błąd ludzki**

Coś analogicznego do burzy pocztowej wynika z bezmyślnego zachowania podczas korzystania z publicznej listy. Typowy przypadek ma miejsce, gdy członek listy publikuje na całej liście komentarze dotyczące tylko jednej osoby. Na przykład członek prosi o przedruk artykułu, a inny odpowiada na liście: „Jutro wyślę ci przedruk". Kilka tysięcy niechętnych czytelników wie teraz o tej planowanej wiadomości e-mail. Jedna z tych zirytowanych osób publikuje wiadomość, mówiąc: „Czy naprawdę musiałeś opublikować tę wiadomość na całej liście?" Ta druga wiadomość jest tak irytująca, że co najmniej jedna inna osoba umieszcza trzecią wiadomość na całej liście, krytykując autora drugiego listu za krytykę autora pierwszego. Ta bezużyteczna burza e-maili jest kontynuowana za pośrednictwem listy publicznej, tworząc tysiące kopii bezużytecznych informacji. Inną formą nierozważnego zachowania jest cytowanie całych wiadomości podczas odpowiadania na e-mail. Do nowej wiadomości należy skopiować tylko te fragmenty tekstu, które wywołały odpowiedź. Zasada ta jest szczególnie ważna na listach publicznych, gdzie zaobserwowano wiadomości zawierające cały tekst, w tym nagłówki internetowe, aż do siedmiu poziomów poprzednich wiadomości. Często ilość nowych informacji zawartych w wiadomościach wysyłanych do grup Usenet jest bardzo mała; reszta to cytaty z cytatów z cytatów.

**Kupowanie w sieci**

Pracodawcy mogą zezwolić na rozsądne (niezależnie od terminu) wykorzystanie zasobów korporacyjnych do działań niezwiązanych z pracą, w tym kupowanie usług i produktów przez Internet. Jednak w interesie pracodawców jest edukowanie pracowników, aby nie stali się ofiarami przestępców. Pracownik zrozpaczony utratą znacznych sum z powodu głupiej łatwowierności nie będzie tak produktywny jak zwykle; w każdym razie nikt nie chce widzieć oszukiwanych przyjaciół i kolegów. Kupowanie od znanych sprzedawców przez Internet może być równie satysfakcjonujące, jak kupowanie w ich sklepach. Jeśli znasz organizacje sprzedające towary i usługi, nie ma większego powodu do obaw związanych z kupowaniem od nich za pośrednictwem połączenia internetowego niż kupowaniem od nich przez telefon lub osobiście w sklepie. Witryny należące do uznanych sprzedawców lub organizacji, takich jak organizacje charytatywne typu non-profit, są godne zaufania, zwłaszcza jeśli zawierają jeden z kilku symboli reprezentujących zgodność z różnymi standardami bezpieczeństwa danych klientów. Niektóre z powszechnie używanych plomb bezpieczeństwa obejmują certyfikaty SSL SiteSafe, TRUSTe, McAfee SECURE i WhiteHat Security Certification.

**Ceny dynamiczne**

Jedną z kontrowersyjnych technik, którą badały niektóre firmy, jest dynamiczna wycena. Ceny dynamiczne przedstawiają różne ceny różnym klientom. Budując profil nawyków zakupowych konkretnego klienta, sprzedawcy mogą zawyżać ceny dla osób, które wydają się być bardziej skłonne do kupowania droższych towarów i obniżać ceny dla tych, którzy zwracają uwagę na koszty. Wiele sklepów stacjonarnych robi to samo, ponieważ sklepy w niektórych częściach miasta mogą obsługiwać

bogatszych ludzi niż w innych obszarach; podobnie udokumentowano, że niektóre sieci sklepów nakładają wyższe ceny na biednych ludzi w gettach niż na przedmieściach, po części dlatego, że w biednych dzielnicach jest mniejsza konkurencja, a koszty prowadzenia działalności mogą być tam wyższe. Inny rodzaj dynamicznych cen występuje w branży lotniczej, gdzie ceny miejsc w samolotach różnią się w zależności od tego, kiedy są rezerwowane i ile miejsc ma zostać sprzedanych. Jednak w przeciwieństwie do tych przykładów, dynamiczne ustalanie cen w Internecie przypomina tradycyjną sprzedaż samochodów, gdzie badania potwierdzają, że kobietom i mniejszościom rasowym konsekwentnie oferowane są wyższe ceny niż oferty dla białych mężczyzn. Zarówno w przypadku sprzedaży samochodów, jak i dynamicznego ustalania cen w sieci, zasadnicza różnica w porównaniu z normalnym modelem wolnorynkowym polega na tym, że ceny są różnicowane potajemnie, tak że oferowaną cenę widzi tylko ofiara drapieżnej polityki cenowej. Bez mechanizmów wymiany informacji między kupującymi, wydaje się, że ten model ustalania cen stawia kupujących w bardzo niekorzystnej sytuacji w stosunku do sprzedającego. Ciekawe będzie obserwowanie, jak to się rozwinie w czasie.

**Prywatność**

Innym kluczowym obszarem zainteresowania przy zakupie produktów w sieci jest prywatność. Wielu konsumentów woli, aby ich nawyki zakupowe pozostały ich własną działalnością. Otrzymywanie niechcianej poczty papierowej lub e-maila z powodu wcześniejszych zakupów wydaje się im uciążliwe i irytujące; klasyfikują wszystkie takie promocje jako niechcianą pocztę. Inni konsumenci doceniają wygodę otrzymywania ukierunkowanych informacji o nowych produktach i specjalnych cenach wyprzedaży na produkty, które wcześniej kupili. W obu przypadkach ważne jest, aby zwracać uwagę na politykę prywatności oferowaną przez dostawców internetowych. Marketerzy muszą zdecydować, czy skonfigurować swoje systemy na zasadzie opt-in, czy opt-out. Jeśli marketerzy wybiorą to pierwsze, wówczas wszystkie osoby muszą w rzeczywistości zgodzić się na umieszczenie informacji o sobie na listach, które mogą być wykorzystywane w organizacji lub sprzedawane stronom trzecim lub wymieniane z nimi. Jeśli system jest skonfigurowany do rezygnacji, wówczas dane wszystkich mogą być swobodnie ujawniane, z wyjątkiem osób, które wyraźnie oświadczą, że nie chcą, aby administratorzy list to robili. Są to ogólne zarysy; polityka prywatności każdej organizacji musi być szczegółowo opisana. Niektóre witryny, takie jak księgarnie internetowe i serwisy muzyczne, mogą przechowywać szczegółowe informacje o tym, co każda osoba w nich kupuje, a nawet jakie pozycje są po prostu przeglądane. Strony te mogą następnie dostosowywać swoje prezentacje handlowe do produktów, które są odpowiednie dla zainteresowań każdego klienta. Amazon.com, na przykład, stara się być pomocnym odwiedzającym, sugerując książki, które mogą zainteresować powracającego gościa na podstawie jego wcześniejszego zachowania. Jednak jedną z nieoczekiwanych konsekwencji profilowania klientów jest to, że praktyka może ujawnić więcej, niż życzyliby sobie użytkownicy; jeśli zobaczysz, jak jeden z twoich pracowników wchodzi na taką witrynę i odkryje, że dominującym tematem jest, powiedzmy, broń i techniki terrorystyczne, możesz chcieć odbyć poważne dyskusje z personelem działu kadr. Ale pozytywne zastosowanie profilowania wywołało lawinę zainteresowanie, gdy informacje o zwyczajach zakupowych pracowników konkretnych firm zostały przypadkowo udostępnione konkurentom tych firm. Inna kwestia często poruszana w dyskusjach na temat prywatności dotyczy plików cookie. Pliki cookie to małe pliki tekstowe, które witryna przechowuje na dysku twardym odwiedzającego w celu przechowywania informacji, które można wykorzystać przy następnej wizycie użytkownika w witrynie. Prawidłowo zdefiniowane pliki cookie mogą być używane tylko przez witrynę, która je umieściła. Przechowywane informacje mogą obejmować sekwencję stron internetowych, które odwiedził odwiedzający, lub osobiste identyfikatory, które pozwalają oprogramowaniu internetowemu rozpoznać odwiedzającego, dzięki czemu Witryna internetowa może zbudować profil preferencji dla każdego odwiedzającego lub klienta i umożliwić te radosne powitania, takie jak „Witamy z powrotem , Bob! Mamy dla Ciebie specjalną ofertę na najnowszy tytuł z serii The

Real Man's Guide to Heavy Artillery!" Pliki cookie mogą być również wykorzystywane do gromadzenia pozycji w koszyku; bez plików cookie każdy zakup musiałby być realizowany oddzielnie. Zasadniczo pliki cookie są nieszkodliwe. Jeśli nie podoba Ci się pomysł przechowywania identyfikatorów w Twoim systemie, możesz zablokować pliki cookie w ustawieniach przeglądarki, zablokować je globalnie lub na poziomie poszczególnych witryn za pomocą osobistej zapory ogniowej lub zainstalować programy do usuwania plików cookie, które usuwają wszystkie pliki cookie za każdym razem, gdy je aktywujesz.

**Aukcje internetowe**

Teoria stojąca za aukcją polega na tym, że rywalizacja o przedmiot lub usługę pomaga uczestnikom ustalić uczciwą cenę. Proces ten może zostać zakłócony w rzeczywistej, fizycznej aukcji, jeśli sprzedawca spiskuje z konfederatami, aby sztucznie podnieść cenę. Niestety, jest to jeszcze łatwiejsze w Internecie, gdzie każdy może mieć tyle tożsamości, ile chce. Łatwość, z jaką przeglądarki i systemy poczty e-mail pozwalają na sfałszowane nagłówki i sfałszowane identyfikatory, oznacza, że sprzedawcy mogą zawyżać ceny swoich własnych ofert. Federalna Komisja Handlu Stanów Zjednoczonych informuje, że aukcje internetowe powodują największą liczbę otrzymywanych corocznie skarg dotyczących oszustw. Ta teoretyczna dyskusja nawet nie zaczyna odnosić się do takich pytań, jak to, czy wylicytowane przedmioty naprawdę istnieją, są zgodne z opisem i czy kiedykolwiek zostaną dostarczone. Przypadek takiego oszustwa miał miejsce w serwisie eBay, gdzie Robert Guest z Los Angeles przyznał się w sądzie w lipcu 1999 r., Że oszukał ofiary na około 37 000 USD, oferując towary na aukcję za pośrednictwem serwisu eBay, ale niczego nie dostarczył. Klienci Pana Gościa z pewnością przekonali się na własnej skórze, że są oszukiwani, ale wygląda na to, że nie mogli wiedzieć z góry, że był niegodny zaufania. Chociaż eBay utrzymuje system, w którym potencjalni licytanci mogą zobaczyć recenzje i komentarze zamieszczone przez wcześniejszych klientów każdego sprzedającego, nowi sprzedawcy, tacy jak Pan Gość, nie mają żadnych danych, a każdy, kto ma złą historię, może przyjąć nową tożsamość. Serwis eBay odpowiedział na te obawy, sugerując korzystanie z usług depozytowych i ostrzegając swoich użytkowników, że nie gwarantuje legalności transakcji, które ułatwia. Istnieją również obawy co do legalności niektórych przedmiotów wystawionych na aukcję. Ktoś oferował przedmioty wykonane z zagrożonych gatunków, z naruszeniem Konwencji o międzynarodowym handlu zagrożonymi gatunkami (CITES). Wśród produktów znalazły się wysuszone łapy słoni i goryli złapanych we wnyki, którym pozwolono umrzeć w straszliwej śmierci, zanim zostały posiekane na kawałki. W Stanach Zjednoczonych kupowanie, sprzedawanie i posiadanie takiej kontrabandy może prowadzić do aresztowania, oskarżenia, grzywny lub pozbawienia wolności. Co bardziej absurdalne, we wrześniu 1999 roku ktoś wystawił ludzką nerkę na eBayu i otrzymał oferty o wartości do 5,8 miliona dolarów. Serwis aukcyjny anulował sprzedaż, ponieważ sprzedaż ludzkich narządów jest przestępstwem federalnym, za które grozi grzywna w wysokości do 250 000 USD i co najmniej pięć lat więzienia. Tydzień później eBay musiał zamknąć aukcję nienarodzonego dziecka. Ceny rzekomego dziecka wzrosły do 100 000 $, zanim eBay zamknął tę aukcję. Wreszcie głupiec lub żartowniś – nie jest jasne, który – próbował sprzedać 500 funtów świeżej marihuany online. Aukcja została zamknięta po 21 godzinach, podczas których oferowane ceny osiągnęły 10 milionów dolarów. W sierpniu 2001 roku pewna para zaproponowała, że nada dziecku imię zgodnie z życzeniem licytanta, który zaoferował najwyższą cenę. Ta aukcja również została zakończona przedwcześnie. Większość ofert prawdopodobnie nie była uzasadniona. Jest mało prawdopodobne, aby każdy, kto licytował nerki, trawkę i dzieci, naprawdę spodziewał się, że zapłaci za to, o co licytował. Być może traktowali aukcję jak grę wideo, bez elementu rzeczywistości. Sytuacje takie jak ta zachęcają do innych nadużyć, a zwykli użytkownicy często nie wiedzą, co z nimi zrobić i jak postępować. Nawet jeśli przedmioty oferowane do sprzedaży online to zwykłe rzeczy, takie jak oprogramowanie lub produkty fizyczne, mogły zostać uzyskane nielegalnie. Aukcje internetowe są często wykorzystywanym kanałem obrony skradzionych towarów. Użytkownicy korporacyjni prawdopodobnie nie powinni używać aukcji internetowych do kupowania lub

sprzedawania produktów, z wyjątkiem ściśle strzeżonych, branżowych witryn, które dowiodły swojej wartości. Z pewnością pracownicy nie powinni wykorzystywać korporacyjnego dostępu do Internetu do angażowania się w takie działania w celach prywatnych.

**Hazard online**

Trudno sobie wyobrazić, aby jakiekolwiek przedsiębiorstwo zezwalało pracownikom na uprawianie hazardu online przy użyciu zasobów korporacyjnych, ale przekazanie pracownikom następujących wskazówek może być cenną usługą.

**Oszustwo i błąd**

W 1998 roku loteria w Arizonie odkryła, że żadna zwycięska liczba w jej grze Pick 3 nigdy nie zawierała nawet jednej cyfry 9.9. Okazało się, że algorytm generatora liczb pseudolosowych miał elementarny błąd programistyczny, który generował tylko cyfry od 0 do 8. Wszyscy, którzy mieli użyli 9 w swoich liczbach na loterii, odczuwali uzasadnioną złość – zwłaszcza, gdy powiedziano im, że mogą otrzymać zwrot pieniędzy, ale tylko pod warunkiem, że zatrzymali swoje stare przegrane kupony. Loteria w Arizonie wykorzystała symulowany losowy proces, aby dać graczom złudzenie, że obstawiają proces fizyczny, taki jak mieszanie się kulek w beczce i wypadanie z tuby. Jeden z problemów z symulacją w Arizonie jest podobny do prawdziwej luki w zastrzeżonych (tj. tajnych) algorytmach kryptograficznych. Jak kryptografowie podkreślali przez wiele dziesięcioleci, bezpieczeństwo schematu szyfrowania nie powinno zależeć od tajności jego algorytmu. Gdyby algorytm loterii został wystawiony na publiczną kontrolę, jego wady zostałyby wykryte wcześniej. Na przykład w latach 80. XX wieku było wiele emocji związanych z nowym schematem szyfrowania zwanym algorytmem plecakowym; po szeroko zakrojonych badaniach przeprowadzonych przez kryptografów okazało się, że jest wadliwy. Można sobie wyobrazić, że ktoś, kto wykrył lukę w loterii w Arizonie, mógł postawić zakłady z większym prawdopodobieństwem wygranej niż osoby niedoinformowane, ale wystawienie algorytmu i jego implementacji na kontrolę, zanim wszedł do produkcji, zmniejszyłoby to prawdopodobieństwo. Te przykłady pokazują, że hazard elektroniczny, podobnie jak starsze, konwencjonalne typy, podlega nie tylko regułom przypadku. Brak zgodności z dobrymi praktykami w zakresie bezpieczeństwa naraża zarówno gracza, jak i kasyno na nadużycia i nieumyślne błędy.

**Brak kontroli**

Fizyczne urządzenia do gier znajdują się w rzeczywistych placówkach pod nominalną kontrolą urzędników regulacyjnych i organów ścigania. Mimo to zawsze są one dostosowywane do określonej z góry ustalonej wypłaty. Gry hazardowe oparte na wynikach rzeczywistych wydarzeń sportowych lub zawodów są potwierdzane przez zewnętrzne doniesienia prasowe, chociaż same zawody mogą być sfałszowane. Ale nie ma podstaw, aby hazardzista ufał wynikom wygenerowanych komputerowo liczb pseudolosowych wyświetlanych na ekranie przeglądarki. Większość indywidualnych graczy nigdy się nie dowie, czy długoterminowa analiza liczb pseudolosowych potwierdzi ich nadzieje na uczciwość szans. Nikt nie śledzi tych danych oprócz osób zarabiających pieniądze na uczestnikach i nie rozpowszechnia wyników. Zastrzeżenie na jednym z internetowych portali hazardowych, findinternetcasino.com, nie jest zbyt zachęcające:

Chociaż dołożono wszelkich starań, aby zapewnić graczowi uczciwość i bezpieczeństwo na każdym z linków, które można znaleźć w katalogach, FindInternetCASINO R nie ponosi odpowiedzialności, jeśli wystąpią rozbieżności między operacjami związanymi z hazardem online a tobą, graczem, po wykonaniu link z tej strony WWW. Skonsultuj się z lokalnymi władzami przed zarejestrowaniem się w jakiejkolwiek usłudze zakładów online. Obywatele USA: Informacje na tej stronie służą wyłącznie do

celów rozrywkowych i informacyjnych. Wykorzystywanie tych informacji z naruszeniem jakichkolwiek przepisów federalnych, stanowych lub lokalnych jest zabronione.

**Zagadnienia prawne**

W niektórych jurysdykcjach obstawianie online jest nielegalne. Na przykład w Stanach Zjednoczonych używanie łączności międzystanowej do obstawiania zakładów jest już nielegalne; ponadto zakłady internetowe są nielegalne w Stanach Zjednoczonych, nawet jeśli gospodarz znajduje się poza Stanami Zjednoczonymi. Jednocześnie, ze względu na niejasności w obowiązujących przepisach i niemożność ich jasnego egzekwowania, korzystanie z zagranicznych serwisów bukmacherskich doprowadziło ten biznes do łącznie ponad 15,5 miliarda dolarów rocznie, z czego ponad połowa pochodzi ze Stanów Zjednoczonych . Niejasności wynikają z braku jasnej definicji nielegalnego hazardu online. Spowodowało to, że niektóre grupy osób uważały, że są zwolnione z prawa, a pokerzyści byli najpowszechniejsi. Ponadto wyścigi konne online są objęte szczególnymi wyjątkami od prawa, ale bez towarzyszącego im wyjaśnienia, czy proces obstawiania stanowi hazard online. Niestety w Wielkiej Brytanii i wielu innych krajach hazard online jest w większości legalny. Powoduje to liczne konflikty interesów i międzynarodowe napięcia między różnymi firmami bukmacherskimi w zalegalizowanych krajach, a wszystkie reklamy skierowane są do Amerykanów, którzy chcą zaryzykować swoje pieniądze, aby mieć szansę na dużą wypłatę. Wydaje się, że dopóki w prawie nie zostaną zawarte jasne definicje, zacierająca się granica między legalną i nielegalną działalnością hazardową z wykorzystaniem zasobów internetowych będzie się utrzymywać.

**Uzależnienie od Internetu**

Podstawą kompulsywnej przesady może stać się każda czynność. Niewielka część, około 5 procent, użytkowników Internetu może kwalifikować się jako uzależniony od którejkolwiek z tych czynności, w których pośredniczy komputer:

* Niepohamowane pragnienie znalezienia i uporządkowania coraz większej ilości informacji na ogromny zakres tematów

* Nadmierne zaangażowanie w gry, hazard i kupowanie rzeczy w Internecie

* Nadmierna koncentracja na relacjach za pośrednictwem poczty elektronicznej i czatów ze szkodą dla relacji w prawdziwym życiu

* Zaangażowanie w długie sesje oglądania pornografii lub stymulacji seksualnej za pośrednictwem poczty elektronicznej, czatów, stron pornograficznych lub gier z fantazjami seksualnymi

Żadna z tych czynności nie stanowi odpowiedniego wykorzystania korporacyjnych zasobów komputerowych, a pracowników należy ostrzec o zasadach zabraniających takich czynności w pracy. Ponadto każdy powinien być świadomy niebezpieczeństw związanych z uzależnieniem od Internetu. Problem polega na tym, co stanowi nadmierne zaangażowanie w te działania. Profesjonalni psychologowie, tacy jak dr Kimberly Young, zidentyfikowali niektóre kryteria diagnostyczne tych zaburzeń, w tym te oparte na jej teście uzależnienia od Internetu:

* Regularnie przebywasz online dłużej niż zamierzałeś

* Często zaniedbując obowiązki spędzania większej ilości czasu online

* Konsekwentne preferowanie spędzania czasu online zamiast ze swoim partnerem

* Częste skargi przyjaciół i rodziny na nadmierne korzystanie z Internetu

* Cierpienie konsekwencji w szkole lub w pracy z powodu czasu spędzonego online

* Nadawanie e-mailom wyższego priorytetu niż inne ważne kwestie

* Ukrywanie zakresu korzystania z Internetu

* Zwrócenie się do Internetu jako substytutu radzenia sobie z niepokojącymi problemami

* Poczucie, że życie bez Internetu byłoby pozbawione sensu i przyjemności

* Denerwuje się, gdy ktoś przeszkadza podczas korzystania z Internetu

* Utrata snu z powodu nocnej aktywności w Internecie

* Tęsknota za powrotem do trybu online

Ci, którzy czują się niekomfortowo z powodu swojego zaangażowania w Internet, powinni wykonać ten test zaproponowany przez dr Younga, a jeśli kilka z ich odpowiedzi jest pozytywnych, zasięgnąć porady, aby zapobiec potencjalnie tragicznym skutkom nieleczonego uzależnienia.

**Randki online i cyberseks**

Podobnie jak w innych tematach , jest mało prawdopodobne, aby polityka korporacyjna pozwalała użytkownikom na angażowanie się w randki online i cyberseks. Niemniej jednak, zgodnie z ogólną orientacją , kolejne sekcje pomogą pracownikom zrozumieć problemy związane z tymi działaniami online.

**Randki online**

Tysiące witryn w sieci specjalizuje się w pomaganiu ludziom w poznawaniu się. W pewnym sensie czaty i systemy tablic ogłoszeń są dla ludzi o podobnych zainteresowaniach sposobami komunikowania się na temat ich hobby i stylu życia. Istnieją również witryny, które specjalizują się w pomaganiu ludziom w znajdowaniu osób pasujących do określonych profili. Niektóre z tych witryn są bezpłatne; inne pobierają opłaty za uczestnictwo. Serwisy randkowe zwykle wyraźnie ograniczają uczestnictwo do osób powyżej 18 roku życia, a większość z nich opiera się na posiadaniu karty kredytowej jako jedynym mechanizmie uwierzytelniania wieku. Bardzo trudno jest wykluczyć nastolatków, a nawet młodsze dzieci, z takich witryn, jeśli mają one dostęp do numerów kart kredytowych. Rodzice, nauczyciele i pracodawcy, którzy chcą wiedzieć, co się dzieje, mogą wpisać „randki online" w polu wyszukiwania wyszukiwarki, takiej jak Google (www.google.com), a następnie odwiedzić kilka witryn. Jeśli dzieci zamieszczają informacje o sobie w takiej lokalizacji cyberprzestrzeni, nawet z fałszywymi informacjami twierdzącymi, że są dorosłymi, istnieje realne ryzyko przyciągnięcia niesmacznych postaci lub być może zwykłych ludzi, którzy mogą się rozgniewać, że dali się nakłonić do ujawnienia swoich uczuć oszustowi.

**Rozmowy o seksie online**

Oprócz matchmakingu, użytkownicy Internetu mogą również zaangażować się w cyberseks. Osoby rozmawiające online mogą opisywać siebie lub innych w interakcjach seksualnych, które są nieodpowiednie dla młodzieży. Taki czat online był również zamieszany w wiele rozwodów, ponieważ wielu małżonków uważa za całkowicie niewłaściwe, że ich ukochany podnieca się seksualnie z nieznajomym przez Internet. W sierpniu 2001 roku 15-letnia dziewczyna z Massachusetts była rzekomo przetrzymywana w niewoli przez co najmniej tydzień, podczas którego była wielokrotnie wykorzystywana seksualnie przez parę, która przywiozła ją na Long Island. Według zawiadomienia o popełnieniu przestępstwa była również wypożyczana na dwa dni innemu mężczyźnie i dalej maltretowana. Para poznała nastolatka na czacie internetowym, gdzie ich rozmowa była wyraźnie

seksualna. W środowisku pracy rozpowszechnianie wiadomości o charakterze seksualnym lub jawnej pornografii może być słusznie postrzegane i opisywane jako sprzyjanie wrogiemu środowisku pracy i może prowadzić do procesów sądowych ze strony pracowników, których to dotyczy. Pracodawcy powinni ogłosić zasady zapobiegania takim nadużyciom i monitorować korporacyjną pocztę e-mail i komunikatory internetowe, aby upewnić się, że nikt z ich pracowników nie angażuje się w te działania przy użyciu zasobów korporacyjnych.

**Ruch kobiet**

Na wielu stronach internetowych, zwłaszcza na terenach byłego bloku sowieckiego, reklamowane są usługi polegające na przedstawianiu mężczyzn chętnym kandydatkom do małżeństwa. Dowody są mocne, że wiele informacji przekazywanych o kobietach rzekomo dojrzałych i zorientowanych na małżeństwo jest fałszywych. Wiele zdjęć pochodzi z publicznych stron internetowych i przedstawia aktorki oraz osoby, które opublikowały swoje zdjęcia w grupach społecznościowych. Czasami ten sam obraz ma dziesiątki nazw. Podobnie jak w przypadku telefonicznych serwisów z seksem, osoby podające się za młodych, atrakcyjnych, w wieku małżeńskim mogą być nikim takim i mogą kopiować/wklejać odpowiedzi z przygotowanych scenariuszy. Kiedy mężczyźni podróżują, aby odwiedzić swoje potencjalne partnerki, mogą zostać obciążeni wysokimi opłatami za przywilej zabierania ich na randki do drogich restauracji. Niektóre kobiety, które faktycznie zawierają małżeństwa, później rozwodzą się ze swoimi nieszczęsnymi ofiarami, gdy zostają one przyjęte do kraju zamieszkania męża w ramach czegoś, co wydaje się być systematycznym oszustwem.

**Gry i rzeczywistość wirtualna**

Niektóre przedsiębiorstwa pozwalają swoim pracownikom na granie w gry o różnych porach dnia — zazwyczaj w porach, w których nie korzysta się z nich, takich jak lunch lub przed i po normalnym dniu pracy. Jednak niektóre gry dla wielu użytkowników z obsługą Internetu mogą zużywać ogromną przepustowość; gra typu shoot-'em-up (strzelanka z perspektywy pierwszej osoby lub FPS) o nazwie Quake była znana w swoim czasie z nasycania całej dostępnej łączności. Kiedy pomagasz pracownikom zrozumieć, jak negocjować niebezpieczeństwa związane z Internetem, możesz zalecić rodzicom przeczytanie recenzji gier wideo, zanim pozwolą swoim dzieciom w nie grać. Niektóre gry mają zdumiewający poziom graficznej przemocy („Genialne krwawienie! Szczegółowe dekapitacje!”) i niezwykłe wartości („Zdobądź punkty, spalając jak najwięcej mieszkańców!”). Ten ostatni przykład opiera się na głośnym przypadku, w którym sprzedawca gier wideo był najwyraźniej zaskoczony publiczną falą wstrętu do gry, która gloryfikowała podpalenie. Niektóre strzelanki wojskowe i policyjne wyraźnie odbierają punkty za trafienie niewinnych przechodniów; inni nie. Niektóre gry wykorzystują graficzną nagość; inni są skromniejsi. Najważniejsze jest to, że poleganie na osądzie ośmiolatków przy wyborze własnej rozrywki może być nierozsądne. Z perspektywy korporacyjnej byłoby czymś niezwykłym znaleźć pracodawców zachęcających do korzystania z gier lokalnych lub sieciowych w godzinach pracy; jednak niektórzy mogą zezwolić na korzystanie ze swoich zasobów poza godzinami pracy, zakładając, że korporacja nie prowadzi operacji całodobowych. Jednak nadal istnieją problemy z przydatnością; niektóre gry mogą przyczyniać się do powstania wrogiego środowiska pracy i prowadzić do skarg i pozwów ze strony urażonych pracowników. Rozwój, który rozpoczął się w latach 90., stał się potencjalnie cennym narzędziem w pierwszych dekadach XXI wieku: wirtualna rzeczywistość lub wirtualne światy, takie jak Second Life (http://secondlife.com). Usługi te wykorzystują kontrolowane reprezentacje zwane awatarami, które umożliwiają pewien stopień ekspresji podczas komunikacji. Uczestnicy widzą reprezentację trójwymiarowego świata wraz z punktem widzenia i perspektywą, który obejmuje ich rozmówców we wspólnej wirtualnej rzeczywistości, która może być kreatywna i zabawna. Niektóre firmy wykorzystują zasoby tych wirtualnych światów do reklamy, świadczenia usług (np. szkoleń i edukacji) oraz wewnętrznych

zdalnych spotkań lub szkoleń. Organizacje muszą określić odpowiednie zasady dotyczące korzystania z takich usług.

**Zmiana adresów e-mail**

Pracownicy mogą odejść z firmy, zmienić jednostkę organizacyjną lub zmienić swoje nazwisko. Wszystkie te zmiany mogą skutkować powstaniem nowych adresów e-mail. Niewłaściwa obsługa takich zmian może prowadzić do problemów. Jedną z reakcji na taką zmianę jest usunięcie pierwotnego adresu e-mail bez powiadamiania kogokolwiek. Wiadomość e-mail wysłana na oryginalny adres jest zwracana z błędem niedostarczenia (brak takiego użytkownika). Nadawca musi następnie dowiedzieć się, co się stało — lub może po prostu całkowicie przerwać połączenie, prawdopodobnie tracąc firmę jako klienta lub niedostarczając ważnych informacji. Jeśli zniknięcie adresu e-mail jest spowodowane zmianą nazwiska użytkownika (na przykład w wyniku małżeństwa lub rozwodu), możliwe jest nawet usunięcie pierwotnej nazwy z firmowego katalogu, co utrudni korespondentom nieświadomym nowej nazwy w ogóle skontaktować się z tą osobą przez e-mail lub telefon. Rozsądniejszą reakcją na taką zmianę jest automatyczne przekazywanie poczty przychodzącej na właściwy adres. Na przykład, jeśli oryginalny adres e-mail Farida Hallingsa brzmiał fhallings@company.com, a teraz to fmalteso@company.com, każda poczta wysłana na pierwszy adres automatycznie trafiłaby do skrzynki pocztowej dla drugiego adresu. Jeśli Farid w ogóle nie pracuje już dla firmy, wiadomość e-mail może zostać przekazana na odpowiedni adres zastępcy. Takie przekazywanie może być utrzymane przez dowolny okres, który wydaje się odpowiedni. Oprócz automatycznego przekazywania pomocne może być wysyłanie automatycznych powiadomień do nadawcy nieaktualnego e-maila. „Nowy adres e-mail Farida Hallinga to fmalteso@company.com; Twoja wiadomość została automatycznie przekazana. Proszę zanotować zmianę w swojej książce adresowej e-mail."

**ODPOWIEDZIALNOŚĆ PRAWNA**

**Zniesławienie**.

Niektórzy skorzystali z wolności publikowania wszystkiego, co chcą, przekraczając granice zniesławienia. Na przykład samozwańczy reporter Matt Drudge posunął się za daleko w swoich wpisach na swoim elektronicznym arkuszu skandali w 1997 roku, kiedy wysunął bezpodstawne oskarżenia dotyczące małżeństwa doradcy Białego Domu Sidneya Blumenthala. Zawodowi dziennikarze rzucili się na niego za tandetne dziennikarstwo. Blumenthal i jego żona złożyli przeciwko Drudge pozew o zniesławienie o wartości 30 milionów dolarów, nawet po tym, jak przeprosił za to, że nie zweryfikował plotek, które rozpowszechniał. Drudge następnie stwierdził, że publiczne poparcie Białego Domu dla Blumenthala stanowiło zagrożenie dla wolności słowa. W innym głośnym przypadku Walter Cronkite, którego sondaże wykazały, że był najbardziej szanowanym człowiekiem w Stanach Zjednoczonych w latach 80., był zbulwersowany, gdy w 1997 r. odkrył w Internecie stronę zawierającą kłamstwa na jego temat. Hughes wymyślił i opublikował obelżywą historię o tym, jak Cronkite wpada w furię na autora, wykrzykując przekleństwa pod adresem Hughesa i jego żony, przechwalając się własną niewiernością i plując w ich cieście korzennym w restauracji na Florydzie. Ponadto strona anty-CronkiteWeb zawierała sfałszowane zdjęcia rzekomo przedstawiające Cronkite na spotkaniu Ku Klux Klanu. Cronkite zagroził pozwem o zniesławienie; Hughes zdjął stronę i słabo zaprotestował, twierdząc, że to wszystko żart. Wpływ tego rodzaju dezinformacji na dzieci lub niedojrzałych pracowników, nieprzeszkolonych w krytycznym myśleniu i pozbawionych sceptycyzmu wobec informacji w Internecie, może być szkodliwy. Innym źródłem informacji jest Usenet — zbiór tysięcy grup dyskusyjnych na każdy możliwy temat. Te grupy dyskusyjne dzielą się na dwie główne klasy: moderowane i niemoderowane. W grupie moderowanej wiadomości są przekazywane przez moderatora, który decyduje o opublikowaniu ich dla uczestników lub usunięciu obraźliwych lub w inny sposób nieodpowiednich wiadomości. Nie wszystkie

grupy moderowane są wiarygodne i nie wszystkie grupy niemoderowane są zawodne. Jednak wiele niemoderowanych grup rozpowszechnia niepotwierdzone informacje od ludzi, którzy wydają się czerpać największą przyjemność z życia z obrażania innych uczestników i wygłaszania oburzających wypowiedzi na każdy poruszany temat. Każdy powinien zostać przeszkolony w rozpoznawaniu emocjonalnego i podżegającego języka oraz powinien być zachęcany do stosowania sceptycznej analizy do wszystkich stwierdzeń, zwłaszcza tych publikowanych w tyradach. W pierwszych dekadach XXI wieku blogi – komentarze publikowane w sieci przez osoby lub grupy – eksplodowały w powszechnej świadomości. Te same zasady krytycznej oceny mają zastosowanie do blogów, jak do każdego innego źródła informacji bez pośrednictwa. W jednym przypadku dotyczącym autora Kabay, szaleńcza strona konspiracyjna nielegalnie opublikowała cały tekst jednej z jego kolumn opisujących InfraGard ze zdjęciami ofiar nazistowskich okrucieństw w obozach koncentracyjnych pomiędzy każdym akapitem. Żądanie usunięcia treści na mocy ustawy Digital Millennium Copyright Act (DMCA) zostało spełnione, ale incydent był dla autora obrzydliwy.

**Skradzione oprogramowanie, muzyka i filmy**

Organizacje nie mogą zezwalać pracownikom na pobieranie i wykonywanie nielegalnych kopii jakiejkolwiek własności intelektualnej. Zasady bezpieczeństwa muszą wyraźnie odnosić się do tych kwestii; monitorowanie bezpieczeństwa musi wyraźnie kontrolować nadużycia zasobów korporacyjnych w takich działaniach. Zagrożenia dla organizacji wynikające z tolerowania takich naruszeń prawa są poważne.

**Plagiat**

Inny rodzaj oszustwa związanego z własnością intelektualną ma miejsce, gdy ludzie fałszywie przedstawiają czyjąś pracę jako własną. Starsi uczniowie wiedzą intelektualnie, że to ma być złe, ale dla małych dzieci problem jest całkowicie abstrakcyjny. Dzisiejszy problem polega na tym, że plagiat jest łatwiejszy niż kiedykolwiek i trudniejszy do wykrycia przez nauczycieli. Wytyczne akademickie starają się wyjaśnić studentom, że kopiowanie pracy innych osób bez podania źródła nazywa się plagiatem i jest bardzo mile widziane. Plagiat obejmuje nie tylko bezpośrednie cytowanie bez wskazania pochodzenia, ale także parafrazę, która jedynie trochę miesza myśli lub zastępuje oryginalne słowa synonimami. W wielu instytucjach plagiat jest podstawą zawieszenia lub wydalenia. We wszystkich przypadkach plagiat mija się z celem pisania zadań, eliminując możliwość krytycznego myślenia i twórczej ekspresji. Niewielu plagiatorów pamięta, co skopiowali od innych po oddaniu materiału. Z pewnością studenci od wieków wymieniają się pracami semestralnymi i innymi zadaniami. Jednak dostępność dokumentów elektronicznych i sieci World Wide Web ogromnie zwiększyła zarówno zasoby materiałów, które można splagiatować, jak i łatwość kopiowania. Co gorsza, niektórzy ludzie czerpią korzyści z łatwej dostępności, sprzedając artykuły przeznaczone specjalnie do plagiatu, a nawet pisząc artykuły na zamówienie. W jednym z badań przeprowadzonych przez Peggy Bates i Margaret Fain z Biblioteki Kimbel na Uniwersytecie Coastal Carolina, autorzy z łatwością zlokalizowali ponad 100 witryn internetowych sprzedających lub przekazujących studentom prace za plagiat. Aby zwalczyć ten problem, nauka przyszła z pomocą oblężonym instruktorom, zapewniając automatyczną analizę podobieństw każdego artykułu przesłanego drogą elektroniczną. System korzysta z banku ponad 100 000 prac semestralnych i esejów, a także dokumentów znajdujących się w Internecie; analiza wykorzystuje rozpoznawanie wzorców do pomiaru podobieństw między różnymi dokumentami i oszacowania prawdopodobieństwa plagiatu. Zgodnie z dokumentacją turnitin.com:

Nasz system jest obecnie używany na większości uniwersytetów w Stanach Zjednoczonych i Wielkiej Brytanii, a także w wielu szkołach na całym świecie. Wiele z tych instytucji, w tym UC Berkeley i pięćdziesiąt osiem szkół członkowskich Consortium of Liberal Arts Colleges, stowarzyszenia najbardziej

szanowanych szkół sztuk wyzwolonych w Stanach Zjednoczonych, zdecydowało się zapewnić uczciwość akademicką wszystkim swoim studentom, wybierając subskrypcji naszej usługi w całej instytucji. Inne uniwersytety, takie jak Harvard i Cornell, zdecydowały się korzystać z naszego systemu na zasadzie wydziału lub pojedynczego instruktora.

Plagiat jest również zagrożeniem dla przedsiębiorstwa; niewłaściwe wykorzystywanie przez pracowników materiałów innych osób lub innych organizacji bez podania źródła może prowadzić do procesów sądowych, zawstydzającego rozgłosu i poważnych kar finansowych. W jednym głośnym przypadku z 2003 r. odkryto, że dokument programowy dotyczący irackich organizacji wywiadowczych rozpowszechniany przez Kancelarię Premiera w Wielkiej Brytanii zawierał duże fragmenty dosłownych materiałów, w tym błędy typograficzne, skopiowane i wklejone bez cudzysłowów i bez wskazania źródła . Praktyczne wskazówki:

* Omów jasno plagiat w pracy, w domu iw szkole.

* Użyj przykładów, aby zilustrować różnicę między plagiatem a legalnym wykorzystaniem pracy innych osób.

* Zachęcaj dzieci do ćwiczenia podsumowywania informacji własnymi słowami.

* Ćwicz pisanie odnośników do cytowanych materiałów.

* Poproś ucznia o przesłanie pracy semestralnej do jednego z serwisów internetowych, które weryfikują oryginalność.

* Omów, w jaki sposób witryny antyplagiatowe analizują dokumenty, aby zmierzyć podobieństwa i pomóc nauczycielom zidentyfikować plagiat.

**Hackowanie przestępcze i haktywizm**

Ważne jest, aby wszyscy pracownicy rozumieli i zgadzali się, że korzystanie z systemów korporacyjnych w celu uzyskania nieautoryzowanego dostępu do komputerów i sieci jest podstawą do zwolnienia i być może wszczęcia postępowania karnego. W szczególności żaden pracownik nie powinien sobie wyobrażać, że testowanie słabych punktów bezpieczeństwa w systemach przedsiębiorstwa bez uprawnień jest wkładem w bezpieczeństwo. Motywacja do działań niezgodnych z prawem nie łagodzi powagi włamania komputerowego. Należy wyraźnie poinformować pracowników, że niezależnie od usprawiedliwienia, żadne naruszenia prawa nie będą tolerowane. Na przykład włamanie się do systemów w innym kraju w celu wsparcia działań wojennych nie jest usprawiedliwione; ani niszczenie stron z pornografią dziecięcą nie jest dobrym pomysłem. Cyberstrażnicy mogą niszczyć dowody potrzebne do ścigania.

**Tworzenie wrogiego środowiska pracy**

W dzisiejszym społeczeństwie istnieje wiele działań i konstrukcji językowych, które osoby określonej rasy, płci, orientacji seksualnej, pochodzenia narodowego, przynależności religijnej lub innych prawnie chronionych cech mogą uznać za obraźliwe. Wszelkiego rodzaju nękanie, w szczególności komentarze lub działania oparte na chronionych cechach, wobec innego pracownika, mogą stworzyć wrogie środowisko pracy. Dwie najczęstsze sytuacje spowodowane wrogim środowiskiem pracy to:

1. Zmniejszenie lub utrata produktywności z powodu nękania fizycznego, słownego lub psychicznego

2. Obniżenie wynagrodzenia, premii, poziomu stanowiska, obowiązków lub innych składników wynagrodzenia ze względu na jedną lub więcej cech prawnie chronionych

Chociaż nie ma formalnych przepisów zakazujących wrogiego środowiska pracy, tytuł VII ustawy o prawach obywatelskich z 1964 r. obejmuje tego typu sytuacje. Przepisy te są napisane w taki sposób, że indywidualny komentarz lub działanie zwykle nie stanowi nękania. Raczej wzorzec częstych, poważnych i wszechobecnych nadużyć może stanowić wrogie środowisko pracy. Ważne jest, aby odróżnić molestowanie quid pro quo, gdzie od pracownika wymaga się tolerowania takiego molestowania w celu utrzymania statusu pracy lub poziomu wynagrodzenia, od wrogiego środowiska pracy. Obie są bardzo poważnymi i potencjalnie nielegalnymi działaniami, ale ta sekcja skupia się na wrogim środowisku. Pracodawcy są prawnie zobowiązani do określenia odpowiednich oczekiwań dotyczących zachowania pracowników oraz do poufnego i szybkiego zbadania każdej skargi pracownika dotyczącej molestowania. Pracownikom przyznaje się pewne zabezpieczenia prawne, takie jak odwet ze strony pracodawcy za wszczęcie alarmu w nieprzyjaznym środowisku jest nielegalne. Kwestie te stają się jeszcze ważniejsze, gdy pojawiają się romanse biurowe. Chociaż wielu pracodawców zabrania parom wspólnej pracy w tym samym dziale, częściowo po to, aby uniknąć wszelkiego postrzegania faworyzowania lub przyszłych przypadków nękania, jeśli romans się nie powiedzie, nadal istnieje możliwość, że romantyczni współpracownicy stworzą wrogie środowisko dla innych. W takim przypadku pracodawcy mają obowiązek określić w polityce, że współpracownicy powinni utrzymywać relacje zawodowe podczas wykonywania obowiązków służbowych. Nawet jeśli dwie osoby mogą uważać, że ich słowa lub czyny są pozornie nieszkodliwe, to postrzeganie innych wokół nich stwarza podstawę do złożenia skargi dotyczącej nękania. Najlepszym rozwiązaniem jest trzymanie życia osobistego poza biurem, co jest trudną, ale odpowiednią rekomendacją dla wszystkich.

**Grupy nienawiści**

Innym źródłem niepokoju pracodawców i rodziców jest łatwa dostępność literatury nienawiści w Internecie. Podżegacze nienawiści w pełni wykorzystali w dużej mierze nieuregulowany charakter sieci, aby rozpowszechniać swoje zgubne wiadomości. Można znaleźć strony internetowe poświęcone nienawiści do każdej możliwej do zidentyfikowania grupy. Rasa, pochodzenie etniczne, religia, płeć, orientacja seksualna, status imigracyjny i ideologia polityczna – wszystko może wywołać nienawiść u podatnych osobowości. Niestety, niektórym grupom nienawiści udało się z powodzeniem rekrutować młodych ludzi przez Internet; publikują propagandę, taką jak pro-nazistowska rewizjonistyczna historia, która może oszukać bezkrytycznych ludzi, aby uwierzyli w ich tyrady. Neo-nazistowskie i rasistowskie grupy skinheadów utworzyły grupy hejt-rockowe, które wykorzystują entuzjazm dzieci do bardzo głośnej muzyki z agresywnymi tekstami. Pracodawcy nie mogą tolerować najmniejszego zaangażowania swoich pracowników w tego typu działania z wykorzystaniem zasobów korporacyjnych. Poza możliwym osobistym wstrętem do takiego szerzenia nienawiści, menedżerowie powinni również mieć świadomość, że tolerowanie nietolerancji może prowadzić do powstania wrogiego środowiska pracy, w którym osoby będące obiektem nienawiści lub pogardy mogą zgodnie z prawem odwoływać się do sądu o odszkodowanie i odszkodowanie. Pracownicy muszą zrozumieć i zaakceptować fakt, że wykorzystywanie zasobów korporacyjnych do udziału w grupach nienawiści stanowi poważne naruszenie zasad korzystania z Internetu. Według Centrum Simona Wiesenthala istnieje ponad 2300 stron internetowych, które promują nienawiść, z których ponad 500 to strony ekstremistyczne hostowane na amerykańskich serwerach, ale autorstwa Europejczyków; w większości krajów europejskich obowiązują surowe przepisy dotyczące nienawiści. Stosując bardziej rygorystyczne kryteria, grupa HateWatch szacuje, że w sieci istnieje ponad 500 ekstremistycznych stron szerzących nienawiść; rozróżnia między propagandą nienawiści a tymi stronami, które składają się głównie z rasistowskich epitetów, odrzucanych jako zwykłe graffiti. Southern Poverty Law Center monitoruje 500 aktywnych organizacji szerzących nienawiść w Stanach Zjednoczonych. Regularnie donosi o rosnącej liczbie i natężeniu takich stron. W komentarzach do artykułu centrum dla Komisji Praw Człowieka ONZ, rzecznik Mark Potok powiedział na konferencji w 2000 roku:

Kilka lat temu członek Klanu musiał włożyć znaczny wysiłek i pieniądze, aby wyprodukować i rozprowadzić tandetną broszurę, która mogła dotrzeć do kilkuset osób. Dzisiaj, mając komputer za 500 dolarów i znikome inne koszty, ten sam członek Klanu może stworzyć zręcznie stworzoną witrynę internetową, która ma milionową potencjalną publiczność.

Fundamentalną rzeczywistością jest to, że istoty ludzkie są towarzyskie. Bardzo łatwo przychodzi im łączenie się z innymi w celu tworzenia grup wewnętrznych, grup, do których czują się uprawnieni przynależeć. Niestety, definiowanie grup wewnętrznych w naturalny sposób oznacza równie łatwe zdefiniowanie grup zewnętrznych: grup, do których nie chcemy należeć. Kliki w szkole podstawowej i liceum są przykładami grup własnych i obcych. Bogactwo badań z zakresu psychologii społecznej potwierdza słuszność powszechnego wrażenia, że mamy tendencję do zawyżania naszego szacunku dla grup własnych i zmniejszania szacunku i sympatii dla grup obcych. Jednak badania pokazują również, że normy społeczne przeciwko dyskryminacji mogą zmniejszyć wrogość wobec grup obcych; wydaje się więc prawdopodobne, że wyartykułowanie przez rodziców i nauczycieli norm tolerancji może znacząco zmniejszyć podatność dzieci na pochlebstwa grup nienawiści.

**Pornografia**

Pornografia – nawet z najbardziej restrykcyjnymi definicjami – jest szeroko rozpowszechniona w Internecie. Obserwatorzy kultury internetowej stwierdzili, że najpewniejszym sposobem na stwierdzenie, czy nowa technologia odniesie sukces w Internecie, jest sprawdzenie, jak szybko mogą ją zastosować twórcy pornografii. Na przykład pojawienie się w lipcu 2000 r. pierwszych witryn z pornografią WAP (protokół aplikacji bezprzewodowych) zasygnalizowało przyjęcie technologii WAP do głównego nurtu. Chociaż strony te oferowały tylko drobne, ziarniste zdjęcia nagich japońskich modelek, socjologowie stwierdzili, że ta sama oczekiwana sekwencja szybkiego postępu technologicznego miała miejsce w przypadku fotografii i kamer wideo.

**Rozpowszechnienie pornografii**

Niektóre badania ruchu internetowego wykazały, że ponad połowa całkowitej przepustowości sieci jest wykorzystywana do przesyłania pornografii lub nakłaniania do zakupu pornografii.

Pornografowie stosują różne sztuczki, aby przyciągnąć ludzi na swoje strony internetowe:

* Korzystanie z innej domeny, takiej jak stara whitehouse.com, która wykorzystywała zainteresowanie „whitehouse.gov" do wyświetlania pornografii (obecnie jest to katalog z kilkoma płatnymi linkami do randek).

* Błędy ortograficzne, takie jak nieaktywna witryna micosoft.com, która opierała się na prawdopodobieństwie błędnego wpisania nazwy „Microsoft.com".

* Wiadomości-śmieci z zaproszeniami z niewinnie wyglądającymi etykietami dla adresów URL, które nie pasują do rzeczywistego linku, ale zamiast tego kierują widza na stronę z pornografią.

* Uzupełnianie metatagów witryn pornograficznych (zwykle niewidoczny tekst używany do opisu witryny) nieszkodliwymi słowami kluczowymi, które umieszczają witrynę wysoko na listach wyszukiwarek, gdzie mogą być atrakcyjne dla dzieci.

* Wyłączanie normalnych funkcji przeglądarki w celu uwięzienia ofiar na stronie pornograficznej. Jeden sprawca, który został zamknięty przez Federalną Komisję Handlu (FTC), faktycznie uruchomił aplety Java, które wyłączyły strzałkę wstecz i uniemożliwiły zamknięcie przeglądarek. Ludzie uwięzieni w porno-piekle musieli zrestartować swoje komputery, aby się wydostać.

Strony pornograficzne są znane z oszustwa w celu oszukania swoich ofiar. Jednym z powszechnie stosowanych oszustw jest żądanie numeru karty kredytowej od odwiedzającego jako dowodu wieku (to nic takiego), a następnie obciążenie karty, mimo że strona wyraźnie informuje, że istnieje okres bezpłatnego użytkowania. W 1996 roku oglądających zdjęcia pornograficzne na stronie sexygirls.com czekała niespodzianka, gdy dostali kolejne rachunki telefoniczne. Ofiary, które pobrały specjalną przeglądarkę, w rzeczywistości instalowały program typu koń trojański, który po cichu rozłączył ich połączenie z normalnym dostawcą usług internetowych i ponownie nawiązał połączenie (z wyłączonym głośnikiem modemu) z numerem w Mołdawii w Europie Środkowej. Następnie opłaty za połączenia długodystansowe rosły, aż użytkownik rozłączył się z sesją — czasami kilka godzin później, nawet gdy ofiary przełączyły się na inne, być może mniej lubieżne strony. Niektóre ofiary, które pozostawały online przez długi czas, zapłaciły ponad 1000 USD opłat za połączenia międzymiastowe. W lutym 1997 roku w Nowym Jorku sędzia federalny nakazał zamknięcie oszustwa. Interesującą informacją jest to, że pracownicy AT&T wykryli oszustwo z powodu niezwykle dużego natężenia ruchu w Mołdawii, która zwykle nie jest celem wielu rozmów telefonicznych w USA. W listopadzie 1997 roku FTC wygrała 2,74 miliona dolarów od mołdawskiej firmy telefonicznej, aby zwrócić oszukanym klientom — lub tym, którzy chcieli przyznać się do tego, że zostali oszukani. Oba opisane powyżej oszustwa polegały częściowo na niechęci ofiar poszukujących pornografii do przyznania się do społecznie odrzuconych zainteresowań. Niewiele ofiar było skłonnych kontynuować tę sprawę, dopóki szkody nie osiągnęły tysięcy dolarów.

**Filtrowanie**

Rozrosła się cała branża próbująca chronić (lub blokować) dzieci przed oglądaniem pornografii lub innych materiałów uznanych za obraźliwe przez ich rodziców lub przez twórców oprogramowania blokującego. Popularne systemy blokowania są piętnowane przez wielu zwolenników wolności słowa i często wyśmiewane z powodu tego, co określa się mianem niezdarnych algorytmów zorientowanych na słowa kluczowe. Klasycznym przykładem niedorzecznego blokowania jest blokowanie dostępu do dowolnej witryny, która używa słowa „pierś", w tym nawet tej samej strony, jeśli czytasz ją w sieci. Inne proste pułapki blokowały użytkownikom dostęp do stron informacyjnych dla lokalizacji geograficznych kończących się starą brytyjską końcówką -sex, takich jak Wessex, Sussex, Middlesex i tak dalej. Wieś Scunthorpe w Anglii została zablokowana przez oprogramowanie używane przez dużego dostawcę usług internetowych, ponieważ jego wewnętrzne filtry uniemożliwiały komukolwiek używanie wulgarnych słów w adresie pocztowym. Niektóre z programów blokujących wykorzystują ukryte założenia dotyczące nieprzydatności szerokiego zakresu tematów, w tym prawa do aborcji, praw obywatelskich, ideologii politycznej i wyzwolenia gejów. Każdy rodzic ma prawo do wyrażania opinii na każdy temat; jednak rodzice będą chcieli sprawdzić, czy dany program nie narzuca ukradkiem politycznego programu swoich twórców. W miejscu pracy pracodawcy korzystający z oprogramowania blokującego szerokie spektrum mogą zakłócać legalne badania prowadzone przez ich pracowników.

**Monitorowanie**

Innym podejściem do ingerencji w nikczemne czyny osób zajmujących się pornografią jest instalowanie oprogramowania monitorującego na komputerach, z których pracownicy korzystają w pracy lub z których dzieci będą korzystać w domu. Produkty te przechowują dziennik lub ścieżkę audytu, która pozwala pracodawcom i rodzicom dokładnie zobaczyć, co użytkownicy robili na swoich komputerach. W kontekście rodzinnym najważniejsza jest jednak zasada, że maszyny i programy same w sobie nie mogą uczyć wartości. Zamiast polegać tylko na pasywnych barierach lub oprogramowaniu typu snoopware, rodzice powinni uczynić surfowanie po Internecie zajęciem rodzinnym, a nie prywatnym hobby. Kiedy dzieci wyrażają zainteresowanie pornografią – ponieważ nasza kultura popularna jest pełna seksualnych insynuacji, które dzieci czytają, słyszą i oglądają – warto omówić te kwestie, zamiast

próbować udawać, że nie istnieją. Jednym ze sposobów zmniejszenia mocy zakazanego owocu oferowanego przez pornografów jest wyjaśnienie dzieciom w wspierający i nie karzący sposób, dlaczego wykorzystywanie seksualne i poniżanie są złe dla ludzi. Dzieci, które przypadkowo trafiły na strony pornograficzne lub w domach swoich przyjaciół, mogą być lepiej przygotowane do radzenia sobie z czasami niepokojącymi obrazami i słowami, jeśli ich rodzice przygotowali je do tego aspektu dzisiejszego świata.

**Archiwizacja wiadomości e-mail**

Organizacje muszą pamiętać, że e-mail może być wymagany jako dowód w sprawach sądowych. Istnieje obowiązek powierniczy dotyczący prowadzenia dokumentacji biznesowej odpowiednio dla każdego rodzaju działalności, a obowiązek ten rozciąga się na dokumentację elektroniczną. Zasady powinny określać, jak długo należy przechowywać zapisy poczty elektronicznej. Niszczenie wiadomości e-mail nigdy nie powinno być selektywne, zwłaszcza jeśli istnieje przewidywana groźba działań prawnych. Selektywne niszczenie określonych akt lub przedwczesne masowe niszczenie poczty elektronicznej może być interpretowane przez sądy jako podstawa do postawienia zarzutów ingerencji w proces sądowy.

**ZALECENIA**

W tej części podsumowano kilka praktycznych zaleceń dla pracowników i ich rodzin. Sformułowanie zasad w sposób, który wspiera troskę pracowników o własne rodziny, jest pomocnym sposobem na zwiększenie postrzeganej wartości wytycznych.

**Ochrona dzieci**

* Wyjaśnij niebezpieczeństwa związane z komunikowaniem się z nieznajomymi za pośrednictwem sieci w taki sam sposób, w jaki omawiasz niebezpieczeństwa związane z rozmawianiem z nieznajomymi gdziekolwiek indziej.

* Ostrzegaj dzieci przed wątpliwą tożsamością każdego, kogo spotkają, wyłącznie za pośrednictwem sieci lub poczty elektronicznej. Omów możliwość, że ludzie nie są tym, za kogo się podają w sieci.

* Ważne jest, aby dzieci miały pewność, że rodzice podejmą odpowiednie kroki, gdy poruszą te kwestie. Stwórz spokojną atmosferę, aby dzieci nie bały się twoich reakcji, jeśli będą zaniepokojone tym, co napotkają w Internecie. Najgorsze byłoby ukaranie dziecka za zgłoszenie niepokojącego incydentu.

* Powiedz dzieciom, aby nie podawały swojego adresu nieznajomym, których poznają drogą elektroniczną.

* Dzieci nie powinny wysyłać swoich zdjęć nieznajomym.

* Wyrób praktykę omawiania relacji online w przyjazny i otwarty sposób w domu. Okazuj zainteresowanie nowym znajomym bez okazywania wrogości lub podejrzliwości; poprosić o udział w niektórych czatach online i korespondencji e-mailowej. Zaproś swoje dzieci, aby siedziały z tobą podczas twoich własnych interakcji online.

* Jeśli dziecko czuje, że inne dziecko poznane w Internecie staje się dobrym przyjacielem, rodzice powinni skontaktować się z rodzicami dziecka telefonicznie i ewentualnie osobiście przed zezwoleniem na kontakty.

* Jeśli dziecko chce poznać kogoś napotkanego w Internecie, upewnij się, że rodzic jest zaangażowany na wszystkich etapach. Nigdy nie pozwól dziecku poznać nikogo w realnym świecie, kogo poznało tylko

w sieci. Wszelkie próby nakłonienia dziecka do samotnego lub potajemnego spotkania z korespondentem należy zgłaszać lokalnym organom policji w celu przeprowadzenia dochodzenia.

* Wyjaśnij, że każdy, kto sugeruje ukrywanie związku online przed rodzicami dziecka, już robi coś złego.

* Wyjaśnij swoim dzieciom, że nikt nie ma prawa wysyłać im materiałów niestosownych do wieku, dwuznacznych seksualnie lub jawnie pornograficznych, zarówno w formie pisemnej, jak i graficznej. Sugestie w Internecie, że dzieci angażują się w wirtualne zabawy seksualne lub fantazje seksualne, należy natychmiast zgłaszać rodzicom. Tworzenie, przesyłanie i przechowywanie pornografii dziecięcej jest przestępstwem; natychmiast zgłaszać takie przypadki lokalnym organom policji.

* Dzieci otrzymujące prośbę o coś nietypowego (np. prośbę o kawałek ubrania lub nagie zdjęcia) powinny natychmiast zgłosić incydent swoim rodzicom. Nauczyciele i inni opiekunowie mogą dostosować te zasady do konkretnych okoliczności ich relacji z dziećmi, którymi się opiekują.

**Groźby**

* Pracodawcy, rodzice i nauczyciele powinni jasno sformułować zasady uniemożliwiające komukolwiek w tym dzieciom — wypowiadanie gróźb użycia przemocy lub innej krzywdy, nawet w wiadomościach e-mail lub na czatach.

* Należy poinstruować pracowników, aby zgłaszali wszystkie groźby skierowane do nich lub innych osób do funkcjonariuszy ds. bezpieczeństwa w ich organizacji; podobnie rodzice, nauczyciele lub bibliotekarze powinni upewnić się, że dzieci wiedzą, że należy natychmiast zgłaszać wszelkie zagrożenia odpowiedniej osobie dorosłej.

**Witryny nienawiści**

* Aby chronić dzieci przed podstępami tych nienawistnych ludzi, najważniejszym krokiem jest otwarta dyskusja na temat mowy nienawiści i grup nienawiści. Rodzice mogą nawet chcieć odwiedzić niektóre z wymienionych poniżej witryn ze swoimi dziećmi, aby dać im poczucie problemu i możliwych środków zaradczych.

* Omów uczucia swoich dzieci na temat obcych grup w ich własnym życiu; na przykład zachęcaj je do swobodnego wypowiadania się, bez obawy o karę lub naganę, o grupach, których nie lubią. Następnie kontynuuj dyskusję, wyjaśniając takie kwestie, jak różnice kulturowe, historia lub cokolwiek innego, co według ciebie pomoże twoim dzieciom spojrzeć z perspektywy na ich własne uczucia i zachowanie. Oczywiście ta pozytywna postawa nie może odnosić się do grup nienawiści lub podobnych wyjętych spod prawa.

* Zapewnij dzieciom pozytywne wzorce społeczne w odniesieniu do grup nienawiści. Mów zdecydowanie przeciwko nietolerancji, zamiast siedzieć cicho, gdy bigoci okazują nienawiść do innych grup.

**Pornografia**

* Umieść komputery z dostępem do Internetu małych dzieci w części rodzinnej domu, a nie w ich sypialniach.

* Interakcja z dziećmi podczas korzystania z Internetu; traktuj przeglądarkę internetową jak okno na świat i bądź obecny, aby pomóc swoim dzieciom interpretować ten świat w sposób zgodny z Twoimi wartościami.

* Rozmawiaj ze swoimi dziećmi o istnieniu i naturze pornografii; gdy dojdą do dojrzałości płciowej, zapewnij je, że zainteresowanie seksem nie jest niczym złym, ale że pornografia nie jest zdrowym sposobem poznawania zdrowych, pełnych miłości relacji.

* Ostrzegaj swoje dzieci o niektórych sztuczkach stosowanych przez pornografów, aby uzyskać ruch na ich stronach internetowych, takich jak nakłanianie ich do pobrania specjalnych czytników. Powiedz im o mołdawskim oszustwie pornograficznym.

* Omów kwestię niechcianych wiadomości e-mail, które reklamują strony pornograficzne. Ostrzeż dzieci, że nikt nigdy nie powinien klikać adresu URL z jakiejkolwiek wiadomości-śmieci, ponieważ wprowadzenie ich na niebezpieczne terytorium może być łatwym podstępem.

* Naucz swoje dzieci, aby zwracały uwagę na rzeczywisty adres URL, który pojawia się w oknie przeglądarki; wszelkie rozbieżności między widocznym adresem URL wyświetlanym na stronie a rzeczywistym adresem URL powinny ostrzegać ich o możliwości oszustwa.

* Wyjaśnij, że osoby zajmujące się pornografią czasami pobierają opłaty za dostęp do swoich witryn bez pozwolenia; upewnij się, że Twoje dzieci rozumieją, jak niebezpieczne byłoby podanie numeru karty kredytowej tym osobom z jakiegokolwiek powodu.

**Uzależnienie od Internetu**

* Poznaj znaki ostrzegawcze uzależnienia od Internetu i samokontroli.

* Omów uzależnienie od Internetu i jego znaki ostrzegawcze ze swoimi pracownikami i dziećmi.

* Zachęcaj do otwartej dyskusji na temat uczuć związanych z siecią, aby dzieci mogły zwrócić się do ciebie o pomoc, jeśli poczują się niekomfortowo lub niezadowoleni z własnych doświadczeń w sieci.

**Randki w Internecie**

* Nie twórz profili online ani nie podawaj adresów, numerów telefonów ani nazw szkół.

* Udostępniaj konta e-mail swoim dzieciom i nadzoruj ich wiadomości.

* Trzymaj komputer w pokoju rodzinnym, w którym można monitorować działania dzieci.

* Pamiętaj, że ludzie mogą kłamać, opisując siebie w Internecie.

* Nie pozwalaj dzieciom spotykać się z użytkownikami online bez pozwolenia i organizuj wszystkie spotkania w miejscach publicznych pod nadzorem osoby dorosłej.

* Przekazuj kopie dwuznacznych lub obscenicznych wiadomości swojemu dostawcy usług internetowych.

* Znajdź sposoby na zablokowanie niepożądanych materiałów.

* Omów randki online z dziećmi, aby zrozumiały, o co chodzi.

* Upewnij się, że dzieci rozumieją, dlaczego udawanie dorosłych w internetowych serwisach randkowych jest dla nich niewłaściwe, a nawet niebezpieczne.

* Nie spiesz się do kontaktu twarzą w twarz; musisz mieć pewność, że spotykasz kogoś, kto jest na poziomie, a nie oszusta, który ma ukryte motywy.

* Możesz skorzystać z usług anonimizacji oferowanych przez niektóre serwisy randkowe, aby uniknąć podawania swojego prawdziwego adresu e-mail nieznajomym.

* Bądź podejrzliwy wobec każdego, kto próbuje na ciebie wywierać presję, w tym żądać pieniędzy lub nalegać na spotkanie, zanim nabierzesz pewności co do dobrych intencji tej osoby.

* Gdy poznajesz kogoś online, zadawaj pytania dotyczące wielu rzeczy, które Cię interesują — na przykład hobby, polityka, religia, wykształcenie, data urodzenia, pochodzenie rodzinne oraz historia i stan cywilny.

* Zachowaj otrzymane odpowiedzi i uważaj na osoby, które przekazują niespójne lub sprzeczne informacje podczas komunikowania się z tobą — każde kłamstwo jest sygnałem niebezpieczeństwa.

* Bądź podejrzliwy wobec każdego, kto wydaje się być zbyt piękny, aby był prawdziwy; jeśli ktoś pasuje do ciebie pod względem wszystkich preferencji lub zainteresowań, o których wspominasz, spróbuj wspomnieć coś przeciwnego do tego, co powiedziałeś wcześniej w komunikacji i sprawdź, czy dana osoba też się z tym zgadza. Zbytnie usilne próby zadowolenia poprzez kłamstwo mogą oznaczać manipulacyjną i potencjalnie niebezpieczną osobowość.

* Bądź szczery wobec siebie; uczciwie przedstawiaj swoje zainteresowania i cechy, w tym rzeczy, które Twoim zdaniem mogą być mniej atrakcyjne niż nakazują stereotypy i normy kulturowe. Dojrzały, dobry człowiek niekoniecznie się wyłączy, jeśli nie będziesz wyglądać jak gwiazda filmowa, lub jeśli nie zagrasz perfekcyjnie na czterech instrumentach muzycznych, lub jeśli seplenisz.

* Jeśli dojdziesz do punktu wymiany zdjęć, upewnij się, że widzisz tę osobę w różnych sytuacjach iz innymi ludźmi; niektórzy randkowicze online wysyłają fałszywe zdjęcia, aby się przedstawić.

* Porozmawiaj z osobą, którą się interesujesz przez telefon; bądź podejrzliwy, jeśli dana osoba długo opiera się takiej prośbie lub zawsze ma wymówki, by nie być dostępna, kiedy zgodziłeś się porozmawiać.

* Słuchaj uważnie, jak dana osoba brzmi przez telefon i bądź podejrzliwy, jeśli teraz otrzymasz informacje, które są sprzeczne z tym, o czym dana osoba do ciebie napisała. Każde kłamstwo powinno ostrzegać o potencjalnych problemach.

* Zanim zgodzisz się na spotkanie, zdobądź pełne imię i nazwisko, adres i numer telefonu swojej randki. Bądź podejrzliwy, jeśli dana osoba odmawia podania numeru domowego: czy może mieć współmałżonka lub obecnego przyjaciela, którego próbuje oszukać? Zadzwoń kilka razy pod numer domowy, aby sprawdzić, czy ktoś inny odbierze.

* Podaj informacje o tej osobie oraz dokładne szczegóły dotyczące miejsca i czasu spotkania, przyjaciołom i rodzinie. Nigdy nie umawiaj się z kimś, kto chce zachować miejsce i czas w tajemnicy. Upewnij się, że miejsce spotkania jest dobrze oświetlone i znajduje się w miejscu publicznym, takim jak kawiarnia.

* Nie pozwól nieznajomemu odebrać cię z domu i upewnij się, że możesz wrócić do domu sam.

* Zanim rozważysz dalsze zaangażowanie, ze względów bezpieczeństwa pomyśl o sprawdzeniu przeszłości osoby, którą lubisz, korzystając z profesjonalnej usługi.

**Gry online**

* Naucz się grać w niektóre gry, którymi Twoje dzieci są zachwycone. Poświęć trochę czasu, aby zanurzyć się w wyimaginowanych światach, w których grają, i przestudiuj podstawowe wartości, które są przekazywane przez twórców gry.

* Korzystaj z opublikowanych recenzji z Internetu lub innych mediów, które odzwierciedlają wartości Twojej rodziny, zanim wpuścisz gry do swojego domu.

* Towarzysz swoim dzieciom w sklepach przy zakupie gier wideo. Sprawdź etykiety ostrzegawcze dla rodziców. Porozmawiaj ze sprzedawcami, jeśli uważasz, że są godni zaufania.

* Zapoznaj się z charakterystyką swojego sprzętu i oprogramowania przed zakupem niedawno wydanych gier. Nie kupuj nowej gry tylko po to, by odkryć, że nie działa ona na twoim przestarzałym systemie. Rozczarowane dziecko może wywierać silną presję, aby wydać pieniądze na nowy system. Niektóre gry są wymagające obliczeniowo i wymagają drogiego, zaawansowanego sprzętu komputerowego i nowoczesnych systemów dźwiękowych, wraz ze wzmacniaczem o dużej mocy napędzającym głośniki niskotonowe i subwoofery.

* Postaraj się, aby gra była okazją do rodzinnej zabawy lub tworzenia więzi rodzic-dziecko, zamiast izolującego doświadczenia, jakim czasami mogą być gry. Sprawdź, czy wszyscy możecie się dobrze bawić w grach zorientowanych na łamigłówki i eksplorację, takich jak Myst i Riven, z których żadna nie zawiera przemocy i obie są piękne wizualnie.

**Zakupy internetowe**

* Zanim wydasz znaczną sumę pieniędzy na nową witrynę sprzedawcy internetowego, przeprowadź podstawowe badania dotyczące niezawodności witryny. Sprawdź reputację firmy;

* Przeprowadź wyszukiwanie w Internecie za pomocą dobrej wyszukiwarki, takiej jak Google, aby sprawdzić, czy są jakieś aktualne raporty na temat wrażeń klientów w witrynie, która Cię interesuje.

* Udawaj, że masz już problem i poszukaj stron obsługi klienta. Czy istnieją jasne instrukcje dotyczące komunikowania problemów? Czy miałbyś do wyboru e-mail, listy lub komunikację telefoniczną? Jeśli masz czas, możesz nawet spróbować zadzwonić do obsługi klienta i dowiedzieć się, jak obsługują połączenia. Jeśli trafisz na firmę, która rozłącza się, gdy jej linie są zajęte „Przepraszamy, ale wszyscy nasi agenci są zajęci; proszę oddzwonić później”), warto się poważnie zastanowić, czy robienie z nimi interesów jest bezpieczne.

* Zapoznaj się z polityką zwrotów firmy; jak radzi sobie z uszkodzeniami w transporcie lub wadliwymi towarami? Czy oferuje gwarancje na czas dostawy? Co się stanie, jeśli w firmie zabraknie określonego artykułu – czy wysyła częściowe przesyłki, czy czeka, aż wszystko będzie gotowe? Czy w przypadku wyczerpania zapasów karta kredytowa jest obciążana natychmiast, czy dopiero po zrealizowaniu wysyłki? Jeśli podzieli twoją przesyłkę, czy pobiera dodatkową opłatę za dostawę późniejszych części?

* Zapoznaj się z polityką prywatności serwisu. Jeśli tekst jest praktycznie niewidoczny 6-punktowy żółty na białym tle, bądź podejrzliwy. Poszukaj w klauzulach łasicowych słów, które mówią na przykład, że ich zasady mogą zostać zmienione w dowolnym momencie bez powiadomienia. Musisz regularnie sprawdzać witrynę, aby sprawdzić, czy zasady się zmieniły, ale jest to nierealne. Zamiast tego szukaj stanowczych, jasnych zapewnień, że Twoje dane osobowe nie zostaną sprzedane, zamienione ani przekazane bez Twojej zgody. Zwykle właściciele witryn twierdzą, że być może będą musieli ujawnić informacje organizacjom partnerskim, które zajmują się takimi normalnymi funkcjami, jak rozliczanie i realizacja zamówień. Nie ma co do tego większych zastrzeżeń, pod warunkiem, że partnerzy są związani akceptowalną polityką bezpieczeństwa.

* Prowadź szczegółowy zapis swoich transakcji. Użyj funkcji przeglądarki, aby zapisać kopie lub wydrukować odpowiednie strony internetowe z opisami produktów, cenami, podsumowaniem zamówienia, numerem zamówienia, obiecanym terminem dostawy i sposobem wysyłki.

**Aukcje internetowe**

* Zanim zaangażujesz się w aukcje internetowe, zbadaj wartość towarów, które chcesz kupić. Sprawdź sklepy stacjonarne, punkty sprzedaży detalicznej online i porównywarki cen, które oferują konkretne ceny.

* Sprawdź zasady i koszty wysyłki, gwarancji i zwrotów.

* Ustaw swój górny limit, zanim zaangażujesz się w aukcję. Nie sugeruj się wartością, jaką inni ludzie wydają się przywiązywać do konkretnego produktu lub usługi, a już na pewno nie wpadnij w szał licytacji.

* Nie traktuj aukcji internetowych jako zawodów, które musisz wygrać.

* Poszukaj serwisów aukcyjnych, które dają gwarancję wsparcia, jeśli zostaniesz oszukany w transakcji. Na przykład sprawdź warunki korzystania z usługi, które obejmują straty do odpowiedniego limitu. Czeki lub polisy ubezpieczeniowe, koszty, warunki i limity. Skorzystaj z wyszukiwarek, aby ocenić wiarygodność usługi, z której zamierzasz skorzystać.

* Jeśli to możliwe, skorzystaj z usługi, która zapewnia funkcję escrow, aby wpłacić pieniądze do usługi, a następnie zwolnić je dopiero po otrzymaniu produktu w dobrym stanie.

* Używaj funkcji przeglądarki do drukowania dokumentów i zapisywania stron internetowych na dysku na każdym etapie każdej transakcji.

**Hazard online**

* Nie graj pieniędzmi, których nie możesz stracić.

* Nie uprawiaj hazardu online, z wyjątkiem dobrze znanych witryn.

* Jeśli uprawiasz hazard online, nie graj pieniędzmi na stronach hostowanych poza Twoim krajem.

* Nie podawaj numeru swojej karty kredytowej centrom gier hazardowych online, które znajdują się poza Twoim krajem.

* Zanim zaczniesz grać online, poszukaj informacji, czy nie było skarg na to kasyno. Sprawdź, czy możesz znaleźć przyjaciół lub znajomych, którzy grali na stronie, którą rozważasz.

**Zapobieganie infekcjom złośliwym oprogramowaniem**

* Dbaj o aktualność ciągów wirusów (automatyczne codzienne aktualizacje są dobre).

* Nie pobieraj ani nie używaj oprogramowania, które rzekomo pomaga łamać prawo lub oszukiwać ludzi i firmy.

* Nie pobieraj ani nie używaj oprogramowania, które zostało skopiowane bez pozwolenia lub z naruszeniem ograniczeń licencyjnych. To jest piractwo komputerowe, naruszenie praw autorskich lub zwykła kradzież.

* Nie uruchamiaj oprogramowania, które ktoś przesłał ci pocztą elektroniczną, nawet jeśli znasz i lubisz osobę, która ci je wysłała. Tylko dlatego, że dana osoba jest miła, nie oznacza, że ma kwalifikacje do sprawdzania programów pod kątem bezpieczeństwa.

* Przed wysłaniem komuś załącznika, takiego jak zdjęcie lub innego rodzaju plik e-mailem, poinformuj odbiorcę, czego może się spodziewać za pośrednictwem wstępnej wiadomości; jeśli nie znasz tej osoby osobiście, wyślij e-mail z prośbą o pozwolenie na przesłanie załącznika.

* Nigdy nie otwieraj otrzymanych załączników bez wcześniejszego powiadomienia, niezależnie od tego, kto je wysłał lub co mówi temat lub tekst. Bądź szczególnie podejrzliwy w stosunku do ogólnych tematów, takich jak „FYI" bez szczegółów lub „Spodoba ci się". Jeśli jesteś naprawdę ciekawy załącznika, zadzwoń lub wyślij e-mail do domniemanego nadawcy, aby dowiedzieć się, czy jest on zgodny z prawem. Pamiętaj jednak, że nie powinieneś uruchamiać programów, które otrzymujesz jako załączniki, niezależnie od tego, co myśli nadawca.

* Nie przesyłaj nikomu programów, nawet niezawodnych; zamiast tego powiedz znajomym, skąd mogą pobrać przydatne programy z godnego zaufania źródła, takiego jak legalna strona internetowa.

* Przed wysłaniem komukolwiek dokumentu Microsoft Word jako załącznika, zapisz dokument jako plik RTF zamiast zwykłego pliku DOC. Pliki RTF nie zawierają makr dokumentów i dlatego nie mogą przenosić makrowirusów.

* Wyłącz makra w Microsoft Word.

* Skorzystaj z opcji oferowanych przez klienta poczty e-mail, aby wyłączyć automatyczne otwieranie lub wykonywanie załączników.

* Nie rozpowszechniaj ostrzeżeń o wirusach; jeśli nalegasz, aby to zrobić, osobiście sprawdź ich ważność na dowolnej z wielu witryn z informacjami o wirusach i oszustwami w sieci Web.

**Ochrona przed oprogramowaniem szpiegującym**

* Przed zainstalowaniem oprogramowania typu freeware lub adware przeczytaj uważnie warunki, aby sprawdzić, czy obecnie zawierają język umożliwiający automatyczne przekazywanie informacji dostawcy lub stronom trzecim. Należy pamiętać, że umowy te często zawierają sformułowania upoważniające dostawcę do zmiany warunków w dowolnym momencie i bez powiadamiania użytkownika.

* Zainstaluj i używaj skanera i programu do usuwania spyware, takiego jak darmowy program Ad-Aware firmy Lavasoft, PestPatrol firmy Computer Associates lub zapora ZoneAlarm.

* Jeśli jesteś szczególnie zirytowany oprogramowaniem szpiegującym, zainstaluj monitor i bloker oprogramowania szpiegującego w czasie rzeczywistym, takie jak te, które właśnie wymieniono.

* Wspieraj próby legislacyjne mające na celu zmuszenie producentów oprogramowania do ujawnienia korzystania przez nich z oprogramowania szpiegującego.

**Wiadomości-śmieci**

* Nie kupuj produktów ani usług od osób, które wysłały Ci niechciane wiadomości e-mail. Jeśli firma jest na tyle nieprofesjonalna lub nierozważna, że stosuje takie metody reklamy, nie zasługuje ani na Twój biznes, ani na Twoje zaufanie.

* Nie zakładaj, że adres OD jest poprawny, ponieważ często albo nie istnieje, albo, co gorsza, oszukańczo błędnie przedstawia pochodzenie, wskazując na legalną firmę, która jest całkowicie niewinna. Nigdy nie bombarduj właściciela adresu OD wieloma kopiami lub nawet jedną kopią obraźliwych wiadomości e-mail. Takie wiadomości, zwane bombami pocztowymi, prawdopodobnie dotrą do niewłaściwego celu - do jakiegoś niewinnego adresata.

* Nigdy nie odpowiadaj na adres podany do usunięcia z listy dystrybucyjnej e-maili, chyba że sam zainicjowałeś kontakt lub masz pewność, że znasz organizację, która wysłała Ci wiadomość (np. publikacje, które już subskrybujesz). Ponieważ zwroty (zwrócone e-maile z powodu złych adresów) nigdy do nich nie docierają, a wysyłanie adresów do niechętnych osób nie wiąże się z dodatkowymi kosztami, operatorzy ci naprawdę nie dbają o to, co myślisz o wysyłanych przez nich śmieciach. Dlatego nieetyczni ludzie, którzy wysyłają wiadomości-śmieci, używają funkcji USUŃ przede wszystkim do zbierania poprawnych adresów e-mail, aby móc je sprzedać komuś innemu.

* Nawet jeśli ufasz organizacji, która wysłała Ci niechcianą wiadomość e-mail, nigdy nie klikaj łącza zawartego w wiadomości. Zamiast tego odwiedź stronę internetową firmy i poproś o usunięcie jej z oficjalnego adresu kontaktowego, który posiada każda renomowana firma.

* Nie odwiedzaj adresów URL wymienionych w wiadomościach-śmieciach. Niektóre z nich są celowo błędnie oznaczone i mogą prowadzić do obraźliwych stron internetowych.

* Jeśli naprawdę czujesz złość z powodu konkretnego e-maila, który zawiera skrzynkę pocztową (prawdziwy adres w treści wiadomości, na który powinieneś odpowiedzieć), to jeśli nie masz nic lepszego do roboty, możesz wysłać kopię e-maila spam na odpowiedni adres (zwykle w formularzu abuse@ISPname.domain, gdzie należy wypełnić zmienne ISPname i domain) adres, na którym działa dropbox. Istnieje jednak duże prawdopodobieństwo, że Twoja wiadomość będzie jednym z setek lub tysięcy podobnych zgłoszeń.

* Nie wysyłaj samodzielnie żadnych wiadomości-śmieci. Zachęć osoby w Twoim otoczeniu (przyjaciół, sąsiadów, dzieci), aby również nie wysyłały wiadomości-śmieci.

**Burze pocztowe**

Oto kilka prostych sugestii, jak zmniejszyć prawdopodobieństwo wystąpienia burz pocztowych:

* Zminimalizuj użycie automatycznych odpowiedzi na swoich kontach e-mail.

* Jeśli automatycznie przesyłasz dalej pocztę, nie pozwól, aby docelowa skrzynka pocztowa się zapełniła.

* Jeśli otrzymujesz wiadomości e-mail przekazywane automatycznie z głównej skrzynki pocztowej, nie przesyłaj ich z powrotem do oryginalnej skrzynki pocztowej.

* Administratorzy systemu poczty e-mail powinni otrzymywać raporty o wyjątkach identyfikujące konta z nadmierną liczbą wiadomości e-mail lub nadmiernym ruchem, aby mogli badać burze poczty.

* Zapory ogniowe sprawdzające zawartość wiadomości e-mail powinny być w stanie zareagować na nadmierną liczbę wiadomości odsyłanych z jednego adresu źródłowego, usuwając ruch lub informując administratora systemu o prawdopodobnej burzy poczty.

* Menedżerowie list niemoderowanych powinni skonfigurować adres OD, inny niż adres, którego uczestnicy używają do wysyłania wiadomości na listę.

* Użytkownicy serwerów list, którzy chcą wysyłać prywatne wiadomości, powinni odpowiadać nadawcy, a nie całej liście.

**Wykrywanie oszustw**

Kluczowe wskaźniki wskazujące, że wiadomość jest mistyfikacją:

* Używanie wykrzykników. Żadne oficjalne ostrzeżenie ich nie używa.

* Używanie dużej ilości tekstu pisanego wielkimi literami, co jest typowe dla młodzieży.

* Błędy ortograficzne i zła gramatyka.

* Brak daty powstania lub wygaśnięcia.

* Włączenie słów takich jak „wczoraj”, gdy w wiadomości nie ma daty.

* Odniesienia do oficjalnie brzmiących źródeł, takich jak Microsoft, Computer Incident Advisory Capability (CIAC), Centrum Koordynacji Zespołu Reagowania na Kryzysy Komputerowe CERT-CC), ale bez szczegółowych adresów URL dokumentów. Adresy URL strony głównej witryny się nie liczą.

* Brak ważnego podpisu cyfrowego od znanej organizacji bezpieczeństwa.

* Prośby o szerokie rozpowszechnianie. W oficjalnych dokumentach nigdy nie pojawia się taka prośba.

* Twierdzi, że ktoś liczy wiadomości e-mail zawierające kopie mistyfikacji.

* Groźby o zgubnych konsekwencjach, jeśli ktoś zerwie łańcuch, odmawiając przekazania wiadomości.

* Roszczenia o nagrody pieniężne, które nie mają sensu. Na przykład organizacja Disneya wyśle ci 5000 $ za przekazanie wiadomości e-mail.

* Używanie skomplikowanego języka technicznego, takiego jak „n-te pętle sterowania o nieskończonej złożoności”, które nie mają sensu.

* Roszczenia z tytułu uszkodzenia sprzętu komputerowego spowodowanego wirusami lub innym oprogramowaniem komputerowym.

**Schematy szybkiego wzbogacenia się**

* Przypomnij wszystkim, aby kierowali się zdrowym rozsądkiem: zarabianie dużych pieniędzy przy niewielkim wysiłku lub bez wysiłku zazwyczaj skutkuje odkryciem czegoś niemożliwego lub nielegalnego.

* Naucz użytkowników mantry sceptyka: „Jeśli brzmi to zbyt dobrze, aby mogło być prawdziwe, zazwyczaj tak jest”.

* Wyjaśnij, jak niebezpieczne jest angażowanie się w przestępcze intrygi, takie jak używanie skradzionych lub sfałszowanych kart kredytowych. Mów o ofiarach takiego oszustwa: o wszystkich, którzy płacą wyższe odsetki od niezapłaconych rachunków za karty kredytowe i niewinnych sklepikarzach, którzy tracą towary na rzecz oszustów z handlu elektronicznego.

* Zwłaszcza rozmawiając z dziećmi, rozmawiaj o kradzieży za pośrednictwem Internetu w taki sam sposób, jak o kradzieży w sklepie. Wyjaśnij, jak działa handel; podkreślić, że wszyscy padają ofiarą wszelkiego rodzaju kradzieży, w tym kradzieży elektronicznych w sklepach.

**Hakowanie**

* Skontaktuj się z lokalnym biurem FBI i dowiedz się, czy mogą wysłać mówcę do Twojej firmy lub na lokalne spotkanie profesjonalnego stowarzyszenia bezpieczeństwa w celu omówienia przestępstw komputerowych.

* Jeśli ty lub określony upoważniony personel (np. z grupy ds. bezpieczeństwa) odwiedzasz strony internetowe, które wspierają przestępcze hakowanie, pamiętaj o użyciu osobistej zapory ogniowej i

ustaw parametry, aby odmówić dostępu do danych osobowych oraz odrzucić pliki cookie i aktywny kod (ActiveX, Java ) z takich witryn.

**UWAGI KOŃCOWE**

Skoncentrowaliśmy się w szczególności na używaniu i nadużywaniu zasobów Internetu i poczty elektronicznej. Staje się jednak jasne, że obie te technologie są po prostu przedłużeniem człowieka stojącego za komputerem. Niezależnie od tego, czy chodzi o pornografię, hazard online, oszukańcze wiadomości e-mail, czy po prostu umieszczanie nieodpowiednich materiałów na publicznej stronie internetowej, istnieje duże prawdopodobieństwo wyrządzenia szkody osobie, rodzinie lub organizacji. Przyjmowanie proaktywnej postawy poprzez edukację i uświadamianie jest jednym z głównych narzędzi zwalczania tych oszukańczych i nieetycznych praktyk.

Pracodawcy mają etyczny, a w wielu przypadkach prawny, obowiązek opracowania i wdrożenia zasad dotyczących właściwego korzystania z Internetu i poczty elektronicznej w pracy. Niestety, samo wprowadzenie zasad dotyczących konsumpcji przez pracowników nie wystarczy. Pracodawcy muszą stale przypominać pracownikom zarówno o niebezpieczeństwach związanych z niewłaściwym użytkowaniem, jak i potencjalnych konsekwencjach dla ich zatrudnienia. A kiedy pracownik zdecyduje się naruszyć zasady, pracodawcy muszą mieć jasno określony proces zachęcania do właściwego zachowania. Zakres oddziaływania tych kwestii nie kończy się po prostu wraz z odejściem pracownika z biura. Ze względu na powszechne korzystanie z Internetu i poczty e-mail w prawie każdym aspekcie naszego życia, zabranie wiadomości do domu rodzinie jest ważnym obowiązkiem każdego. Dzieciobójcy wykorzystują Internet do żerowania na niczego niepodejrzewających lub naiwnych dzieciach w celu wykorzystania ich do dowolnej niemoralnej działalności. Rodzice mają wówczas obowiązek wprowadzenia własnej polityki rodzinnej dotyczącej tego, co jest, a co nie jest dopuszczalnym korzystaniem z Internetu i poczty elektronicznej w domu. Niestety nie ma prostej odpowiedzi na problemy opisane w tym rozdziale. Zarówno Internet, jak i poczta elektroniczna nie są ani dobre, ani złe. Stają się dobre lub złe tylko dzięki użytkownikom i ich działaniom. Ponieważ technologia wciąż przyspiesza i umożliwia przechowywanie większej ilości danych na mniejszej przestrzeni, wszyscy muszą odgrywać aktywną rolę we wzajemnej ochronie na poziomie korporacyjnym i w domu.