Jaromir Bogacz

Ciemna strona Internetu

To był jeden z internetowych hitów 2006 roku. Na amatorskim nagraniu widać jak Ghyslain Raza, pulchny 15-latek, z wielkim zaangażowaniem wymachuje drągiem udając, że jest jednym z rycerzy Jedi. Kiedyś taki film skończyłby pewnie jako niewinny dowcip, przypominany przez krewnych, ku zażenowaniu głównego bohatera. Pech chciał, że jeden z kolegów postanowił skorzystać z możliwości oferowanych przez nowe technologie i umieścił film w Internecie. Autor znany od teraz jako „Star Wars Kid" niemal od razu stał się obiektem kpin milionów ludzi na całym świecie. Wyśmiewany przez kolegów przestał chodzić do szkoły i znalazł się pod opieką psychologa. Rzeczywiście trudno sobie nawet wyobrazić wstyd dziecka, które przez głupi żart staje się pośmiewiskiem – dosłownie – całego świata.

Ta historia bardzo dobrze pokazuje nowe problemy, jakie pojawiły się wraz z rozwojem Internetu, i nowe wyzwania, jakie stoją przed pedagogami. Pytani o zagrożenia w sieci, niektórzy natychmiast wyobrażają sobie wirusy błyskawicznie przeskakujące z komputera na komputer i niszczące nasze dane. Inni przede wszystkim dostrzegają jakieś ciemne zakamarki Internetu – strony pełne przemocy lub pornografii dziecięcej. I dobrze, bo to wciąż są aktualne problemy. Ale ich rozwiązanie należy w dużej mierze do policji i informatyków, a nauczyciel może przed nimi co najwyżej ostrzegać.

Natomiast przygotowanie uczniów do życia w wirtualnym społeczeństwie, to przede wszystkim rola pedagogów. Internet już dawno przestał być tylko źródłem pożytecznych informacji, a stał się zupełnie nowym środowiskiem, w którym możemy robić zakupy, wymieniać plotki i zawierać znajomości. Tylko że ten drugi świat rządzi się swoimi prawami, a to co nam (albo naszym uczniom) wydaje się bezpieczne w świecie rzeczywistym, nie musi być takie w jego wirtualnym odpowiedniku. W powyższym przykładzie zachowanie kolegów miało być zapewne głupim żartem, a jednak już na zawsze naznaczyło kanadyjskiego nastolatka.

Żyjemy w świecie, w którym dane w tempie błyskawicy okrążają świat. Coraz rzadziej mamy pewność, jak naprawdę wygląda i reaguje osoba, z którą rozmawiamy, a każda przypadkowo ujawniona informacja może zostać w Internecie już na zawsze. Często nie zdajemy sobie sprawy zarówno z możliwości, jak i zagrożeń, jakie to stwarza. Tym bardziej nie są ich świadomi (lub o nich nie myślą) uczniowie. W Wielkiej Brytanii rząd zdecydował się wprowadzić do obowiązkowego programu szkoły podstawowej kurs uczący dzieci bezpiecznego zachowania w sieci. Program brytyjski, prowadzony pod hasłem „Zip it, Block it, Flag it"[1] uczy dzieci:

- ochrony prywatności (*zip it* – tu w znaczeniu: trzymaj buzię zamkniętą na kłódkę),
- radzenia sobie z agresją innych użytkowników sieci (*block it* – blokuj tych, którzy sprawiają, że czujesz się nieswojo),
- radzenia sobie z niechcianymi treściami (*flag it* – oznacz i poinformuj opiekuna, gdy się na takie natkniesz).

W swoim krótkim opisie podstawowych zagrożeń, jakie stoją przed uczniami, do tej listy dodałem wciąż jeszcze aktualny problem złośliwego oprogramowania.

Prywatność

Większość z nas pewnie pamięta billboardy i spoty reklamowe z opasłym panem w przykrótkiej koszulce, przedstawiającym się na czacie jako „Wojtek, lat 12". Niewątpliwie kampanii prowadzonej pod hasłem „Nigdy nie wiadomo, kto jest po drugiej stronie" udało się wzbudzić społeczne zainteresowanie. I bardzo dobrze, bo ta wcale nieoczywista dla małego dziecka prawda, stanowi dobry początek do rozmowy o bezpiecznym przeglądaniu Internetu.

[1] Na stronie programu (http://clickcleverclicksafe.direct.gov.uk/index.html) można uzyskać informacje, czego brytyjskie dzieci będą się uczyły w ramach zajęć z bezpieczeństwa w Internecie.

Właśnie dlatego, że nigdy nie wiadomo, kto jest po drugiej stronie, dziecko nie powinno ujawniać żadnych wiadomości prywatnych (adresu, numeru telefonu czy nawet imienia i nazwiska – lepiej, żeby surfując, korzystało z jakiegoś *nicka*). Kolejnymi zasadami, jakie Perry Aftab wymienia w książce „Internet a dzieci. Uzależnienie i inne niebezpieczeństwa[2]", są niespotykanie się bez zgody rodziców z osobami poznanymi przez Internet oraz informowanie rodziców o osobach poznanych w sieci. Te reguły powinny być dla dziecka jasne, gdy zaczyna swoją przygodę z Internetem.

Ujawnianie poufnych informacji, to nie tylko problem małych dzieci. Starsi użytkownicy okazują się równie podatni na podobne zagrożenia, jeśli tylko prośba o ich dane zostanie sformułowana trochę bardziej formalnie. Jedna z najpopularniejszych obecnie metod stosowanych przez *hackerów*, zwana *phishingiem* (co po polsku znaczy mniej więcej tyle co łowienie haseł), polega na masowym wysyłaniu formalnie wyglądających wiadomości z prośbą o podanie numeru i hasła do naszego konta bankowego, np. z powodu rzekomej weryfikacji. Zwykle podany jest link, który prowadzi na przygotowaną wcześniej przez *hackera* stronę, łudząco podobną do oryginalnej witryny banku. Ta prosta metoda niestety okazuje się bardzo skuteczna – na tyle, że dał się na nią nabrać nawet sam dyrektor FBI Robert Mueller.

W przypadku starszych uczniów nie mają sensu tak mocne ograniczenia, jak te proponowane przez Perry'ego Afaba. Ważniejsze jest, aby uświadamiać im, jak ważna jest umiejętność decydowania, które informacje powinny być dostępne publicznie. W badaniach amerykańskiej firmy Career Builder okazało się, że 45% pracodawców sprawdza informacje o kandydatach w sieci, a 35% odrzuca podania pod wpływem informacji tam znalezionych. W dodatku te liczby podwoiły się w porównaniu z rokiem ubiegłym[3].

Nawet kiedy nasz profil jest dostępny tylko dla znajomych, nic to nie zmieni, jeśli nie będziemy zachowywali innych środków ostrożności. W grudniu 2009 roku reporterzy „Dziennika" w ramach prowokacji założyli fikcyjne konta na Naszej Klasie i Facebooku i wysyłali zaproszenia losowo wybranym użytkownikom[4]. Okazało się, że prawie co trzeci z nich potwierdził swoją znajomość z zupełnie obcą sobie osobą i dał jej dostęp do wszystkich swoich danych. Zadziałał tu prosty mechanizm wzajemności – skoro ty mnie uważasz za znajomego, to choć cię nie pamiętam, zaprzeczenie znajomości byłoby nieuprzejme.

Na koniec warto też pomyśleć o jakimś dobrym haśle, czymś bardziej kreatywnym niż „abc123" lub *password* (hasło) – te dwa należą do najczęściej używanych w sieci. Bywa, że *hackerzy* szukają słabo zabezpieczonych kont na portalach społecznościowych, korzystając z listy najpopularniejszych haseł. Później wykorzystują te konta np. do rozsyłania spamu wśród znajomych ofiary.

Agresja

Na lekcjach bezpieczeństwa internetowego brytyjskie dzieci, poza poznaniem zasad zachowania prywatności, dowiadują się, jak reagować na agresywne zaczepki i niechciane treści. Nawet w zwykłych dyskusjach prowadzonych w Internecie poziom agresji jest dużo wyższy niż poza nim. Naukowcy próbowali to zjawisko wytłumaczyć na różne dziwne sposoby, np. frustracją z powodu wolnego przepływu danych, który jakoby uniemożliwiał płynną rozmowę.

Patricia Wallace[5] próbuje tłumaczyć takie zachowania poczuciem bezkarności, jakie daje anonimowość, oraz brakiem komunikacji niewerbalnej. Gdy nie widzimy reakcji wywołanej przez nasze słowa, dużo trudniej o empatię.

Czy agresja „sieciowa" może przenieść się do realnego świata? Odpowiedź wcale nie jest oczywista – duża część internautów traktuje te wirtualne „pyskówki" (*flame war*) niezupełnie serio, jako pewną konwencję, charakterystyczną dla nowego medium. Bardzo często któryś z nich celowo umieszcza prowokacyjny wpis (takie działanie nazywane jest *trollingiem*), aby wywołać „pyskówkę". Niektóre portale są nawet podejrzewane o zatrudnianie zawodowych *trolli*, aby pobudzić dyskusję na swoim forum (jak choćby w przypadku Jasia Śmietany na forum Onetu).

Problemy zaczynają się, gdy internauci zjednoczą się przeciw pewnej grupie (zwłaszcza na polskich forach bardzo dużo jest wątków rasistowskich, homofobicznych itd.) lub, co gorsza, przeciw konkretnej osobie. To ostatnie zjawisko nazwane zostało *cyberbullyingiem* (czyli „nękaniem w sieci"). W polskim Internecie gwałtowna dyskusja na ten temat przetoczyła się po opublikowaniu

[2] Aftab P. *Internet a dzieci. Uzależnienia i inne niebezpieczeństwa*, Prószyński i S-ka, Warszawa 2003.
[3] www.careerbuilder.com
[4] Czubkowska S. *Tak Polacy obnażają się w sieci* (http://www.dziennik.pl/wydarzenia/article513430/Tak_Polacy_obnazaja_sie_w_sieci.html).
[5] Wallace P. *Psychologia Internetu*, Rebis, Poznań 2001.

w „Dużym Formacie" reportażu Magdaleny Grzebałkowskiej[6] o gdańskiej licealistce, która naraziła się klasowej elicie, a w konsekwencji była przez nią wyśmiewana i obrażana na jednym z portali internetowych. Łatwo można przytoczyć przypadki dużo bardziej drastyczne, ale ten wydaje się szczególnie interesujący właśnie ze względu na ową dyskusję. Okazało się, że bardzo duża część internautów zbagatelizowała problem, zresztą podobnie jak rodzice napastliwych nastolatków. Pojawiły się głosy, że gazeta rozdmuchała niewinny w sumie incydent – obmawianie jednych uczniów przez innych nie jest oczywiście niczym chwalebnym, ale też niczym nowym – nowe jest tylko medium.

A jednak zmiana medium tylko pozornie jest zupełnie nieznacząca. W opisanym przypadku u ofiary oprócz poczucia odtrącenia i winy (co sprawiło, że właśnie na mnie się uwzięli?), dołącza się wstyd z publicznego charakteru poniżenia. Sytuacja, w której każdy człowiek może bez żadnych kosztów opublikować informację na całym świecie, jest czymś absolutnie bezprecedensowym. Wszelkie analogie z wcześniejszymi mediami zawodzą – umieszczenie czegoś na blogu nie jest tym samym co opisanie zdarzenia w pamiętniku, a obmowa w dyskusji na forum to nie to samo co w telefonicznej rozmowie. Przynajmniej częścią odpowiedzialności, która kiedyś spoczywała tylko na dziennikarzach i osobach publicznych, zostają teraz obarczone dzieci. I dlatego właśnie niezbędna jest edukacja medialna. O wadze problemu niech świadczą dane pochodzące z badań firmy Gemius dla Fundacji Dzieci Niczyje przeprowadzonych wśród kilkuset osób w wieku 12-17 lat i przytoczone przez „Gazetę Wyborczą"[7]. Co drugi z respondentów (52%) miał do czynienia z jakimś rodzajem agresji w Internecie lub poprzez komórkę. Co piąty badany (21%) był w Internecie ośmieszany, poniżany lub upokarzany. Straszenia i szantażu doświadczyło 16% badanych.

Pornografia

Strony pornograficzne nieodmiennie zajmują pierwsze miejsce pośród zagrożeń wymienianych przez rodziców, których dzieci korzystają z Internetu[8]. Z danych przytaczanych przez Aleksandrę Jaszczak w artykule „Cyberedukacja seksualna i cyberseks młodzieży"[9] wynika, że spośród badanych, których średnia wieku wynosiła 19 lat, zaledwie 22% nigdy nie przeglądało stron pornograficznych w celu osiągnięcia satysfakcji seksualnej, a aż 67% przyznało, że wiedzę na tematy związane ze sferą seksualną czerpało m.in. właśnie z oglądania pornografii. Gdy naukowcy z Montrealu chcieli przeprowadzić badania nad wpływem pornografii na młodych mężczyzn, musieli się wycofać, ponieważ… nie znaleźli żadnego mężczyzn, który by takich materiałów nie oglądał.

Dostęp do pornografii powoli staje się więc czymś powszechnym. Jakie to będzie miało skutki? Naukowcy raczej nie wieszczą katastrofy, choć przyznają, że w różnych badaniach widać pewną zależność pomiędzy oglądaniem przez nastolatków pornografii a oddzielaniem seksu od uczuć i traktowaniem go jako zwykłej fizjologicznej potrzeby. Dużo większym problemem pozostaje dostępność tzw. twardej pornografii (z użyciem przemocy). Patricia Wallace przytacza eksperymenty potwierdzające jej wpływ na poziom agresji, zwłaszcza względem kobiet, a to tylko wierzchołek góry lodowej. Internet jest pełen materiałów pedofilskich, wzywających do przemocy czy nawet uczących, jak skonstruować bombę. Niestety na takie strony można się natknąć zupełnie przypadkowo, wpisując całkiem niewinne hasła do wyszukiwarki. Dlatego, aby małe dzieci mogły bezpiecznie przeglądać Internet, niezbędne są programy blokujące niepożądane strony – a i tak warto ostrzec dzieci przed możliwym zagrożeniem i nauczyć je, co powinny w takim wypadku zrobić (rozłączyć się i porozmawiać z opiekunem). Starszym uczniom warto podać adres strony, gdzie mogą zgłaszać treści niezgodne z prawem – np. dyzurnet.pl. Trzeba też pamiętać, że jeśli uczniowie będą chcieli wejść na zakazaną stronę, programy filtrujące mogą nie wystarczyć. Często można je w prosty sposób obejść przy pomocy serwerów Proxy, łączących się z żądaną stroną i przesyłających jej treść na dany komputer.

Niestety próba zwalczania ciemnej strony Internetu przypomina czasem wysiłki Syzyfa. W 2006 roku, po dużej kampanii medialnej udało się doprowadzić do zamknięcia strony RedWatch, na której faszyści nawoływali do ataków na „zdrajców białej rasy", prezentując zdjęcia i adresy znienawidzonych przez siebie działaczy społecznych i dziennikarzy. Niedługo później witryna wróciła do sieci – została przeniesiona na inny serwer. Sprawę utrudnia fakt, że strona funkcjonuje na serwerach amerykańskich i do jej każdorazowego zamknięcia potrzebna jest koordynacja działań z FBI. To oczy-

6 Grzebałkowska M. *Żal mi dziewczyny z mojej klasy*, Duży Format, 25.06.2008.
7 Domaszewicz Z. *Czy cyberbullying zniszczy anonimowość w internecie*? (http://wyborcza.pl/1,86669,4299345.html).
8 Por. np. badanie „Mądry Internet".
9 Jaszczak A. *Cyberedukacja seksualna i cyberseks młodzieży* [w:] Szmigielska B. [red.] *Całe życie w Sieci*, WUJ, Kraków 2008, s. 95-136.

wiście nie oznacza, że niewielki wysiłek podjęty w celu przeciwdziałania faszystom, pedofilom itp. nie jest wart zachodu. Specyfika Internetu polega jednak na tym, że dużo łatwiej w nim coś umieścić, niż później stamtąd usunąć.

Złośliwe oprogramowanie

Kto tworzy wirusy? Wciąż panuje wyobrażenie, że jest to sprawka genialnych nastolatków, którzy z nudów, chęci sprawdzenia się czy też czystej złośliwości bawią się *hackingiem*. Jak w wywiadzie dla „Computerworld" tłumaczy znany amerykański ekspert do spraw bezpieczeństwa Bruce Schneider[10], czasy samozwańczych naśladowców Neo z „Matrixa" mamy już dawno za sobą. Teraz atakami na komputery zajmują się głównie zorganizowane grupy przestępcze. Jakie znaczenie ma dla przeciętnego internauty wiadomość, kto go atakuje? Wbrew pozorom spore, bo równocześnie zmienił się charakter zagrożeń. Coraz rzadsze są wirusy, które np. niszczą dane. Współczesne wirusy wyszukują w sieci słabiej zabezpieczone komputery, włamują się do nich i… początkowo nie robią nic. Takie przejęcie kontroli nad komputerem ma zazwyczaj jeden z dwóch celów: może chodzić o zdobycie poufnych danych, przede wszystkim numerów kart kredytowych, np. poprzez zainstalowanie programów odczytujących każdy naciśnięty klawisz. Drugim motywem może być chęć uczynienia z naszego komputera *zombie*, czekającego na rozkaz swojego pana. Takie komputery łączone są w sieci zwane botnetami i mogą zostać wykorzystane do masowego rozsyłania spamu bądź ataków na wybrane strony.

Niewątpliwie kluczem do sukcesu dla *hackera* jest ukrycie włamania. W badaniu przeprowadzonym przez American Online okazało się, że ponad 66% posiadaczy zawirusowanych komputerów nie jest świadomych obecności wirusa. Dlatego nie ma sensu zabezpieczanie komputera dopiero, gdy zauważymy jakieś nieprawidłowości – wtedy będzie już na to za późno. Specjaliści od bezpieczeństwa komputerowego ze złością mówią o użytkownikach, którzy lekceważąc podstawowe zasady bezpieczeństwa, nie tylko zagrażają sobie, ale mimowolnie pomagają cybergangsterom. A zasady te są rzeczywiście proste: wgrywanie dostępnych aktualizacji i zaopatrzenie się w dobry, koniecznie regularnie uaktualniany program antywirusowy z *firewallem*. Warto też unikać podejrzanych stron (zwłaszcza z pirackim oprogramowaniem) i w żadnym wypadku nie instalować programów niewiadomego pochodzenia. Częstym trickiem *hackerów* jest przedstawianie wirusa jako... antywirusa. Po wejściu na stronę pojawia się informacja o wykrytym robaku i propozycja instalacji programu, który zagrożenie usunie.

Na zakończenie

Nie ma sensu spierać się o wady i zalety Internetu – i tak stał się medium, do którego przenosi się coraz większa część naszego życia. A jeśli nawet nie naszego, to na pewno naszych uczniów. I niewątpliwie to się już nie zmieni. Dlatego warto wiedzieć, co powinno nam się wydawać podejrzane i jakie działania mogą być niebezpieczne – bo tu, tak jak w rzeczywistym życiu, zagrożenia czekają przede wszystkim na tych, którzy są ich nieświadomi. Przed nauczycielami i rodzicami stoi niemałe wyzwanie – uczyć dzieci i młodzież podstawowych zasad korzystania z nowego medium, aby Internet, mimo ciemnych stron, stawał się coraz szerzej otwartym oknem na świat informacji.

Autor jest absolwentem informatyki UJ, studentem filmoznawstwa

Gry oznaczone tym znakiem uznaje się za odpowiednie dla wszystkich grup wiekowych. Dopuszczalna jest pewna ilość przemocy w komicznym kontekście. W grze nie występują dźwięki i obrazy, które mogą przestraszyć dziecko oraz wulgaryzmy, nagość ani odwołania do czynności seksualnych.

Przykładowe gry z tej grupy: Super Mario Galaxy, Catz, SingStar.

[10] Schneier B. *Bezpieczeństwo nie jest sexi* (http://www.pcworld.pl/news/144463/Bruce.Schneier.Bezpieczenstwo.nie.jest.sexi.html).