Maciej Górnicki

Bezpieczeństwo w internecie: korzystanie z poczty elektronicznej

Gliwice, 6.09.2010

1. Konto pocztowe (email) z perspektywy duszpasterza.

W 2010 roku nie trzeba już chyba przekonywać, że posiadanie konta emailowego jest czymś niemal tak oczywistym jak posiadanie telefonu czy zegarka. Oczywiście jest pewna liczba osób, które potrafią się w XXI w. obyć bez telefonu, zegarka czy emaila, jednak moim zdaniem, w normalnej pracy współczesnego duszpasterza obywanie się bez telefonu, zegarka czy emaila jest raczej utrudnianiem sobie i innym życia niż cnotą. Co daje korzystanie z poczty elektronicznej?

- Ułatwia kontakt z osobami, które są przedmiotem duszpasterstwa:
  - grupy parafialne, zwłaszcza młodzieżowe
  - katechizowana młodzież (np. rozsyłanie dodatkowych materiałów do katechezy)
  - osoby z „trudnymi" pytaniami, które nie odważyłyby się przyjść do księdza
  - osoby, którym trudno się skontaktować bezpośrednio (niepełnosprawni, parafianie za granicą itp.)
- Znacznie usprawnia kontakt z diecezją i innymi instytucjami kościelnymi (przykład – okólniki, pisma do proboszczów, listy do odczytania itp.)
- Jest wymagane w przypadku kontaktu z niektórymi urzędami (np. ZUS)
- Umożliwia zakupy w internecie
- Pozwala na uczestnictwo w rozmaitych formach interaktywnych w internecie (fora dyskusyjne, głosowania, petycje itp.)
- Ułatwia utrzymanie relacji osobistych (rodzina, znajomi itp.)

2. Bezpieczeństwo? Mało ważne!

W wielu sytuacjach bezpieczeństwo korzystania z poczty internetowej wydaje się sprawą drugorzędną. Bardziej niż bezpieczeństwo cenimy sobie wygodę. Po co korzystać z bezpiecznych serwerów, po co zabezpieczać swoje konto trudnym hasłem, po co zmieniać hasło co jakiś czas – to tylko niepotrzebne komplikowanie sobie życia. Kto ma na to czas?

Lekceważenie bezpieczeństwa, choć jest to postawa bardzo rozpowszechniona, często okazuje się niezwykle brzemienne w skutkach. Podam tylko kilka przykładów, choć można by ich podać bardzo wiele - jest to bowiem powszechny problem:

– Pewien misjonarz posiadał konto na darmowym serwerze, zabezpieczone prostym do złamania hasłem. W pewnym momencie jego znajomi zaczęli otrzymywać od niego maile, mówiące, że znajduje się on w trudnej sytuacji, potrzebuje pomocy i prosi o wpłacenie pewnej kwoty na jego konto bankowe. Jednemu z tych znajomych wydało się to trochę podejrzane, dlatego zanim wpłacił pieniądze, zadał sobie trud, żeby zadzwonić za granicę i zapytać misjonarza, czy to prawda. Co się okazało? Otóż ktoś włamał się na konto internetowe misjonarza, wysłał do jego znajomych list z błaganiem o pomoc, a następnie zmienił hasło, tak że sam misjonarz nie mógł już wejść na własne konto. W tym przypadku konsekwencją było nadużycie zaufania znajomych i strata finansowa – niestety nie wiadomo nawet, do ilu osób hacker rozesłał list z prośbą o pieniądze i ile osób wpłaciło coś na jego konto, a wielu znajomych prawdopodobnie do dziś nie wie, że pisząc na stary adres email wysyłają listy nie do misjonarza, ale do hackera…

– Do środowisk wrogich Kościołowi (w tym do antykościelnych mediów – takich jak *NIE* czy *Fakty i Mity*) często docierają rozmaite informacje na temat Kościoła, które teoretycznie nie miały prawa „przeciec". Czasem są to sprawy tzw. obyczajowe, czasem finansowe, czasem wewnętrzne informacje kościelne. Nieraz duchowni, czytając o sobie w

antykościelnych mediach albo otrzymując wezwanie do prokuratury zachodzą w głowę, skąd media czy urzędnicy uzyskali informacje. Tymczasem powodem było lekceważenie zasad bezpieczeństwa w internecie. Mylnie zakładamy, że korespondencja poprzez email może być odczytana tylko przez nadawcę i odbiorcę. Wręcz przeciwnie – protokół przesyłania emaili można porównać do wysyłania kartki pocztowej: email jest przekazywany wieloma skokami, z serwera na serwer, a każdy po drodze może odczytać dane zawarte w emailu.

– W sierpniu 2010 cyberprzestępcy wyprowadzili z katolickiej diecezji w USA (Des Moines, Iowa) 600 tys. dolarów. Skorzystali z lekceważenia przez diecezję procedur bezpieczeństwa internetowego, dzięki czemu uzyskali dane dostępowe do kont bankowych, z których wyjęli ok. 600 tys. USD. Jak to zwykle bywa w przypadkach takich przestępstw, posłużyli się tzw. „słupami", czyli podstawionymi osobami, tak więc nie wiadomo, do kogo ostatecznie pieniądze trafiły i zdecydowanej większości nie udało się odzyskać.

Oczywiście problemy dotyczą nie tylko środowiska kościelnego

– Student został oskarżony o plagiat w swojej pracy naukowej. Powód? Rozdział jego pracy, zanim został oddany promotorowi, był wielokrotnie wysyłany do konsultacji drogą mailową. Ktoś (administrator serwera? hacker?) wyciągnął te dane z maila, dał znajomemu, który wykorzystał je w swojej pracy naukowej.

– Nagle dowiadujemy się, że ktoś podszywając się pod nas założył sobie konto w banku, wziął kredyt, szantażował kogoś, wyłudzał pieniądze, rozpowszechniał fałszywe informacje. Zazwyczaj informacja przychodzi do nas od policji, banku czy prokuratury. Dopiero w tym momencie zaczynamy się zastanawiać, jak to możliwe, żeby bezkarnie podszywać się pod inną osobę. Niestety, jest to możliwe, a nawet niezbyt skomplikowane. Wyjaśnienie, jak to możliwe wymagałoby osobnego artykułu (poza tym środki działania przestępców szybko się zmieniają), niech więc wystarczy uświadomienie sobie, iż mniej więcej w 50% przypadków rozpoczyna się od zlekceważenia zasad bezpieczeństwa w internecie. Kradzież tożsamości to nie zjawisko marginalne. Nie znam danych dotyczących Polski, ale w USA około 10 milionów osób rocznie pada ofiarą tego procederu (co stanowi ok. 5% populacji!).

3. Typowe błędy dotyczące korzystania z poczty internetowej:

A. Wybór niewłaściwego serwera.

Tzw. darmowe serwery, czy to polskie, czy zagraniczne, oferują wszystko za nic. Transfer bez limitu! Import i eksport książki adresowej! Miejsce na 7 gigabajtów danych! Czy ktokolwiek zadaje sobie pytanie, dlaczego ktoś w ogóle daje coś za darmo? Czy miejsce na serwerze nie kosztuje? Czy łącza internetowe nie kosztują? Czy obsługa informatyczna nic nie kosztuje? Ależ nie, wszystko to wiąże się z kosztami i wcale nie są one takie małe. W zależności od typu serwera i świadczonych usług, rzeczywisty koszt rocznego utrzymania jednego konta email wynosi od kilku do ponad 100 zł. Dlaczego więc ktoś oferuje to za darmo? Przede wszystkim z przyczyn marketingowych: po pierwsze użytkownik „darmowego" konta staje się niewyczerpanym medium reklamowym – jest on jak żywa reklama chodząca po mieście – do jego maili doczepiane są informacje reklamowe, sam też otrzymuje reklamy, za wszystko płacą więc reklamodawcy. Po drugie – użytkownik posiadający w swoim adresie nazwę typu „onet.pl" czy „wp.pl" czy „o2.pl" automatycznie promuje samego usługodawcę. We współczesnym marketingu tworzenie tzw. „świadomości marki" jest jednym z kluczowych elementów. W tym przypadku marką jest właśnie nazwa „onet.pl" czy „wp.pl".

Czy bycie „nosicielem" reklam i promotorem marki to dla użytkownika jedyny koszt „darmowego" konta? Niestety nie. Przede wszystkim, powierza on swoje dane firmie, która nie ma wobec niego żadnych zobowiązań, nic nie gwarantuje i może w zasadzie zrobić z jego danymi, co tylko chce. W tym także, na przykład, sprzedać antykościelnym mediom. Miejmy świadomość tego, że administrator serwera ma pełny dostęp do tego, co trzymamy na

serwerze. To znaczy, że np. jeśli trzymamy pocztę na serwerze Onetu czy WP, administrator Onetu czy WP może zrobić z naszymi danymi osobowymi oraz z naszymi mailami praktycznie wszystko, nie mając jednocześnie wobec nas żadnych zobowiązań. Często wręcz w regulaminie darmowych usług zawarta jest klauzula, że użytkownik zgadza się na udostępnianie jego danych osobom trzecim w celach marketingowych oraz informacja, że serwer nie zapewnia tajemnicy przechowywanych lub przesyłanych danych.. Kto jednak zadaje sobie trud, żeby czytać regulaminy?

Nie chcę powiedzieć, że korzystanie z darmowych serwerów email jest w każdej sytuacji niewskazane. Jednak duszpasterz, chcąc nie chcąc, jest osobą publiczną, która musi brać pod uwagę zarówno swój własny wizerunek, wizerunek instytucji, którą reprezentuje, jak i zaufanie, którym obdarzają go wierni. Dlatego do celów związanych z pracą duszpasterską powinien korzystać z emaila oferowanego na serwerach kościelnych (np. w Kurii Diecezjalnej czy na Opoce), a jeśli decyduje się wykupić konto emailowe w jakiejś świeckiej firmie, powinien dobrze sprawdzić jej wiarygodność i uważnie przeczytać regulamin świadczenia usług.

B. Trzymanie wszystkich danych na serwerze (zamiast na własnym komputerze).

Dlaczego firmy oferujące darmowe konta email prześcigają się w tym, ile miejsca ma użytkownik na serwerze? Czy komuś normalnemu przyszłoby do głowy, żeby trzymać w skrzynce pocztowej wszystkie otrzymane przesyłki zamiast codziennie wyciągać z niej pocztę? Dlaczego normalna skrzynka pocztowa miałaby mieć rozmiar domu? Wystarczy, że zmieści się w niej kilka czy kilkanaście przesyłek. Tymczasem w przypadku poczty internetowej postępujemy odwrotnie – wydaje nam się, że im więcej możemy trzymać na serwerze, tym lepiej. Nieświadomie dajemy się złapać w pułapkę. To właścicielom serwerów zależy na tym, żebyśmy jak najwięcej danych trzymali u nich na serwerze, zamiast u siebie na komputerze. Dzięki temu, oni również mają dostęp do tych danych i mogą z nimi robić, co tylko chcą. Poza tym, jeśli rzeczywiście trzymamy na serwerze kilka gigabajtów danych, to łatwo nie zrezygnujemy z konta na tymże serwerze – w przypadku rezygnacji utracilibyśmy zbyt dużo cennych danych.

Większość internautów nie zdaje sobie sprawy z tego, jak wiele informacji o sobie samych zostawiają w internecie. Korzystają, na przykład, z wyszukiwarki Google, z konta Gmail, z Facebooka czy „Naszej klasy” – a każde ich wyszukiwanie, wysłanie maila, wpis na serwisie społecznościowym, każda odwiedzona strona jest gdzieś odnotowana, przetworzona przez potężne komputerowe systemy obrabiające dane osobowe i dodana do ich „profilu”. Niektóre elementy tego profilu zapisane są na naszym własnym komputerze (tzw. „ciasteczka”, czyli cookie, które pozostawiają po sobie odwiedzone strony internetowe), inne elementy lądują w odległych bazach danych. Głównym celem takich zabiegów jest utworzenie naszego profilu jako potencjalnego konsumenta, nikt jednak nie potrafi odpowiedzieć na pytanie, czy jest to jedyny cel. Z całą pewnością treść naszych emaili jest analizowana przez potężne komputerowe systemy rządu USA i CIA pod kątem zagrożenia bezpieczeństwa publicznego (m.in. system Echelon). Wydajność tych systemów jest jednak zbyt mała, aby przetworzyć wszystkie dane przepływające przez internet. Trzymając swoje dane na odległych serwerach zamiast na własnym komputerze bardzo ułatwiamy pracę takim systemom szpiegowskim.

W jaki sposób utrudnić innym dostęp do naszych danych? Przede wszystkim, pobierając dane na własny komputer i usuwając je z serwera. W ten sposób utrudniamy życie nie tylko szpiegom i marketingowcom, ale także potencjalnym hackerom. Nawet gdyby włamali się na nasze konto, zastaną je puste.

Normalnym narzędziem do odbioru i wysyłania poczty powinien być program taki jak

Outlook (lub Outlook Express), Windows Live Mail, Thunderbird, The Bat – czyli klient pobierający dane na nasz komputer, a nie przeglądarka internetowa (Internet Explorer czy Firefox), która tylko wyświetla nam dane, chwilowo przetrzymując w tzw. pamięci cache, nie pobierając ich na stałe na nasz komputer. Oczywiście w opcjach takiego programu należy zaznaczyć, żeby usuwał z serwera pobrane wiadomości.

C. Zbyt łatwe hasło lub słabo zabezpieczony serwer

Większość ludzi rozumie, że własny dom należy zabezpieczyć porządnym zamkiem, a klucz do tego zamka nie powinien być łatwy do podrobienia. Poza tym, raczej nie używamy tego samego klucza do wszystkich zamków, ale do każdego mamy inny klucz. Tymczasem w stosunku do naszego elektronicznego klucza, czyli hasła zabezpieczającego nasz komputer, konto mailowe i cenne dane, postępujemy zupełnie odwrotnie. Znów wygoda bierze górę nad bezpieczeństwem. Hasło, które jest słowem ze słownika (np. „mama", „Grudziądz", „Artur") jest jak klucz bez ząbków. Złamanie takiego pseudozabezpieczenia to dla hakera kwestia kilku minut. Niewiele bezpieczniejsze jest hasło niesłownikowe, ale zbyt krótkie. Np. hasło zawierające 8 znaków - same małe litery, daje się złamać w przeciągu jednego-dwóch dni. To samo hasło zawierające kombinację dużych, małych liter, cyfr i innych znaków (np. Artks!Ma4) staje się bardzo trudne do złamania – hacker musiałby być bardzo zdeterminowany, bo zajęłoby mu to kilka lat.

W jaki sposób utworzyć bezpieczne hasło? Albo skorzystać z generatora haseł przypadkowych – wtedy niestety będzie ono trudne do zapamiętania, albo skorzystać z jakiejś metody mnemotechnicznej. Na przykład, pierwsze litery słów mojego ulubionego wiersza: „męczy się człowiek Miron męczy znów jest zeń słów niepotraf" dają hasło: „mscMmzjzsn", które jest wystarczająco bezpieczne do większości celów. Jeśli dołożymy do tego jeszcze jakąś cyfrę albo wykrzyknik, to hasło jest praktycznie nie do złamania.

Najlepszy zamek jest tylko tak dobry, jak drzwi, w których tkwi. Jeśli wstawimy pancerny zamek do drzwi zrobionych z tektury, nie utrudnimy życia złodziejowi. Niestety wiele serwerów, w tym większość serwerów darmowych jest słabo zabezpieczone i może się zdarzyć, że pomimo najlepszego hasła, ktoś włamie się nam na konto – nie dość, że pozna treść naszej korespondencji, to jeszcze zmieni hasło i uniemożliwi nam dostęp do własnej poczty!

D. Stosowanie tego samego hasła do wielu rzeczy

Biorąc pod uwagę, że nawet najlepsze hasło może wyciec – z naszej winy, bo np. zapisaliśmy je gdzieś na kartce, którą zgubiliśmy albo z powodu włamania na jakiś serwer, trzeba przyjąć zasadę, że nie stosujemy tego samego hasła do różnych celów. Oczywiście utrudnia to życie, ale czy nasze pieniądze na koncie bankowym czy też dane na koncie internetowym nie są warte odrobiny wysiłku umysłowego? Niestety stosowanie tego samego hasła do różnych celów jest powszechnym problemem – zdarzyło się już wiele razy, że hakerzy wykradli hasła z jakiegoś serwisu (najczęściej z serwisu społecznościowego lub darmowych emaili), a potem użyli je do zalogowania się na inne serwisy internetowe, w tym oczywiście – także do banków. Jako minimum powinniśmy przyjąć, że hasła do najważniejszych celów: do własnej poczty email, do banku i w ogóle związane z kwestiami finansowymi, są stosowane wyłącznie do tego celu, są bezpieczne i każde jest inne.

E. Korzystanie z obcych komputerów i użyczanie swojego komputera innym

Jeszcze jeden problem, o którym jedynie wspomnę – to sytuacja, w której korzystamy z obcego komputera (np. w szkole) albo gdy użyczamy swój komputer innej osobie (np. ktoś pyta: „mogę szybciutko sprawdzić sobie emaila?"). Mówiąc wprost – powinniśmy zachowywać w takich sytuacjach maksymalną nieufność. Nigdy nie mamy pewności, jak skonfigurowany jest i zabezpieczony cudzy komputer – może na nim być np. złośliwe

oprogramowanie, które zapamięta nasze dane, nasze hasła i przekaże je w niepowołane ręce. Sama przeglądarka internetowa zazwyczaj zapamiętuje wpisane hasła, więc kolejna osoba, logująca się po nas, będzie mogła bez problemu przejrzeć nasze emaile lub stan konta bankowego.

Podobnie, druga osoba korzystająca z naszego własnego komputera również może w bardzo łatwy sposób wykraść nasze dane, a także zainfekować, choćby niechcący, nasz komputer wirusem czy programem szpiegującym. Udostępniajmy swój komputer tylko takim osobom, którym powierzylibyśmy własny portfel i dowód osobisty!

F. Wirusy komputerowe i hackerstwo

Kolejne zagadnienie, które tylko zasygnalizuję, to wirusy komputerowe oraz inne złośliwe oprogramowanie oraz włamania na nasz własny komputer. Obecnie wirusy przenoszą się przez email, przez strony internetowe, a także przez przenośne pamięci USB, niefrasobliwie wkładane do własnego komputera. Niektóre wirusy działają tak, aby zaszkodzić naszemu komputerowi i zniszczyć nasze dane. Coraz więcej jednak działa tak, że nie niszczy danych, tylko je wykrada, przesyłając do rozmaitych przestępców. Najlepszy serwer pocztowy i najlepsze hasło do konta email niewiele pomogą, jeśli wirus pobierze z naszego komputera to hasło i prześle je hakerowi. Skala problemu jest taka, że obecnie jeśli nie zabezpieczymy komputera odpowiednim programem antywirusowym i tzw. firewallem, prawdopodobnie już pierwszego dnia po podłączeniu do internetu nasz komputer padnie ofiarą wirusa lub hakera.

G. Szyfrowanie danych

Zarówno poczta internetowa, jak i strony internetowe zazwyczaj docierają do nas w postaci niezaszyfrowanej. Oznacza to, że każdy właściciel serwera czy łącza, przez które te dane przechodzą, może je odczytać. Istnieje jednak możliwość zaszyfrowania danych. Jeśli korzystamy z przeglądarki internetowej, powinniśmy zwrócić uwagę na to, czy w przypadku logowania się do banku czy sklepu internetowego, włącza się protokół szyfrowania. Zazwyczaj przeglądarka informuje nas o tym, wyświetlając u dołu symbol zamkniętej kłódki. Jeśli klikniemy na ten symbol, możemy sprawdzić, czy dane są szyfrowane, a także, czy witryna internetowa jest faktycznie tą, za którą się podaje.

W przypadku emaila istnieje możliwość szyfrowania danych w trakcie ich przesyłania. Jeśli serwer, z którego korzystamy, oferuje możliwość korzystania z protokołu SSL, użyjmy jej. W ten sposób zabezpieczymy swoje dane przed możliwością podejrzenia w trakcie przesyłania (to tak, jakbyśmy zakleili list w kopercie). Nie zabezpiecza to jednak przed możliwością odczytania danych, gdy już dotrą na serwer adresata. W tym przypadku potrzebne byłoby zaszyfrowanie samego maila (np. poprzez tzw. PGP, niestety niezbyt popularne), albo korzystanie z podpisu elektronicznego – to jednak temat na osobny artykuł.

4. Wnioski i sugestie

Spróbujmy teraz zebrać to, co zostało powiedziane i przedstawić wnioski.

Przede wszystkim, nasze dane – zarówno osobiste, jak i urzędowe – są równie cenne jak nasze pieniądze. Warto poważnie podejść do kwestii bezpieczeństwa i nie ułatwiać życia przestępcom, hackerom, szpiegom i wrogom Kościoła. Spróbuj zapamiętać i zastosować praktyczne zasady:

1. **Nie korzystaj z tzw. darmowego serwera do prowadzenia korespondencji, która może wymagać poufności, korespondencji urzędowej i oficjalnej**. Możesz oczywiście korzystać z takiego „darmowego” emaila w sytuacjach, gdy nie jest istotne bezpieczeństwo danych – np. gdy jakieś internetowe forum dyskusyjne pozwala brać udział w dyskusji tylko użytkownikom, którzy podali swój adres email. Właśnie do takich sytuacji dobrze jest mieć „zapasowy” czy „darmowy” email, który nie jest naszym głównym adresem. Do każdej poważniejszej korespondencji powinieneś

jednak używać emaila gwarantującego bezpieczeństwo i prywatność danych, takiego jak emaile oferowane na serwerach Opoki czy Kurii Diecezjalnej.

2. **Jeśli jako duszpasterz korzystasz z emaila w jakiejś niekościelnej domenie, miej świadomość, kogo promujesz**. Zarówno Onet, Interia, Wirtualna Polska, jak i – zwłaszcza – O2.pl świadomie i celowo rozpowszechniają treści demoralizujące i antykościelne (w razie potrzeby służę licznymi przykładami). Jak wyglądasz w oczach swoich odbiorców, kiedy do twoich emaili doczepiane są hasła typu: „jestem sexy, jestem cool, kocham pompon i mój strój”? Jak przekonasz swoich uczniów do konieczności bycia konsekwentnym w codziennym życiu, gdy sam swoim adresem email promujesz portal internetowy, który „bije po oczach” hasłami typu: „Śluby w kościele są nieopłacalne. Można to zrobić taniej i dużo bardziej oryginalnie” (o2.pl, 1.09.2010), „Cała prawda o finansach Kościoła: oto miliardy, które wypłaca państwo” (wp.pl, 5.09.2010), „Pali, pije i wygląda jak Jezus” (onet.pl, 7.04.2010), „Boże Narodzenie bez Boga” (onet.pl, 25.12.2008)
3. Zadbaj o to, żeby twoje konto emailowe było zabezpieczone **odpowiednim hasłem**. Wygoda, tzn. zbyt proste hasło, może bardzo dużo kosztować!
4. Do odbierania poczty używaj **prawdziwego programu pocztowego** (Outlook, Thunderbird, Bat), a nie przeglądarki internetowej.
5. Bierz pod uwagę, że ludzi nieuczciwych i złośliwych nie brakuje na tym świecie – **zabezpiecz więc swój komputer przed atakami**, a gdy korzystasz z obcego komputera, nie loguj się do własnej poczty ani banku!