Poradnik Bezpiecznego Korzystania z Internetu

1. Bezpieczeństwo najmłodszych sieciomaniaków

Alternatywna rzeczywistość

Internet pomyślany jako narzędzie do pracy, komunikacji i baza danych ewoluował do rangi alternatywnego świata – przestrzeń wirtualna stała się płaszczyzną dla poważnych działań biznesowych, obrotu pieniędzmi , intensywnych kontaktów międzyludzkich, uprawiania hobby, edukacji, komunikowania się z administracją publiczną i zapewniania sobie rozrywki… Wymieniać można w nieskończoność. Bogactwo korzyści czerpanych z Sieci przez miliardy mieszkańców naszego globu przekłada się na równie liczne zagrożenia. Tam, gdzie są pieniądze, są i złodzieje, tam, gdzie konsumenci – agresywna reklama i konkurencja za wszelką cenę, tam, gdzie odbiorcy informacji – manipulacje właściwe wszystkim mediom masowym. A tam, gdzie możliwość spotkania z nieznanymi osobami– zagrożenie tożsame spotkaniu z nieznajomym.

Nie umniejszając olbrzymiej dodatniej roli pełnionej przez Internet w życiu towarzyskim, relacjach biznesowych i rozprzestrzenianiu wiedzy i informacji, trzeba mieć świadomość ryzyka, jakie niesie beztroskie korzystanie z Sieci. Szczególnie w przypadku, gdy użytkownikiem są najmłodsi – i najbardziej bezbronni.

Najczęstsze zagrożenia

Wśród najczęstszych zagrożeń dla bezpieczeństwa nieletnich (i nie tylko) internautów, na jakie powinni zwrócić uwagę rodzice, opiekunowie i nauczyciele, znajdują się:

- przechwytywanie danych i zagrożenie utratą prywatności
- fałszowanie danych
- kradzież danych personalnych
- przejęcie komputera przez hakerów
- kradzież haseł – a co za tym idzie, zagrożenie utraty plików dostępnych na komputerze
- phishing – podszywanie się przez hakerów za instytucje zaufania publicznego, na przykład bank, w celu wyłudzenia danych (na przykład danych dostępowych do e-konta)
- programy szpiegujące mające na celu targetowanie reklam kierowanych do użytkownika
- oszustwo internetowe – na przykład w postaci wyłudzenia opłaty za towar wadliwy bądź realnie nieistniejący
- demoralizacja – ilość informacji propagujących przemoc, pornografię, prostytucję, przestępczość i używki jest w Sieci tak ogromna, że niemożliwa jest ich pełna kontrola i blokada. W szczególności dzieci narażone na kontakt z takimi treściami mogą ulec błędnemu wrażeniu co do wartości oglądanych treści.
- zaufanie wobec nieznajomych, kontakt z osobami o nieuczciwych zamiarach

Przykazania główne

Najbardziej podstawowe zalecenia dotyczących ochrony dzieci i młodzieży przed internetowymi niebezpieczeństwami można streścić w zasadzie ograniczonego zaufania. Ponadto ważne są:

- elementarna ostrożność w kontaktach z nieznajomymi,

- korzystanie z ofert sprawdzonych i rekomendowanych firm,
- używanie bezpiecznych haseł i loginów,
- rozsądne zamieszczanie informacji personalnych w internetowych ankietach, sondach, w serwisach społecznościowych,
- nieotwieranie plików z niepewnego źródła
- nieodbieranie wiadomości email od nieznanych osób
- niekorzystanie z niepewnych komputerów do logowania się w banku (na przykład w kafejce internetowej)
- instalowanie legalnego i bezpiecznego oprogramowania
- bieżąca aktualizacja oprogramowania
- korzystanie z zaufanych stron.
- nieotwieranie linków na komunikatorze od nieznajomych
- unikanie pobierania programów z nieoficjalnych
- pobieranie plików muzycznych, filmowych, gier itp. wyłącznie z legalnych źródeł
- instalacja programów antywirusowych, antyszpiegowskich, zapór sieciowych
- regularne skanowanie komputera przy pomocy w/w oprogramowania
- właściwe skonfigurowanie przeglądarki – np. z kasowanie plików cookies
- formatowanie urządzeń przenośnych (dyskietek, pamięci USB) przed udostępnieniem innym osobom
- zachowanie loginów, haseł, kont mailowych i społecznościowych wyłącznie dla siebie

Internetu trzeba nauczyć

Rodzice powinni być pierwszymi nauczycielami korzystania z mediów, szczególnie interaktywnych. Jak dbać o bezpieczeństwo dziecka, jak ukształtować właściwe postawy wobec treści zamieszczanych w Sieci?

- Odkrywanie Internetu powinno być wspólnym zajęciem – strony z informacjami, grami i zabawami interesującymi pociechę rodzic powinien znaleźć i mądrze wskazać dziecku. Warto razem szukać danych potrzebnych do szkoły, stron z ciekawostkami dla dzieci.
- Nigdy za wiele ostrzeżeń i przypomnień, że nieznajomemu nie można ufać, że Internet daje nie tylko okazję do świetnej zabawy i nauki, ale bywa źródłem niebezpieczeństw.
- W przypadku nawiązania przez dziecko / nastolatka znajomości przez Internet, należy czuwać nad rozwojem kontaktów, przede wszystkim uczulić dziecko, że spotkanie może nastąpić wyłącznie za zgodą rodzica.
- Warto mówić wprost o możliwych zagrożeniach: rozczarowaniu po konfrontacji wirtualnej osoby z rzeczywistą, o groźbie napaści seksualnej, nadużyciu zaufania.
- Anonimowość bywa cnotą. Mimo iż najmłodsze dzieci nie korzystają z serwisów społecznościowych, bankowości internetowej ani nie dokonują zakupów online, jak najwcześniej należy wyjaśnić im, że nie na każde pytanie o imię, nazwisko, numer telefonu i adres należy odpowiadać – a już na pewno nie należy odpowiadać bez wyraźnej zgody rodzica.
- Jak wobec innych mediów, tak i wobec Internetu należy kształtować w dziecku postawę krytyczną. Nie każda informacja wyczytana w Sieci jest prawdziwa, nie każda definicja i ściągawka na popularnym serwisie dla uczniów ma wartość encyklopedyczną.

- Szkodliwe i zakazane treści trzeba piętnować aktywnie – każda strona promująca pornografię, przemoc, narkotyki powinna być zgłaszana, na przykład na stronie www.dyzurnet.pl czy www.hotline.org.pl Taka konsekwencja upewni dziecko, że pewne informacje są niepożądane i szkodliwe dla niego.
- Troskliwa kontrola – tak, by nie narazić się na utratę zaufania dziecka. Dobre wychowanie nie gwarantuje pełnego bezpieczeństwa. Można postarać się na przykład o to, by komputer stał w pomieszczeniu używanym przez wszystkich domowników. Warto go również wyposażyć w oprogramowanie filtrujące typu Cenzor oraz kontrolnie sprawdzać w przeglądarce, na jakie strony wchodzą użytkownicy (dzieci).
- Trudne słowa są potrzebne - pornografia, narkotyki, sekty, pedofilia, gwałt, kradzież, haker – dziecko musi znać nazwy zjawisk, przed którymi jest przestrzegane, rozumieć je w możliwym zakresie i poznawać ich właściwy kontekst.
- Żadne z pytań synonimicznych do:
  Jak się nazywasz? Jak wyglądasz? Prześlesz mi zdjęcie? Ile zarabiają twoi rodzice? Jakie masz kieszonkowe? Czy lubisz się przytulać? Masz kartę kredytową? W co jesteś ubrany? Czy chciałbyś dostać prezent? Gdzie mieszkasz? Czy jesteś sam w domu? Możemy się spotkać u mnie w domu? Mogę odebrać Cię ze szkoły?
  nie jest bezpieczne, powinno wzbudzić nieufność w dziecku i spowodować zerwanie kontaktu z nieznajomym internautą.
- Jasne zasady: warto ustalić z dzieckiem, o jakiej porze i jak długo może ono korzystać z Internetu – dla dobra własnych oczu, kręgosłupa, oraz dla równowagi między surfowaniem po Sieci a nauką, życiem rodzinnym i aktywnością towarzyską w rzeczywistym świecie.
- Prowadzenie bloga to forma ekspresji, czasem literacka próba, często sposób zyskiwania popularności wśród rówieśników. Należy mieć jednak świadomość, że zbytnia szczerość, otwarcie się może powodować złośliwe, obraźliwe komentarze ze strony nieodpowiedzialnych użytkowników.
- „Czy naprawdę chcesz pokazać wszystkim te zdjęcia?" – warto pytać o to dziecko, które w portalu społecznościowym lubi zamieszczać swoje fotografie. Warto wskazać wartość z posiadania prywatności, dyskrecji oraz zwrócić uwagę, czy postronni bohaterowie zamieszczanych zdjęć nie mają nic przeciwko.
- Świadomość, że netykieta obowiązuje także nasze dziecko – dbając, by nie stało się ofiara manipulacji,, należy zwrócić uwagę, by samo nie działało w żaden sposób na czyjąś szkodę., na przykład nie wykorzystywało forów do rozsiewania nieprawdziwych, nieuprzejmych czy obraźliwych opinii albo nie zamieszczało w Sieci zdjęć i filmów naruszających czyjąś prywatność, godność.

Sytuacje alarmowe

Co powinno zaalarmować rodzica?

- Wyłączanie monitora po wejściu rodzica do pokoju albo szybka zmiana przeglądanej strony – z jednej strony można takie zachowanie traktować jako naturalną chęć do zachowania prywatności, z drugiej strony powtarzające się ukrywanie oglądanych treści, w połączeniu z innymi nietypowymi reakcjami, powinno zaniepokoić.
- Telefony od nieznajomych
- Surfowanie w Sieci bardzo długo, przesiadywanie po nocach.
- Unikanie kontaktów towarzyskich i rodzinnych poza Siecią.
- Zwiększone wydatki, posiadanie nieuzasadnionych sum pieniędzy, prezenty, z których dziecko nie potrafi się wytłumaczyć – oczywiście, niekoniecznie Internet jest źródłem znajomości przynoszących takie profity, należy jednak założyć, że w Sieci najłatwiej – bo bez

wychodzenia z domu - poznać kogoś, kto pod pozorami sympatii tak naprawdę próbuje dziecko do czegoś nakłonić, przekupić. Może to być sposób wabienia ofiar prze pedofila albo sektę.

- Zawirusowany komputer.
- Nagła utrata danych.
- Zaobserwowana ingerencja w informacje zamieszczone na profilu w serwisie społecznościowym.
- Niewytłumaczalne operacje na koncie bankowym.
- Zaobserwowane wykorzystanie danych osobowych do celów, na które nie wyraziliśmy zgody.
- Wykorzystanie przez osobę postronną informacji zawartych w wiadomościach e-mail.
- Nagły wzrost liczby reklam wyświetlanych na monitorze podczas surfowania w Sieci.

Reakcja rodzica musi być spokojna – nie można dziecka obwiniać bez ustalenia, co się dzieje, a przede wszystkim – czy nie stało się ono ofiarą oszustwa, manipulacji, wykorzystania. W przypadku, gdy dziecko zostało skrzywdzone lub choćby przestraszone, należy skorzystać z pomocy specjalistów - policji, pedagoga, psychologa, organizacji walczących o prawa i bezpieczeństwo dzieci (na przykład Fundacja Kidprotect).

Najlepszą ochroną dla dziecka są właściwie ukształtowane postawy: wiedza, czemu ma służyć Internet, że surfowanie po Sieci jest tylko jedną z wielu form aktywności, umiejętność odróżnienia wartościowych treści od internetowych śmieci, instynkt samozachowawczy w kontaktach z obcymi ludźmi. Świadomość zagrożeń potencjalnie płynących z Sieci jest wciąż niska i to na rodzicach ciąży obowiązek pokazania, jak korzystać z tego narzędzia. Dorośli użytkownicy bywają niestety równie naiwni, a dodatkowo narażeni są na inne niebezpieczeństwa: związane z działalnością zawodową, poszukiwaniem partnera, dokonywaniem przelewów, zakupów, uczestnictwa w aukcjach oraz korzystania ze zbyt łatwo dostępnego nielegalnego oprogramowania. Rozwaga dorosłych jest najlepszym wzorcem dla dzieci i odwrotnie – brak rozwagi zniweczy wszelkie dydaktyczne działania (żadne dziecko nie będzie słuchać o szkodliwości całonocnego przesiadywania przed monitorem, jeśli rodzić robi dokładnie to samo…).

2. Bezpieczeństwo dla zaawansowanych

Dzieciom Internet kojarzy się z zabawą, rozrywką, pomocą szkolną, nowymi kolegami i koleżankami. Wrodzona ufność naraża je na ryzyka opisane powyżej – tożsame z niebezpieczeństwami występującymi „ w realu” w sytuacji kontaktów z nieznajomymi. Internet rodzi jednakże zagrożenia zupełnie specyficzne, na które narażone są także nastolatki, oraz dorośli: wirusy, phishing, hakerzy, wyłudzenia, kradzieże, utrata danych, włamania do bazy, przejęcie domeny. Można oceniać, że im wyższe zaawansowanie w korzystaniu z Sieci, tym stopień ryzyka rośnie – domowy czy służbowy komputer wchodzi bowiem w większą liczbę interakcji z zasobami Sieci i komputerami innych użytkowników.

Metodą ochrony jest oczywiście wiedza w zakresie zagrożeń i ostrożność – np. w kreowaniu haseł, otwieraniu obcych plików, wchodzeniu na stronę banku przez niesprawdzone komputery – lecz także korzystanie z zabezpieczeń technologicznych: programów skanujących, antywirusowych.

Największe zagrożenia

Zależne od człowieka:

- rozsyłanie spamu,
- rozsyłanie wirusów komputerowych,

- phishing - podszywanie się pod instytucję zaufania publicznego w celu wyłudzenia danych, np. numeru konta (fałszowane maile i strony banków) pod pozorem „weryfikacji danych”,
- działania przestępcze na obiektach fizycznych (np. instalacja podsłuchu na komputerze),
- przechwytywanie domen,
- piractwo,
- wady sprzętu,
- nieumiejętne obchodzenie się z komputerem, oprogramowaniem,
- niewłaściwa organizacja pracy,
- brak wiedzy.

Zależne od środowiska

- fizyczne uszkodzenie komputera, sieci, serwera, nośnika danych w wyniku wypadków losowych (pożarów, powodzi, włamania)

Przyjrzyjmy się najpowszechniejszym zjawiskom szkodliwym i utrudniającym korzystanie z Internetu.

WIRUSY KOMPUTEROWE

Wirusy komputerowe to proste programy o zdolności do samopowielania się (replikacji), które po zainfekowaniu komputera mogą powodować:

- kasowanie i niszczenie danych,
- rozsyłanie spamu,
- dokonywanie ataków na serwery internetowe,
- kradzież danych (hasła, numery kart płatniczych, dane osobowe),
- wyłączenie komputera,
- wyświetlanie grafiki lub odgrywanie dźwięków,
- uniemożliwienie pracy na komputerze,
- umożliwienie przejęcia kontroli nad komputerem osobie nieupoważnionej,
- tworzenie botnetu

Stworzenie wirusa nie wymaga dużych umiejętności, w Internecie są dostępne generatory wirusów o intuicyjnym menu. Przenoszone są poprzez pliki, przenośne pamięci danych i elementy dysku twardego. Ich niewielki rozmiar powoduje, że łatwo je ukryć w bazie danych, programie. Atakują pliki, dyski, skrypty, a także coraz częściej oprogramowanie internetowe urządzeń mobilnych. Według kryterium sposobu działania dzielimy je na:

- wirusy pasożytnicze – infekują pliki i uszkadzają je; to najczęstszy typ wirusów. Ratunkiem jest użycie szczepionki bądź zastąpienie uszkodzonego pliku kopią zapasową.
- wirusy towarzyszące – tworzone w językach wysokiego poziomu.
- wirusy plików wsadowych – atakują pliki BAT, COM i EXE, potencjalnie groźne.
- makrowirusy – stosunkowo rzadkie i niegroźne, działają w środowisku Microsoft Office i łatwo je wykryć i zablokować.

… I INNE SZKODNIKI

- konie trojańskie – wykonują szkodliwe operacje w sposób niezauważalny dla użytkownika, najczęściej przenoszone są poprzez popularne gry i programy komputerowe.
- programy szpiegujące – gromadzą informacje o użytkowniku i przesyłają je twórcy programu. Najczęściej zbierane dane to: dane osobowe, numery kart płatniczych, adresy odwiedzanych stron www, hasła, adresy e-mail, wpisywane słowa kluczowe. Do ich wykrywania i eliminowania służą liczne programy typu anty-spy.
- fałszywki – fałszywe ostrzeżenia przed wirusami, rozsyłane drogą mailową z prośbą o rozpowszechnienie lub o usunięcie wskazanego pliku, który często jest częścią systemu operacyjnego użytkownika. W przypadku otrzymania takiego maila, należy sprawdzić na stronie producenta oprogramowania antywirusowego, czy typ wirusa opisany przez nadawcę nie jest rozpoznany jako fałszywka.
- bomby logiczne – wykonują szkodliwe operacje „z opóźnionym zapłonem", czyli jakiś czas po zainfekowaniu obiektu.
- robaki – ich zadaniem jest samo powielanie, które skutkuje zajmowaniem miejsca na dysku użytkownika.
- króliki (inaczej bakterie) – ich celem jest samokopiowanie w postępie wykładniczym, co w efekcie prowadzi do użycia całej mocy obliczeniowej procesora.

Formą ochrony przed wirusami i innym szkodliwym oprogramowaniem jest przede wszystkim ostrożność w otwieraniu nieznanych plików, ściąganiu ich z niesprawdzonej strony. Najlepszą profilaktykę stanowi użycie dobrego oprogramowania antywirusowego oraz praca na oryginalnym oprogramowaniu. Użytkownicy pirackich wersji nie korzystają z aktualizacji producenta, co powoduje, ze nie nabierają odporności na ataki wirusów i robaków, stając się ich nosicielem.

PHISHING

W początkach istnienia zjawiska, wymyślonego przez crackerów w latach 90., wyłudzania haseł do kont służyło możliwości wysyłania spamu. Obecnie phishing ma cel zarobkowy: włamanie na internetowe konto bankowe ofiary i przelanie z niego pieniędzy. Najczęstszą metodą jest wysyłanie maili rzekomo z banku z informacją o dezaktywacji konta czy hasła, i prośbą o jego ponowne podanie. Pretekstem są także aukcje internetowe: wysyła się masowe maile do uczestników aukcji w imieniu banku internetowego, z prośbą o podanie danych konta. W treści maili phishingowych zazwyczaj znajduje się hiperłącze do strony banku – docelowa strona bywa tak łudząco podobna do serwisu prawdziwego banku, że użytkownicy niekiedy dają się nabrać i wpisują w okienka login i hasło, tym samym podając je na tacy oszustom.

Najlepszą formą obrony jest ignorowanie takich maili: banki nigdy nie proszą w taki sposób o weryfikację czy podawanie danych. Logując się przez Internet do własnego konta bankowego, należy także zwracać uwagę, czy w adresie strony widnieje protokół https. Ponadto zaleca się aktualizacje przeglądarki i stosowanie oprogramowania antyphishingowego. Ataku można uniknąć.

PHARMING

To odmiana phishingu, polegająca na przekserowaniu użytkownika na podrabianą stronę – internauta może wpisywać adres strony banku, a trafić na nieprawdziwą, której autorem jest haker. Wpisanie danych logowania daje przestępcom dostęp do konta.

DRIVE-BY-PHARMING

To pharming połączony z metodami socjotechniki: atak polega na nakłonieniu użytkownika do wejścia na konkretną stronę internetową, co powoduje zmiany w systemie DNS na routerze, z którego

korzysta internauta. Na takie ataki narażonych jest prawdopodobnie aż 50% użytkowników z dostępem do szerokopasmowego Internetu. W celu ochrony, należy ustawiać na routerze trudne rozszyfrowania hasła i nie ulegać namowom od nieznajomych do wejścia na nieznane strony www.

SPAM

Nazwa tego internetowego śmiecia pierwotnie oznaczała … konserwową mielonkę wieprzową jedzoną przez amerykańskich żołnierzy.

W odniesieniu do komunikatów elektronicznych nazwy takiej użyto prawdopodobnie po raz pierwszy wobec bezsensownych treści generowanych złośliwie przez graczy tekstowych MUD-ów działających w sieci BBS-ów. Następnie spamem został nazwany sposób zwalczania nielubianych dyskutantów poprzez zasypywanie ich masowo bezsensownymi wiadomościami.

Tym, co łączy spam sieciowy, czyli niechcianą komercyjną wiadomość elektroniczną z konserwą todostarczanie masowo pewnej zawartości, która po otwarciu sprawia niespodziankę…

Mianem spamu określa się każdą wiadomość spełniającą trzy następujące warunki jednocześnie:

- treść jest niezależna od tożsamości odbiorcy,
- odbiorca nie wyraził uprzedniej zgody na otrzymanie takiej wiadomości,
- treść wiadomości sugeruje, że nadawca odniesie wymierną korzyść kosztem odbiorcy.

Warto zwrócić uwagę na to, że korzyść ta nie musi być typowo komercyjna, spamem bowiem określa się też e-maile, które nie przemycają oferty handlowej: apele organizacji społecznych i charytatywnych czy partii politycznych, prośby o pomoc czy masowe rozsyłanie ostrzeżeń, np. o wirusach komputerowych. Takie spamy nazywane są Unsolicited Bulk Email (UBE), natomiast typowy, najbardziej denerwujący – prawnie zabroniony - spam komercyjny, czyli niezamawiana oferta handlowa, nazywany jest Unsolicited Commercial Email (UCE).

Pierwszy spam właściwie nie był śmieciem – 1 maja 1978 Einar Stefferud, korzystając z dostępu do kompletnego zbioru adresów mailowych w sieci ARPANET, wysłał 1000 maili z zaproszeniem na swoje urodziny. W odpowiedzi odbiorcy rozesłali swoje komentarze, które zablokowały twarde dyski nadawcy zaproszenia.

Pierwszy prawdziwy śmieć, czyli niepożądany e-mail reklamowy, został napisany i rozesłany dwa dni później przez producenta mini-komputerów, Gary’ego Thuerka.

W Usenecie pierwszy spam, z tytułem „HELP ME!”, został rozesłany w 1988 roku przez Roba Noha. W poście tym prosił o pomoc finansową dla swojego kolegi, któremu zabrakło funduszy na kontynuowanie studiów.

Etykietkę spamera przylepiono Richardowi Depew, który stworzył skrypt kasujący z listy USENET-u wszystkich użytkowników łamiących netykietę. Niestety, skrypt wymknął się spod kontroli. Ale skutki spamowania po raz pierwszy odczuto, gdy firma adwokacka Lawrence’a Cantera oraz Marthy Siegel z Phoenix, rozesłała ofertę usług w zakresie wypełniania formularzy amerykańskiej loterii wizowej. Na skutek negatywnej reakcji użytkowników sieci, administrator zablokował firmie dostęp do kont pocztowych.

Największa liczba wiadomości spamowych według firmy Sophos pochodzi ze Stanów, dalej są Chiny, Polska, Korea Południowa, Włochy.

Mimo zabezpieczeń, spamy zasypują nas masowo – ich nadawcy należą do bardzo kreatywnych spryciarzy. Mówi się więc o metodach rozsyłania wiadomości poprzez podszywanie się pod na bank czy inną budzącą zaufanie instytucją albo tytułowanie wiadomości „dostałeś spadek" czy „wygrałeś milion". Trudno uwierzyć, ale wielu daje się na to nabrać.

Żadna forma natrętnej reklamy nie jest pożądana, spam jest ponadto niebezpieczny, ponieważ:

- blokuje miejsce na twardych dyskach,
- spowalnia serwery ich działanie,
- powoduje stratę czasu poszczególnych użytkowników Internetu,
- stwarza ryzyko utraty normalnej poczty z powodu blokad antyspamowych, przepełnienia skrzynki lub niezauważenia,
- powoduje dodatkowe koszty dla operatorów internetowych i odbiorców korespondencji, narusza prywatność i bezpieczeństwo odbiorców,
- wiąże się często z różnego rodzaju wirusami i innymi złośliwymi programami, powoduje utratę zaufania do komunikacji elektronicznej jako takiej.

Aby zabezpieczyć się przed niechcianą pocztą, warto na skrzynkach mailowych instalować filtr antyspamowy. Stosunkowo skutecznie odsiewa on wiadomości od nieznanych nadawców, z dziwnych adresów bądź z tematami typu: „Blue pills".

CYBERSQUATTING

Każda domena, szczególnie ta oparta na potocznej nazwie, np. www.buty.pl, zagrożona jest cybersquattingiem – praktyką przejęcia jej albo zarejestrowania z innym rozszerzeniem i odsprzedawania po zawyżonej cenie. Przyczyną podkupywania i przejmowania domen oraz rejestrowania ich z inną nazwą jest fakt, iż do legalnego kupienia pozostaje coraz mniej marketingowo atrakcyjnych nazw - język polski jest przecież bogaty, ale słownikowo ograniczony. Na rynku wtórnym, czyli u cybersquattera, który za kilka złotych kupił domenę z niewykorzystanym dotąd rozszerzeniem albo przejął domenę nieprzedłuzoną na czas przez dotychczasowego właściciela i chce ją odsprzedać z dużym zyskiem, dobrych nazw jest za to mnóstwo. Trzeba tylko zaproponować odpowiednią kwotę…

Problemu by nie było, gdyby każde przedsiębiorstwo chciało w domenie mieć swoją nazwę - ale z różnych względów nie każde chce. Marketerzy polują na nazwy odzwierciedlające charakter oferty - tak, by klientowi zapadła w pamięć jako synonim poszukiwanego produktu.

Spory co do własności domeny czy zawartego w nazwie słowa – znaku towarowego są rozstrzygane w ramach procesu Uniform Domain Name Resolution Policy (UDRP) opracowanego przez Internet Corporation for Assigned Names and Numbers (ICANN) bądź przez sądy. Ustawodawstwo wielu krajów traktuje nazwę domeny jako znak towarowy i takie też przepisy (i restrykcje) dotyczą cybersquattingu.

Zjawisko ma charakter narastający. Liczba skarg kierowanych do Światowej Organizacji ds. Własności Intelektualnej rośnie z roku na rok.

Co ciekawe, najwięcej przypadków cybarsquattingu zdarza się w odniesieniu do produktów farmaceutycznych – ziół czy zarejestrowanych leków. Cierpią na tym apteki internetowe. Inne branże, których ten problem dotyka najczęściej, to sektor finansowy i przemysł.

W celu zabezpieczenia swoich interesów marketingowych i wizerunkowych, właściciel domeny powinien rejestrować ją z wszelkimi logicznymi rozszerzeniami. Ma to swoje uzasadnienie także w kontekście globalizowania się rynków i wychodzenia z ofertą na głębsze wody.