AUGUSTYN SURDYK

PODSTAWY INŻYNIERII BEZPIECZEŃSTWA W KSZTAŁCENIU ZAWODOWYM NAUCZYCIELI JĘZYKÓW OBCYCH

1. WSTĘP

Funkcjonowanie w „społeczeństwie informacyjnym" w XXI wieku, z dawna zapowiadanym jako wiek komunikacji, wymaga stałego nadążania za nowinkami technologicznymi, zwłaszcza w dziedzinie komunikacji międzyludzkiej i informacji oferowanymi głównie przez *world wide web*. W krajach rozwiniętych internet już w ostatniej dekadzie ubiegłego wieku stał się najpopularniejszym źródłem informacji, wiadomości ze świata i podstawowym, jednocześnie najszybszym i najtańszym, medium komunikacji. Coraz większa liczba osób rezygnuje z dotychczas dominujących mediów (jak telewizja radio, prasa) oraz środków komunikacji (np. telefon, fax) na rzecz mediów dostępnych online. Same media również szybko zrozumiały, że funkcjonowanie wyłącznie w tradycyjnej formie nie jest już wystarczające. Dlatego drukowanym wydaniom gazet coraz częściej towarzyszą wydania internetowe, a stacje telewizyjne i radiowe są dostępne również w sieci. Media zaś, dotąd występujące pojedynczo, łączą się w koncerny medialne oferując kompletne, współdziałające i skoordynowane grupy (portal internetowy, telewizja, radio, prasa). Wzrastająca w zawrotnym tempie liczba mediów służących komunikacji przez internet (w tym komunikatorów, list dyskusyjnych, forów, portali społecznościowych itp.) niejako zmusza osoby chcące nadążyć za rozwojem oferowanych przez nie możliwości kontaktu do ciągłego ich odkrywania. Każda forma użytkowania internetu, zwłaszcza nowa, nie jest jednak pozbawiona zagrożeń, a niestety znakomita większość użytkowników sieci nadal nie zdaje sobie z nich sprawy lub wykazuje znikomą świadomość w tej materii. Nauczyciele języków obcych, a także studenci oraz absolwenci studiów neofilologicznych pracujący coraz częściej również w innych zawodach (poza sferą edukacji), jak wszyscy inni obywatele są użytkownikami internetu i poczty elektronicznej i jak wszyscy inni ludzie są niestety w równym stopniu narażeni na zagrożenia płynące z wykorzystywania tych mediów,

czy to dla celów osobistych czy na użytek pracy zawodowej. Należy przy tym dodać, że nie wszyscy absolwenci studiów neofilologicznych są przygotowani w toku studiów do wykonywania zawodu nauczyciela, lecz nawet spośród absolwentów specjalizacji nauczycielskich nie wszyscy wybierają tę profesję. Skala tego zjawiska jest tak duża, iż można by powiedzieć, że spośród absolwentów neofilologii nauczyciele wkrótce mogą znaleźć się wręcz w mniejszości. Wzrastająca z roku na rok liczba specjalności i specjalizacji w ramach kierunków neofilologicznych na uczelniach krajowych stwarza coraz większe możliwości kształcenia i przygotowania do pracy w wielu innych zawodach poza sferą edukacji. Wśród absolwentów neofilologii wzrasta liczba tłumaczy (działających w różnoraki sposób – od jednoosobowych firm poprzez zorganizowane biura tłumaczy do zatrudnionych w strukturach Parlamentu Europejskiego w Brukseli włącznie) oraz innych specjalistów znajdujących zatrudnienie w wielu dziedzinach gospodarki i życia publicznego. Ostatecznie nie można też wykluczyć, że absolwent neofilologii sam zostanie (euro)posłem, członkiem gabinetu rządowego lub innym wysoko postawionym urzędnikiem państwowym, przy pełnieniu których to urzędów znajomość języków obcych jest wielce pożądana, choć, jak wskazuje praktyka ostatnich dekad, nadal niestety pozostawia wiele do życzenia.

W każdym z zawodów absolwenci neofilologii mogą wykorzystywać internet i pocztę elektroniczną na użytek prywatny oraz korzystać z tych mediów w celach służbowych (w tym z użyciem prywatnych bądź służbowych komputerów). O ile jednak padnięcie ofiarą **cyberprzestępstwa** osoby prywatnej z powodu jego wymiaru indywidualnego może nie być zbyt groźne, choć bywa dotkliwe dla bezpośrednio zainteresowanego (np. w przypadku kradzieży pieniędzy z konta, utraty danych lub uszkodzenia bądź zniszczenia oprogramowania lub nawet sprzętu komputerowego), o tyle padnięcie ofiarą przestępstw popełnianych za pośrednictwem sieci przy wykorzystaniu komputerów służbowych, często dysponujących dostępem do wewnętrznej sieci – intranetu – i baz danych (w tym niejawnych, poufnych, utajnionych lub ściśle tajnych) firmy (np. banku, firmy ubezpieczeniowej itp.), korporacji, czy instytucji administracji państwowej może mieć poważne konsekwencje w wymiarze globalnym (w ostatecznym rozrachunku również dla bezpieczeństwa państwa), przybierając formę **cyberterroryzmu**. Dlatego edukacja jednostki w zakresie bezpiecznego korzystania z internetu i poczty elektronicznej oraz potencjalnych zagrożeń z nimi związanych może okazać się kluczowym elementem globalnej polityki prowadzonej w ramach projektowania inżynierii bezpieczeństwa na różnych płaszczyznach. Co więcej, w dobie gwałtownie postępującego rozwoju technologicznego i pojawiających się coraz to nowszych form komunikacji przez internet, edukacja ta powinna przyjmować formę powszechną, obowiązkową i winna rozpoczynać się na jak najwcześniejszych

szczeblach szkolnictwa[1]. Programy szkolne i standardy studiów pozwalają na przekazywanie tej wiedzy w ramach wybranych istniejących przedmiotów, jednak niestety brak jest wykwalifikowanych specjalistów, którzy byliby przygotowani do prowadzenia takich zajęć czy szkoleń w profesjonalny i rzetelny sposób.

Autor niniejszego artykułu będąc wykładowcą akademickim podjął działania w kierunku podwyższenia świadomości studentów kierunku filologia-lingwistyka stosowana w zakresie potencjalnych zagrożeń, jakie niesie ze sobą wykorzystanie internetu i poczty elektronicznej. Z jego inicjatywy w macierzystym Instytucie Lingwistyki Stosowanej Wydziału Neofilologii Uniwersytetu im. Adama Mickiewicza w Poznaniu do programu studiów niestacjonarnych drugiego stopnia na wspomnianym kierunku dla specjalności glottodydaktycznej (nauczycielskiej) wprowadzono w roku akademickim 2007/2008 przedmiot fakultatywny „Multimedia w kształceniu obcojęzycznym". W ramach tego przedmiotu studenci poza nabywaniem wiedzy z zakresu wykorzystania nowych technologii w nauczaniu języków obcych zapoznawani są z podstawowymi wiadomościami ze wspomnianego wyżej zakresu i informowani o sposobach zapobiegania owym zagrożeniom. Ponadto podobny zakres tematyczny, choć w znacznie większym wymiarze godzin, ma kurs dokształcający dla nauczycieli języków obcych pod nazwą „Nowe technologie w nauczaniu języków obcych" powołany do życia we wspomnianym instytucie również z inicjatywy autora w roku akademickim 2009/2010. Inny kurs dokształcający skierowany do nauczycieli języków obcych i zainicjowany również przez autora w tym samym roku – „Konstruowanie gier edukacyjnych w nauczaniu języków obcych" – choć dotyczący odmiennej tematyki, jednak znajdującej się w sferze nowych technologii, lecz bardziej zawężonej do tytułowego zakresu, także przekazuje m.in. te informacje o ww. zagrożeniach. Fakt podjęcia przez autora działalności w tym zakresie w ramach kształcenia nauczycieli języków obcych uwarunkował temat niniejszego artykułu w obecnym kształcie, jednak równie dobrze tytułowe zagadnienie można by rozszerzyć do kształcenia studentów neofilologii ogólnie. Programy studiów neofilologicznych, bowiem, w przeciwieństwie do wielu innych kierunków humanistycznych, stwarzają większe możliwości przekazywania wiadomości tego typu w powiązaniu z praktyczną wiedzą zawodową (w tym wypadku z zakresu zastosowania nowych technologii, platform e-learningowych itp. w glottodydaktyce), choć znalezienie podobnych możliwości w przypadku innych kierunków prawdopodobnie zależy

[1] Na niższych szczeblach edukacji np. podczas lekcji informatyki, w szkolnictwie wyższym na zajęciach o pokrewnej tematyce, w tym dodatkowo w zakresie uświadamiania nieletnich i ich rodziców o innych niebezpieczeństwach grożących im w internecie (np. uzależnienia, hazard, pedofilia, pornografia, przemoc, uprowadzenia itp.) i sposobach ich unikania.

w dużej mierze od otwartości i dobrej woli dyrekcji poszczególnych jednostek i wykładowców. Paradoksalnie jednak, mimo tego, iż program filologicznych studiów nauczycielskich przewiduje już na pierwszym stopniu kształcenia (studiów licencjackich) przedmiot „Technologie informacyjne"[2] większość nauczycieli nie jest we właściwy sposób wyedukowana w tym zakresie i nie przejawia potrzeby wykorzystania nowych technologii w swojej praktyce dydaktycznej ani też potrzeby dokształcania się (Drews, 2008) tłumacząc to brakiem zmotywowania niskim poziomem zarobków z jednoczesnym brakiem środków na samodokształcanie się i nadmiarem obciążeń wynikających z obowiązków zawodowych i podyktowanych wymogami ścieżki awansu zawodowego nauczyciela.

Problem zagrożeń płynących z użytkowania internetu jest niewątpliwie istotny, ponieważ mimo stale zwiększającej się dostępności internetu zdarza się, że jego użytkownicy mają często kłopoty z obsługą nawet podstawowych funkcji skrzynki pocztowej (jak np. przesyłanie i odbieranie załączników), lub zwykłą edycją tekstów, co wydaje się niedorzeczne (zwłaszcza w przypadku zawodów wymagających stałej pracy z tekstem), a jednak ma miejsce. I nie dotyczy to, jakby się wydawało, jedynie starszych wiekiem użytkowników sieci, lecz występuje niezależnie od wieku. Zatem nie powinno dziwić, że osoby takie mogą całkowicie nie orientować się w dynamicznie rozwijających się technikach cyberprzestepstw.

W dalszej części artykułu zostaną przedstawione i pokrótce omówione najważniejsze z zagrożeń prezentowanych w ramach wspomnianych przedmiotów i kursów, a następnie sposoby zapobiegania ich występowaniu. Niestety, prawdopodobnie z powodu dynamiki rozwoju zjawiska, brak jest fachowych i zarazem naukowych publikacji i kompleksowych opracowań na ten temat, nadążających za zmieniającymi się i wciąż pojawiającymi się nowymi strategiami, metodami i technikami m.in. spamowania. Tak więc całkiem zrozumiałym jest, iż zjawiska ściśle związane z aktywnością w internecie, jak *spamming, hacking* i ich odmiany, towarzyszące mu od początku

[2] Zgodnie ze standardami kształcenia na kierunku filologia programy nauczania powinny przewidywać zajęcia z zakresu technologii informacyjnej – w wymiarze 30 godzin, którym należy przypisać 2 punkty ECTS. Treści kształcenia w zakresie technologii informacyjnej mają obejmować: podstawy technik informatycznych, przetwarzanie tekstów, arkusze kalkulacyjne, bazy danych, grafika menedżerska i/lub prezentacyjna, usługi w sieciach informatycznych, pozyskiwanie i przetwarzanie informacji – powinny stanowić co najmniej odpowiednio dobrany podzbiór informacji zawartych w modułach wymaganych do uzyskania Europejskiego Certyfikatu Umiejętności Komputerowych (ECDL – European Computer Driving Licence). Pomijając fakt, że przekazanie wszystkich tych treści kształcenia i nauczenie studentów poszczególnych umiejętności (np. nauka obsługi arkuszy kalkulacyjnych i baz danych) w ciągu 30 godzin zajęć graniczyłoby z cudem (zwłaszcza w przypadku nauki od podstaw), niestety wśród zalecanych treści nie ma ani słowa o środkach bezpieczeństwa w korzystaniu z internetu, co stanowiłoby niewątpliwie bardziej użyteczną i praktyczną wiedzę.

jego istnienia również tam zostały najwcześniej zdefiniowane (niewykluczone, że również z udziałem samych spammerów i hackerów), dlatego poniższe informacje w dużej mierze oparte są na wiadomościach zaczerpniętych z polsko- i anglojęzycznych stron wolnej encyklopedii Wikipedia[3].

2. SPAMMING

Termin *spam* odnosi się do niechcianej i najczęściej niepotrzebnej poczty przesyłanej drogą elektroniczną, za pośrednictwem USENETu (ang. ***USEr NETwork*** – sieć użytkowników, ogólnoświatowy system grup dyskusyjnych), coraz częściej również poprzez komunikatory internetowe typu Gadu-gadu, ICQ itp. (ang. *instant messaging spam*), wyszukiwarki internetowe typu Google, Yahoo itp. (ang. *Spamdexing, search spam, search engine spam, web spam*) – w celu uzyskania lepszego pozycjonowania/indeksacji konkretnego hasła w danej wyszukiwarce, blogi internetowe (ang. *blog spam, blam*), wikipedię, reklamy zamieszczane w sieci (ang. *online classified ads spam*), dyskusyjne fora internetowe, portale społecznościowe, programy i platformy sieciowe służące wymianie plików typu *peer-to-peer / P2P* (ang. *file sharing network spam*), sieciowe gry komputerowe, lecz również odnosi się do faksów, reklam telewizyjnych, a nawet informacji rozpowszechnianych za pomocą krótkich wiadomości tekstowych (SMS) przesyłanych na telefony komórkowe (ang. *SpaSMS*). Najbardziej charakterystyczną cechą *spamu* jest to, iż jest to wiadomość rozsyłana masowo do nieznanych adresatów, niezależnie od jej treści. Aby daną wiadomość zaklasyfikować do *spamu* musi ona spełniać jednocześnie trzy warunki: 1) treść wiadomości nie ma związku z tożsamością odbiorcy, 2) odbiorca nie wyraził zgody na jej otrzymanie, 3) na podstawie treści wiadomości można wnioskować, iż nadawca wskutek jej wysłania może odnieść niewspółmiernie większe korzyści niż odbiorca.

Interesujące jest pochodzenie nazwy *spam*. Jest to nazwa bardzo popularnej, produkowanej od lat trzydziestych XX w. przez amerykańską firmę „Hormel Foods" konserwowej mielonki wieprzowej. Przed wprowadzeniem tej nazwy produkt nosił nazwę *Hormel Spiced Ham*. Skrót najprawdopodobniej utworzono od ***Spiced Ham*** lub opisu pochodzenia zawartości konserwy ***Shoulder Pork and Ham***. Produkt zyskał na popularności zwłaszcza podczas II wojny światowej. Okoliczności zastosowania tej nazwy do niechcianej poczty elektronicznej nie są dokładnie znane, lecz jedną z najczęściej przytaczanych hipotez jest nawiązanie do znanego skeczu słynnej brytyjskiej grupy

[3] Lista haseł w bibliografii na końcu artykułu. Polecamy również odpowiedniki na anglojęzycznych stronach Wikipedii. Autor chciałby jednocześnie wyrazić podziękowania za konsultację merytoryczną Jakubowi Marszałkowskiemu, Jakubowi Jarudze i Bartoszowi Kuczyńskiemu.

komików „Monty Python's Flying Circus" z 1970 roku. W skeczu tym klient pytający w restauracji o menu dowiaduje się, że w każdym z dań z karty znajduje się mielonka (*Spam*) i nie jest możliwe zamówienie dania bez niej, mimo protestów żony (*„I don't like Spam!"*). Nazwa produktu powtarzana jest w skeczu dziesiątki razy.

Wyróżnia się dwie zasadnicze kategorie *spamu* przesyłanego w poczcie elektronicznej: 1) niezamawiane oferty handlowe lub usługowe o charakterze komercyjnym (ang. *Unsolicited Commercial Email* – UCE) lub reklamowym (w wielu krajach zakazany przez prawo, w tym również w Polsce i krajach UE na mocy dyrektywy UE); 2) niezamawiana poczta o charakterze niekomercyjnym (ang. *Unsolicited Bulk Email* – UBE) np. apele organizacji społecznych, charytatywnych, religijnych lub partii politycznych. Należałoby jednak wyodrębnić również trzecią, w dodatku najprawdopodobniej najliczniejszą grupę *spamu*, pozornie należącego do drugiej z powyższych grup. Jego treść jednak nie jest istotna, lecz w ostatecznym rozrachunku pożądana reakcja ze strony odbiorcy (najczęściej wejście na stronę, której adres podany jest w treści) może przynieść korzyści nadawcy i osiągnięcie zamierzonego celu. Należą do tej grupy głównie maile o różnorakiej, mniej lub bardziej, lecz jednak podejrzanej treści, takich jak oferty sprzedaży podróbek oryginalnych produktów (np. markowych zegarków), oprogramowania komputerowego, gier komputerowych, farmaceutyków (najczęściej medykamentów zwiększających potencję u mężczyzn), dyplomów renomowanych uczelni (najczęściej amerykańskich), zaproszenia na strony internetowych biur matrymonialnych (w przeważającej liczbie rosyjskich, lub ogólnie wschodnioeuropejskich – pochodzących z byłych krajów Z.S.R.R.), czy strony o zawartości erotycznej oraz informacje o zbliżających się wydarzeniach giełdowych mających rzekomo przynieść ogromne korzyści inwestującym w akcje. Wejście na stronę, której adres podano w takim spamie najczęściej kończy się pobraniem „na własne życzenie" złośliwego oprogramowania (ang. *malicious software*), które automatycznie instaluje się na komputerze ofiary przejmując nad nim częściową lub całkowitą kontrolę bez wiedzy użytkownika. Komputery w ten sposób pozyskane i połączone w sieć (ang. *botnet, zombie network*) służą nadawcy (spammerowi/hackerowi) do dalszego rozsyłania spamu (bez wiedzy właściciela – ofiary) z wykorzystaniem adresów z książek adresowych ich programów pocztowych. Zainstalowane w ten sposób złośliwe oprogramowanie może również skanować zawartość twardych dysków w poszukiwaniu danych kont bankowych, aby umożliwić cyber-przestępcy kradzież zasobów konta lub późniejsze wyłudzenie ich metodą *phishingu*, o której będzie mowa w dalszej części artykułu.

Innym sposobem gromadzenia bazy adresów poczty elektronicznej przez spammerów jest rozsyłanie różnego typu **„łańcuszków"** (ang. *chain e-mail*). Wyjątkowo podli wydają się być nadawcy łańcuszków bazujących na nieszczęściu ludzkim, które nazwalibyśmy **„łańcuszkami nieszczęścia"**

[A.S.] i mających na celu wzbudzenie litości odbiorcy. Należą do nich prośby o pomoc w zbieraniu funduszy na leczenie ciężko chorego dziecka (cierpiącego na poważną lecz nie nieuleczalną chorobę) lub przechodzącego rehabilitację (np. po odniesieniu poparzeń, poważnej operacji itp.), które rzekomo miałoby przynieść samo przesłanie dalej maila (pieniądze mają być przekazane potrzebującym rodzicom przez operatora danej poczty za każdy wysłany mail[4]). Treść maili z tej grupy zwykle skonstruowana jest w sposób imitujący list od zrozpaczonych i zdesperowanych rodziców chorego dziecka, często przepełniony wzruszającymi zwrotami i wskazujący na głęboką religijność rodziców. Prośba o przesyłanie maila bez zmian w treści umożliwia spammerowi zebranie wszystkich adresów, na które został przesłany dalej.

Do innego rodzaju spamu należą **„łańcuszki-wróżby"** (najczęściej z załączonymi barwnymi prezentacjami przepełnionymi złotymi myślami i sentencjami filozoficznymi lub/i różnego typu (w gruncie rzeczy pozytywnymi) radami (np. „jak być dobrym człowiekiem", „jak żyć w zgodzie z innymi ludźmi" itp.), które na końcu wiadomości obiecują spełnienie marzeń (finansowych, zawodowych, osobistych i innych) i osiągnięcie szczęścia pod warunkiem rozesłania wiadomości do jak największej grupy nowych adresatów (im większa ich liczba tym większa obiecana szansa, czy wręcz gwarancja, spełnienia marzeń). Podają nieraz przy tym przykłady rzekomych szczęśliwców, których marzenia spełniły się w różnym stopniu w zależności od liczby osób, do których przesłali łańcuszek. Podobne w swej konstrukcji, lecz działające na zasadzie przeciwnego mechanizmu oddziaływania psychologicznego na odbiorcę są tzw. **„łańcuszki-horrory"**, które zawierają groźby nieszczęść, jakie mogą przytrafić się adresatowi, jeśli nie prześle ich dalej (z podobną listą rzekomych przykładowych odbiorców i nieszczęść, jakie ich spotkały za zbagatelizowanie i zlekceważenie gróźb). W rozpoznaniu łańcuszka pomagają coraz liczniejsze serwisy internetowe, jak np. atrapa.net gromadzące i omawiające łańcuszki oraz instruujące o sposobach ich rozpoznawania.

Wiele wspólnego z łańcuszkami mają tzw. **legendy miejskie** (ang. *urban legends*) przybierające formy opowieści. Treść legendy miejskiej charakteryzuje się następującymi cechami (za: atrapa.net): 1) jej akcja rozgrywa się niedawno, 2) jej bohaterem jest opowiadający, jego krewny czy znajomy lub — częściej — „znajomy znajomego", 3) opowiadana jest jako prawdziwa, opisywane zdarzenia miały zdarzyć się naprawdę, 4) rozprzestrzenia się spontanicznie — słuchacze stają się opowiadającymi i rozprzestrzeniają opowieść dalej, 5) w trakcie przekazywania ulega modyfikacjom, w opowieści pojawiają

[4] Spam tego typu najczęściej kończy się formułką: „Ciebie kosztuje to tylko kliknięcie, a rodzice dostają 3 grosze za każdego maila przesłanego w tej formie. Mail zawiera skrypt html, który zlicza ile razy był wysłany a płaci firma zajmująca się badaniami skuteczności mailingu jako formy marketingowej.", co jest oczywiście niedorzecznością.

się nowe szczegóły, inne giną „po drodze", często modyfikacje mają na celu dostosowanie opowieści do lokalnych realiów, 6) źródła miejskiej legendy są na ogół nieznane, często niemożliwe do ustalenia, 7) zawiera emocjonalne elementy (często humoru lub makabry), ostrzega przed fatalnymi skutkami działań sprzecznych z zasadami obowiązującymi w danej społeczności, potwierdza lęki i obawy przez złem czyhającym wokół.

Innego typu cele ma spam zawierający informacje o rzekomych nowych niebezpiecznych wirusach (ang. *false positives*) i sposobach zapobiegania zainfekowania nimi systemu operacyjnego. Informacje o wirusie są oczywiście nieprawdziwe, a wykonanie przez ofiarę poleceń z instrukcji prowadzi do zgoła przeciwnych rezultatów – zwykle do usunięcia lub uszkodzenia ważnych plików systemowych i w efekcie unieruchomienia systemu operacyjnego. Jest to więc swego rodzaju złośliwy sabotaż dokonany na ofierze, która uwierzyła w ostrzeżenie.

Przedmiotem spamu (treścią wiadomości lub załącznika) mogą być również zasadniczo użyteczne informacje, jak np. instrukcje udzielania pierwszej pomocy (również samemu sobie) w przypadku zawału mięśnia sercowego, czy udaru mózgu (jak najbardziej prawdziwe i wręcz podręcznikowe). Bywają uwiarygodniane przez listy dołączane rzekomo przez uznane medyczne uczelnie wyższe – akademie i uniwersytety. Użyteczności tych informacji, zwłaszcza w obliczu wysokiej skali występowania wspomnianych chorób w społeczeństwie, z pewnością może skuteczniej zadziałać na odbiorcę niż inne metody (obietnice nagrody, groźby itp.) i sprawi, że wiadomość zostanie przesłana dalej w dobrej wierze. Nie umniejsza to jednak niebezpieczeństwa, jakie przesłanie takiego maila dalej może spowodować.

Amerykańska firma CISCO Systems, zajmująca się m.in. zabezpieczeniami sieciowymi, opublikowała w 2009 r. raport, w którym ujawniła ranking krajów z których wysłano najwięcej spamu w tym roku (w bilionach sztuk). NA pierwszym miejscu uplasowała się Brazylia (7,7), a dalej USA (6,6), Indie (3,6), Korea Płd. (3,1), Turcja (2,6), Wietnam (2,5), Chiny (2,4), Polska (2,4), Rosja (2,3), Argentyna (1,5). Wśród globalnych rezultatów spammingu należy wymienić: 1) zatykanie łączy internetowych i blokowanie miejsca na twardych dyskach komputerów indywidualnych odbiorców; 2) spowalnianie działania serwerów zmuszonych do przetwarzania spamu; 3) strata czasu użytkowników internetu zmuszanych do czytania i kasowania spamu, utrudnienia w odbiorze „normalnej" poczty (z powodu blokad antyspamowych lub przepełnionej skrzynki pocztowej) lub przeoczenia jej wśród dużej ilości spamu; 4) generowanie kosztów przeciwdziałania spamowi u operatorów internetowych, przerzucanie kosztów promocji na operatorów internetowych i odbiorców korespondencji – czyli jest to forma wyłudzenia; 5) naruszanie prywatności i bezpieczeństwa odbiorców, godzenie w przekonania moralne, religijne i inne (np. poprzez przesyłanie niepożądanych treści – obraźliwych, wulgarnych, pornograficznych, nieodpowiednich dla nieletnich itp.);

6) stwarzanie zagrożenia wirusami i innym złośliwym oprogramowaniem; 7) spadek zaufania publicznego do mediów elektronicznych w ogóle. Wśród sposobów ochrony przeciwno spamowi i jego odmianom można wskazać kilka najważniejszych zasad: 1) podstawową rzeczą w korzystaniu z jakichkolwiek form użytkowania internetu jest uprzednie zainstalowanie programu antywirusowego i zwalczającego programy szpiegowskie (ang. spyware); 2) na spam z pewnością nie należy odpowiadać, nawet jeśli tylko z zamiarem odpłacenia się tym samym – zaśmiecenia skrzynki pocztowej intruza (tzw. flames); 3) w przypadku spamu wysyłanego systematycznie z tego samego adresu najlepiej jest powiadomić administratora i założyć filtr antyspamowy (dołączyć nadawcę do niepożądanych nadawców); 4) nie należy pozytywnie reagować na spam – spełniać zawartych w nim próśb, czyli przede wszystkim nie odwiedzać podanych adresów internetowych, nie podawać swoich danych, nie przesyłać wiadomości dalej; 5) w programie pocztowym należy wyłączyć automatyczną obsługę JavaScript oraz HTML, a także automatyczne otwieranie załączników maili i opcję autopodglądu wiadomości (automatyczne otwieranie obrazków w mailu może działać, jak klikanie adresów w treści spamu – może spowodować odnotowanie w bazie spamera, iż dany mail jest aktywny, a wiadomości odczytywane; skutkiem będzie nadsyłanie jeszcze większej liczby spamu); 6) warto instalować uaktualnienia programu pocztowego lub/i używać niestandardowych programów pocztowych (najpopularniejsze bowiem, choć oferujące podobny poziom bezpieczeństwa, są bardziej narażone na ataki np. koni trojańskich skonstruowanych w taki sposób aby z nimi współpracowały); 7) należy unikać podawania swojego adresu poczty elektronicznej, jeśli nie jest to konieczne lub zamieszczając go w miejscach ogólnodostępnych (jak strony i fora intenetowe itp.) podawać go w zamaskowanej formie na przykład poprzez zastąpienie znaku „@" innym symbolem lub ciągiem znaków („$", „#", „at" itp. np. (np. „adres[at]domena.eu"), wstawienie w miejsce kropki wyrazu „kropka" (np. „adres@domena(kropka)eu") lub używanie innych „wstawek antyspamowych" w postaci dodatkowego tekstu (np. „_wytnij_to_" lub „_NIE_SPAMEROM_").

Fałszowanie adresów utrudnia działanie automatycznych programów pozyskujących adresy mailowe (ang. *harvester*) przeszukującym sieć w poszukiwaniu „małpek". „Wstawki" najlepiej jest dodawać na końcu adresu (np. „konto@domena.eu_wytnij_to"), ponieważ dodane przed nazwą domeny, choć chronią adresata przed spamem, nadal narażają operatora poczty na obciążenia łączy i procesorów serwera. Jeśli wymagane jest podanie adresu poczty bez modyfikacji warto przeznaczyć do tego celu osobne konto lub alias pocztowy. Szereg ze wspomnianych „wstawek" może jednak obecnie okazać się mało skutecznymi technikami ochrony przed wciąż udoskonalanymi *harvesterami*. W tej chwili najskuteczniejszą techniką ochrony przed *harvesterami* jest publikowanie adresu w postaci

obrazka zamiast tekstu. Administratorzy stron i serwisów internetowych mogą zaś ze swojej strony zadbać o bezpieczeństwo użytkowników i zamiast publikować listę adresów mogą wprowadzać mniej wygodne lecz bezpieczne formularze kontaktowe.

Metody stosowania spammingu doskonalone przez dekady egzystowania w internecie doczekały się szeregu swych coraz bardziej wyrafinowanych i skuteczniejszych w swym działaniu odmian, spośród których najistotniejsze (zwłaszcza znane pod nazwą scammingu) zostaną omówione w kolejnych częściach artykułu.

3. SCAMMING

Scamming (ang. *confidence trick, confidence game,* inne nazwy: *bunko, con, flim flam, gaffle, grift, hustle, scheme, swindle, bamboozle*) jest odmianą spammingu, występującą w większości tych samych mediów co spam, opartą na zaskarbieniu przez oszusta (ang. *a confidence man, con man, confidence trickster, con artist*) lub też jego wspólników (ang. *shills*) zaufania ofiary (ang. *the mark*) i wprowadzeniu odbiorcy wiadomości w błąd poprzez informację, iż jest lub może być beneficjentem określonego dobra (najczęściej finansowego) np. wygranej na loterii (zwykle wielomilionowej kwoty w dolarach amerykańskich, funtach brytyjskich lub euro) poprzez wytypowanie tego właśnie adresu pocztowego; odziedziczenia spadku lub mówiącą o innym depozycie i nakłanianiu do nieczystych transakcji.

W ostatnim przypadku (spadek, depozyt) znanym pod nazwą „nigeryjskiego przekrętu", „nigeryjskiego szwindlu" lub „przekrętu nr 419"[5]) list skonstruowany jest celowo w sposób wskazujący na przypadkowość wyboru adresata (nadawca tego nie ukrywa), zwykle z powodu zbieżności nazwiska z rzekomym spadkodawcą. W jednej z odmian „nigeryjskiego przekrętu" oszust podający się za prawnika, pełnomocnika zmarłego (najczęściej tragicznie np. w katastrofie samolotowej w Afryce), wdowę po wysoko postawionym oficjelu, itp. otwarcie nakłania do podziału (zwykle po połowie) najczęściej wielomilionowej kwoty pozostawionej w zamrożonym depozycie bankowym przez zmarłego, a następnie wyłudza od ofiary, która dała się oszukać, kolejne kwoty pieniędzy na rzekome pokrycie opłat manipulacyjnych, łapówek itp. w celu odzyskania całego depozytu bankowego denata. Pierwszy mail wygenerowany jest automatycznie, w przypadku odpowiedzi dalszą korespondencję prowadzi już człowiek – *scammer*. Sama treść maila bywa napisana poprawną angielszczyzną, z zachowaniem konwenansów

[5] Od numeru artykułu w kodeksie karnym Nigerii, dotyczącego tego przestępstwa. Nigeryjski Bank Centralny ostrzegał przed oszustwami tego typu już w 1998 r. Źródło: IS 10.

korespondencji formalnej. Bywa również przepełniona religijnymi zwrotami (być może w zależności od kraju, do którego jest wysyłany dostosowuje się je do wiodącej religii danego kraju).

Mechanizm oddziaływania psychologicznego tego typu *scamu* bazuje na naiwności ludzkiej, pokusie łatwego i szybkiego wzbogacenia się o fortunę, nawet jeśli niejasnego pochodzenia (lub wprost z nieczystych interesów), nieosiągalną dla przeciętnego człowieka. Ta myśl może skusić nawet uważających się dotąd za uczciwych i prawych odbiorców. Można powiedzieć, że jest to jeden z najbardziej misternie opracowanych *scamów* i dlatego najbardziej niebezpieczny. Ta metoda oszustwa znana była już w latach 1904-1911 (chodziło wtedy o pomoc w wykupieniu rzekomego rosyjskiego więźnia z hiszpańskiego więzienia). Według witryny snopes.com około 1997 r. za pomocą tego mechanizmu wyłudzono od obywateli USA ok. 100 milionów dolarów w ciągu piętnastu miesięcy. W skrajnych przypadkach w wyniku dokonanego oszustwa tą metodą dochodziło także do uprowadzeń a nawet śmierci ofiary (gdy naiwny adresat wybrał się w daleką podróż lub pałający żądzą zemsty za popełnione oszustwo szukał sprawiedliwości na własną rękę).

4. PRZYKŁADY SOCIAL ENGINEERING: PHISHING I PHARMING

Mechanizm inżynierii społecznej (ang. *social engineering*), którego jedną z podstawowych metod jest *phishing* (inna nazwa to *spoofing* – nabieranie) należy do najbardziej wyrafinowanych metod oszustw. Polega na podszywaniu się i odgrywaniu roli osoby lub instytucji godnej zaufania (np. informatyka, administratora sieci, banku itp.) w celu dokonania oszustwa i osiągnięcia korzyści materialnych. Metodom internetowej IS mogą towarzyszyć metody telefoniczne. Istnieje również forma SMSowa *phishingu*, która nosi nazwę *SMiShingu*.

Podstawowym założeniem inżynierii społecznej jest fakt, iż najsłabszym ogniwem systemów bezpieczeństwa jest najczęściej człowiek. Zamiast używać zaawansowanych technologii do włamania się do danego systemu nieraz łatwiej jest uzyskać dostęp do niego bezpośrednio od jego pracownika używając podstępu. Za twórcę tego typu ataków i „ojca *hackingu*" uważa się Kevina Mitnicka (IS 4). Jak sam stwierdził w jednej ze swych publikacji (2004: 4):*„it is much easier to trick someone into giving a password for a system than to spend the effort to crack into the system"*. Według Mitnicka (2003) atak metodą IS składa się z **4 cykli: 1) poszukiwanie informacji** – gromadzenie informacji dotyczących ataku, 2) **zdobywanie zaufania** – dotyczy osób, od których mają zostać pozyskane informacje, 3) **wykorzystywanie zaufania** – np. do nieautoryzowanego dostępu do systemu, 4) **zdobycie**

informacji – uzyskiwanie niejawnych informacji lub dostęp do zasobów, do których intruz nie ma prawa.

Celem *phishingu* jest osiągnięcie korzyści finansowych poprzez wyłudzenie od ofiary danych, poświadczeń, haseł z zamiarem przejęcia konta poczty elektronicznej i dalszego rozsyłania z niego spamu lub/i wyłudzenie dostępu do konta bankowego, karty kredytowej itp. w celu kradzieży zasobów finansowych. W takiej postaci *phishing* ma wymiar indywidualny – dotyka pojedynczą ofiarę. Na większą skalę mechanizm ten może posłużyć do włamania się do większych, korporacyjnych systemów informatycznych, inwigilację i kradzież niejawnych, tajnych i innych danych narażającą firmę/korporację na poważne wydatki związane z naprawieniem szkód wyrządzonych przez taką działalność sabotażową oraz poważne problemy związane z utratą zaufania, wiarygodności, spadkiem wartości notowań giełdowych/rynkowych i bankructwem włącznie. Na szczeblu instytucji administracji państwowej atak metoda *phishingu* może zagrażać bezpieczeństwu narodowemu i nosić znamiona szpiegostwa. Popularnym celem ataków przeprowadzonych metodą phishingu są banki i aukcje internetowe. Atak zazwyczaj polega na wysłaniu spamu do licznej grupy potencjalnych ofiar kierując je na stronę internetową, która do złudzenia przypomina stronę banku internetowego, a w rzeczywistości służy do przechwytywania danych wprowadzonych przez ofiarę. Innym typowym sposobem wyłudzania danych jest informacja o rzekomym zagrożeniu wygaśnięciem konta i konieczności jego reaktywowania (z podaniem poufnych danych różnego typu z hasłem do konta włącznie) lub przepełnieniu skrzynki pocztowej na serwerze operatora. W obu przypadkach phisher podaje aktywny link do strony, której adres na pierwszy rzut oka wygląda prawidłowo. Zawiera jednak drobne, łatwe do przeoczenia zmiany np. www.paypai.com zamiast www.paypal.com.

Jeśli chodzi o pochodzenie słowa phishing termin ten najczęściej rozszyfrowuje się jako ***password harvesting fishing*** (łowienie haseł) i został ponoć ukuty w połowie lat 90. XX w. przez *crackerów* próbujących wykraść konta w popularnym serwisie AOL (*America OnLine*). Inna teoria mówi, iż określenie to pochodzi od nazwiska Briana Phisha jako ponoć pierwszego złodzieja kard kredytowych z lat 80. XX w. stosującego techniki psychologiczne. Według jeszcze innej teorii B. Phish był fikcyjną postacią, za pomocą której *spammerzy* wzajemnie się rozpoznawali. Określenie *phishing* mogło być też zainspirowane przez inny termin – *phreaking* (*phone* + *freak*) – wcześniej znaną metodą łamania zabezpieczeń sieci telefonicznych, najczęściej celem uzyskania połączenia darmowego, lub tańszego niż tradycyjne.

Groźniejszą i trudniejszą do wykrycia formą *phishingu* jest *pharming*. Jest to metoda ataku w ramach mechanizmu IS polegająca na przekierowaniu nawet właściwie wpisanego przez użytkownika internetu adresu na fałszywą stronę imitującą najczęściej oficjalną stronę banku w celu przejęcia danych

(haseł itp.) i docelowo – kradzieży środków z konta, karty kredytowej itp. Nazwa jest wynikiem połączenia wyrazów *phishing* i *farming*.

Aby właściwy adres URL (*Uniform Resource Locator*) prowadził do fałszywej strony www, konieczne jest przeprowadzenie dodatkowego ataku. Najczęściej wykonywana jest jedna z dwóch wersji takiego ataku: 1) Atak polegający na zatruciu globalnego serwera DNS (*Domain Name System*), w celu skojarzenia prawdziwego adresu URL z serwerem zawierającym stronę WWW wykradającą poufne dane; 2) Atak z wykorzystaniem „trojanów", modyfikujących lokalne pliki w systemie użytkownika, odpowiedzialne za wstępne tłumaczenie nazw URL na fałszywy adres IP (*Internet Protocole*), z pominięciem globalnego serwera DNS. W zdecydowanej większości przypadków wystarczającą ochronę przed atakiem metodami pharmingu stanowią standardowe programy antywirusowe z uaktualnionymi bazami wirusów. Pojawia się również szereg programów wyspecjalizowanych w ochronie przeciwko *pharmingowi* (tzw. *Anti-pharming software*), jednak oprogramowania jak i sam termin budzą kontrowersje w środowisku informatycznym. Jego przeciwnicy uważają termin *pharming* za marketingowy neologizm służący wyłącznie do przekonania banków do konieczności kupowania nowych pakietów usług bezpieczeństwa (ang. *security services*). Podstawowym sposobem zabezpieczenia się przed atakami metodami phishingu i pharmingu jest przede wszystkim upewnienie się, czy wyświetlana strona wymagająca poufnych danych jest oryginalna, wiarygodna i bezpieczna. W tym celu należy sprawdzić jej certyfikat SSL (*Security Socets Layer*), który powinien być wystawiony na prawowitego właściciela strony. Można tego dokonać klikając symbol kłódki w przeglądarce, który powinien być widoczny przy odwiedzaniu tego typu stron (banków itp.). Poza tym sam adres stron widoczny w oknie przeglądarki powinien rozpoczynać się od https:// (ang. *Hypertext Transfer Protocol Secure*).

5. MALICIOUS SOFTWARE – ZŁOŚLIWE OPROGRAMOWANIE

Atakom w postaci wymienionych wyżej odmian *spammingu* może towarzyszyć (lub być jego konsekwencją) wykorzystanie złośliwego oprogramowania (ang. *malicious software, malware* – „złoprogramowanie" [prop. tłum. A.S.]) dołączonego do wiadomości w postaci załącznika lub zakodowanego w nim lub w samej wiadomości (sprzyja temu kod HTML). W wyniku tego samo odebranie i otworzenie wiadomości i/lub załącznika, bez potrzeby dalszego jej przesłania może już spełniać zamierzenie spammera (potwierdzenie aktywności konta pocztowego, przejęcie konta lub opanowanie komputera ofiary). Z powodu ograniczonych ram niniejszej publikacji nie

jesteśmy w stanie nawet pokrótce scharakteryzować tutaj licznych typów złośliwego oprogramowania i podać przykłady oprogramowania chroniącego przed nimi, a jedynie możemy odesłać na stronę pod adresem oznaczonym w bibliografii jako IS 16.

6. HACKING/CRACKING

Spammerzy i posługujący się innymi, wymienionymi w poprzednich punktach formami nękania drogą poczty elektronicznej lub poprzez inne formy komunikacji poprzez internet często zaliczają się do jednej z poniższych grup *hackerów* (w większości przypadków pierwszej). Najogólniej rozróżnia się następujące rodzaje *hackingu*, stosując nazewnictwo przez analogię do znanych z klasycznych westernów stereotypów rozpoznawania pozytywnego bohatera lub czarnego charakteru po kolorze kapelusza (choć w środowisku informatycznym nie ma zgody co do takiego podziału): 1) *black hat* (działający na granicy lub poza granicami prawa), 2) *white hat* (działający w pełni legalnie), 3) *grey hat* – crackerzy (korzystający po części z metod działania obu powyższych grup). Do ostatnich najgłośniejszych przykładów działalności hackerskiej na szeroką skalę należą zmasowane ataki organizacji „Anonymous" – jednej z największych na świecie anarchistycznych organizacji hackerskich – w ramach operacji „Payback", przeprowadzone w dniach 9-10.12.2010, skierowane m.in. przeciwko serwisom internetowym Visa i Master Card. Miała to być zemsta hackerów za utrudnianie działalności strony Wikileaks (IS 15),

7. ŚRODKI BEZPIECZEŃSTWA

Poza wspomnianymi we wcześniejszych punktach sposobami ochrony przed atakami metodami spammingu i jego pochodnych w celu zapobieżenia zagrożeniom w sieci wśród najważniejszych środków bezpieczeństwa należy wymienić następujące czynności: 1) instalacja programu antywirusowego i *antimalware*, 2) stała aktualizacja ich baz danych, 3) regularne skanowanie antywirusowe i *antimalware* wszystkich dysków twardych, 4) stosowanie zapór sieciowych typu *firewall;* 5) „higiena" korzystania z internetu i poczty e-mail (szerzej omówiona w punkcie 1 niniejszego artykułu), 6) upewnianie się o szyfrowaniu transferu danych przy płatnościach bankowych on-line (HTTPS). Do powyższych, zgodnie z przesłaniem niniejszego artykułu dodalibyśmy: edukację obywateli w zakresie uświadamiania zagrożeń i sposobów ich unikania od najniższych poziomów szkolnictwa (m.in. np. w toku studiów nauczycielskich). W razie podejrzenia ataku spammera/hackera należy niezwłocznie poinformować administratora serwisu, poczty lub bank,

administratora aukcji internetowej itp. (w przypadku podejrzenia ataku phishera/pharmer) a i niezwłocznie zmienić hasła dostępu do swoich kont.

Co się tyczy samego stosowania haseł w coraz liczniejszych i różnorodnych miejscach w internecie (skrzynce pocztowej, portalach społecznościowych, komunikatorach, serwisach, forach internetowych, księgarniach i bibliotekach online, platformach e-learningowych, portalach, wortalach, bankach, aukcjach internetowych itd.) warto również stosować się do kilku podstawowych zasad przy ich tworzeniu i przechowywaniu. Serwis PCWorld.pl (wydawany równolegle z informatycznym czasopismem branżowym) podaje **pięć najczęstszych błędów przy tworzeniu haseł[6] oraz podaje sposoby ich unikania: Błąd 1** – hasło jest zbyt krótkie, więc można je szybko złamać, **Błąd 2** – hasło jest zbyt proste, więc można je odgadnąć, **Błąd 3** – hasło jest gdzieś zanotowane lub zapisane cyfrowo, **Błąd 4** – używanie latami tego samego hasła, **Błąd 5** – używanie jednego hasła do wszystkiego. Firma ESET (producent programu antywirusowego), z kolei, przedstawiła **dziewięć zasad tworzenia bezpiecznego i łatwego do spamiętania hasła** (Sobiech, A.; Makosz, A. 2011: 66): **1)** Łącz i przeplataj znaki dwóch słów, stosując przy tym duże i małe litery, np. czerwony garnek = CeZwRnOy-GraEnK; **2)** Przeplataj litery dowolnego wyrazu z cyframi, np. flash 9708 = f9L7a0s8H; **3)** Łącz ze sobą dwa słowa, używając jako łącznika dowolnego symbolu, np. CzeRwo-NyarNek; **4)** Wpleć w hasło znaki specjalne (!@#$%); **5)** Twórz hasło z błędną pisownią (bądź przy tym konsekwentny), np. mózg = MuSk; **6)** Stosuj duże litery w niekonwencjonalnych miejscach, np. waRszAwa; **7)** Twórz hasło jako zlepek pierwszych liter wyrazów tworzących dłuższa frazę, np. MtRdM (mamy tego roku deszczowy maj); **8)** Zastępuj litery cyframi – E=3, A=4, T=7 itd., np. K4$74 (kasta); **9)** Nie wykorzystuj tego samego hasła do zabezpieczenia kilku serwisów lub komputerów.

8. WNIOSKI

O ile w pracy nauczyciela języka obcego w przypadku ataku hackera poza potencjalnymi stratami własnymi raczej nie ma ryzyka narażenia placówki oświatowej, w której jest zatrudniony na ataki hackerów przeprowadzone metodami inżynierii społecznej (szkolnictwo nie stanowi dla nich wystarczająco atrakcyjnego celu, może jedynie cel „treningowy" dla wspomnianych *script kiddies*), o tyle wykształceni filologowie (w tym niedoszli nauczyciele), którzy znajdują zatrudnienie w dużych firmach, korporacjach (np. bankach, jako tłumacze i inni urzędnicy biurowi) nieuświadomieni w zakresie zagrożeń IS mogą niechcąco przysporzyć swoim pracodawcom kłopotów.

[6] Źródło: IS 1. Pod podanym źródłowym adresem znaleźć można obszerniejsze opisy podanych błędów wraz z przykładami oraz zaleceniami dot. środków bezpieczeństwa.

Najsłabszym punktem systemu bezpieczeństwa, najbardziej podatnym na ataki metodami inżynierii społecznej, okazuje się być najczęściej człowiek dlatego elementarna edukacja w zakresie bezpieczeństwa wykorzystania internetu na poziomie jednostki – pojedynczego użytkownika sieci – może okazać się drogą do zapewnienia bezpieczeństwa globalnego. Edukacja na wszelkich jej szczeblach (w tym na studiach filologicznych o specjalizacji nauczycielskiej) daje takie możliwości. Wystarczy je tylko dostrzec, nie bagatelizować problemu zagrożeń związanych z wykorzystaniem internetu i zapewnić kadrę wykwalifikowanych instruktorów, wykładowców, którzy w rzetelny i profesjonalny sposób przekażą niezbędną wiedzę w tym zakresie i poinstruują jak nie paść ofiarą cyberprzestepców.

BIBLIOGRAFIA

- Drews, M., (2008). „Gry komputerowe a analfabetyzm funkcjonalny i informacyjny". W: Surdyk A., Szeja J. Z. (red.), (2008). *Kulturotwórcza funkcja gier. Gra w kontekście edukacyjnym, społecznym i medialnym,* „Homo Communicativus" 2(4)/2008.
- Kasprzycki, D., (2005). *Spam, czyli niezamawiana komercyjna poczta elektroniczna: zagadnienia cywilnoprawne,* Kraków: Uniwersytet Jagielloński.
- Miller, S., (2003). *E-mailowy savoir-vivre,* (tłum. J. Kasprzak-Śliwińska). Poznań: Dom Wydawniczy Rebis.
- Mitnick, K., Kasperavičius, A. (2004). *CSEPS course workbook.* Mitnick Security Publishing.
- Mitnick, K., Simon, W. L. (2003). *The art of deception: Controlling the human element of security.* Indianapolis: Wiley Books.
- Mitnick, K., Simon, W. L. (2005). *The art of intrusion: the real stories behind the-eExploits ofhHackers, intruders & deceivers.* Indianapolis: Wiley Books.
- Sobiech, Ł., Makosz, A., (2011). *Co legalne, co nielegalne w internecie.* Warszawa: INFOR Biznes Sp. z o.o.
- Zdziarski, J., (2006). *Spamowi stop!: bayesowskie filtrowanie zawartości i sztuka statystycznej klasyfikacji języka,* (tłum. Leksem). Warszawa: Wydawnictwo Naukowe PWN.

Źródła internetowe

- IS 1: Daszkiewicz, K., Arnold, A., Schischka, B., (2010). Pięć najczęstszych błędów przy tworzeniu haseł, http://www.pcworld.pl/news/356910_1/Piec.najczestszych.bledow.przy.tworzeniu.hasel.html
- IS 2: Haker, bezpieczeństwo komputerowe, Wikipedia, (2011). http://pl.wikipedia.org/wiki/Haker_(bezpiecze%C5%84stwo_komputerowe)
- IS 3 : Inżynieria społeczna (informatyka), Wikipedia, (2011). http://pl.wikipedia.org/wiki/In%C5%BCynieria_spo%C5%82eczna_(informatyka)
- IS 4: Kevin Mitnick, Wikipedia, (2011). http://pl.wikipedia.org/wiki/Kevin_Mitnick

- IS 5: Krakowiak, L., (2010). Czy można rozpoznać sztuczki inżynierii społecznej, http://www.idg.pl/news/360704/Czy.mozna.rozpoznac.sztuczki.inzynierii.spolecznej.html
- IS 6: Łańcuszek internetowy, Wikipedia, (2011). http://pl.wikipedia.org/wiki/%C5%81a%C5%84cuszek_internetowy
- IS 7: Nigeryjski szwindel, Wikipedia, (2011). http://pl.wikipedia.org/wiki/Nigeryjski_szwindel
- IS 8: Pharming, Wikipedia, (2011). http://pl.wikipedia.org/wiki/Pharming
- IS 9: Phishing, Wikipedia, (2011). http://pl.wikipedia.org/wiki/Phishing
- IS 10: Pręgowski, M. P., (2007). „Nigeryjski przekręt" z Putinem w tle, http://technoblog.gazeta.pl/blog/1,84947,4648026.html
- IS 11: Rusiecki, P., (2007). „Internetowy aspekt inżynierii społecznej czyli nieautoryzowany dostęp do zasobów informatycznych przedsiębiorstwa", w: *Teoretyczne podstawy tworzenia SWO i strategie budowy e-biznesu,* (231-238), http://swo.ae.katowice.pl/_pdf/133.pdf
- IS 12: Scam, Wikipedia, (2011). http://pl.wikipedia.org/wiki/Scam
- IS 13: Spam, Wikipedia, (2011). http://pl.wikipedia.org/wiki/Spam
- IS 14: Sysło, M. M., (2011). „Technologia informacyjna w edukacji", http://www.snti.pl/snti/files/ti_w_edukacji.pdf
- IS 15: „Wypowiedzieli wojnę < <zdrajcom Wikileaks> >", (2010). http://www.tvn24.pl/12691,1685462,0,1,atak-hakerow-nazdrajcow-wikileaks,wiadomosc.html
- IS 16: Złośliwe oprogramowanie, Wikipedia, (2011). http://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie

Dostęp do wszystkich źródeł internetowych: 15 marca 2011.

ABSTRACT

The basics of security engineering in FL teacher education

This paper is meant to acquaint the reader with the common dangers stemming from daily use of the internet, especially one of its services – email – which remains the most popular form of communication online in the professional life of teachers of foreign languages, and with the means of preventing these dangers through education in departments training future teachers, using the example of applied linguistics studies. The article covers, on the basis of real examples, the issues of *spamming, scamming, phishing, pharming, hacking* (on the level of personal security), up to the phenomenon most dangerous to big companies and threatening global security – the phenomenon of *social engineering*. Moreover, issues related to *malware – malicious software* and related dangers are covered as well. In the chapter's conclusion the importance of civic awareness of the individual will be emphasised related to the existence of the discussed threats and the knowledge of preventing them through reliable and professional education during, among other things, classes in IT.

ABSTRACT

Die Grundlagen der Ingenieurkunst der Sicherkeit in der Berufsschulung der Fremdsprachenlehrer

Der Artikel hat zum Zweck, die allgemeinen Gefahren näherzubringen, die die Folge der täglichen Benutzung des Internets und der elektronischen Post sind als der weiterhin populärsten Kommunikationsform im Netz, in der didaktischen Praxis der Fremdsprachenlehrer. Er hat auch die Aufgabe, die Methoden zu zeigen, wie man diesen Gefahren durch entsprechende Edukation im Laufe des Lehrerstudiums, am Beispiel des Studiums an der Richtung Philologie-Angewandte Linguistik, vorbeugen könnte. In dem Artikel werden an konkreten Beispielen kurz die Fragen des spammings, scammings, phishings, pharmings und hackings besprochen (Im Rahmen der persönlichen Sicherheit) bis zu der für die Sicherheit der großen Korporationen und für die globale Sicherheit gefährlichsten Erscheinung genannt social engineering. Außerdem werden auch die Fragen einer boshaften Programmierung (engl. *malware – malicious software*) und die mit ihnen verbundenen Gefahren nähergebracht In den Schlußfolgerunden wird die Wichtigkeit des zivilen Bewußtseins des Menschen unterstrichen, und zwar zum Thema des Vorkommens der früher genannten Gefahren und der Kenntnis der Methoden, ihnen durch ehrliche und professionelle Edukation vorzubeugen – unter anderen während des Unterrichts im Bereich der Informationstechnologien.