

Z miesiąca na miesiąc rośnie dostępność naszych danych osobowych w Internecie. Popularne portale społecznościowe ułatwiają życie nie tylko naszym znajomym, lecz także marketerom i internetowym przestępcom. Tych ostatnich łączy kreatywność, za którą stara się nadać prawo i administratorzy serwisów internetowych. Gdzie zakończy się ten wyścig i kto zostanie jego zwycięzcą? Czy istnieje złoty środek na prywatność w sieci?

„Musimy przygotować się na wielkie zmiany” – powiedział w styczniu 2010 roku Mark Zuckerberg, założyciel Facebooka, w odniesieniu do coraz bardziej rozluźnionych zasad prywatności na swoim portalu. Facebook przywitał rok 2010 z blisko dwumilionową rzeszą użytkowników w samej Polsce, szacowanym na siedemset milionów dolarów przychodem, a także coraz bardziej palącym problemem cyberprzestępców, których zbiorowe szaleństwo społeczności przyciąga niczym magnes.

Domyślne ustawienia prywatności profili tworzonych obecnie na Facebooku ujawniają dane dotyczące rodziny, zainteresowań czy edukacji użytkownika. Jak pokazały badania – blisko połowa osób korzystających z portali społecznościowych akceptuje zaproszenia od nieznajomych. Powiększając sieć kontaktów i ilość dostępnych informacji na swój temat, przeciętny Kowalski nie zawsze domyśla się skutków swoich działań.

Marketerzy i złodzieje szyją na miarę

W bieżącym kwartale kampanie oparte o portale społecznościowe zawładnęły wyobraźnią setek tysięcy Polaków. Akcje marketingowe na Facebooku przeprowadziły m.in. Netia, Samsung, Danone czy Maxwell House. Przeciętna strona fanów marki osiąga ok. 50 tysięcy użytkowników. Teraz Jan Kowalski dzięki swojej aktywności w społecznościach otrzymuje oferty skrojone na miarę – np. ofertę pakietu ubezpieczeń przygotowaną na bazie jego daty urodzenia, obecnego pracodawcy i samochodu.

Z pomocą tych samych, łatwo dostępnych danych, cyberprzestępca może podszyć się pod osobę, która – jak wynika z profilu Kowalskiego – jest jego szefem lub żoną. Może dzięki temu zastosować tzw. phishing, wyłudzać od ofiary, pod pretekstem i presją czasu, hasło do konta bankowego. „To obecnie najbardziej dokuczliwa forma cyberprzestępstw. Takiego targetowania nie powstydziliby się nawet najwięksi reklamodawcy” – komentuje Tomasz Zamarlik z G Data Software, znanej firmy zajmującej się bezpieczeństwem sieciowym.

Reklama to nie SPAM

Jak podają firmy e-mail marketingowe, przeciętna wysyłka newslettera daje skuteczność na poziomie od trzech do ośmiu procent. Prosta matematyka prowadzi do konkluzji, że aby zdobyć tysiąc nowych klientów, trzeba wysłać ponad trzydzieści tysięcy maili. Dlatego e-mail Kowalskiego jest w cenie. Podobnie jak jego zgoda na wysyłanie przesyłek reklamowych, niezbędna, by marketer nie stał się przestępcą i nie podlegał karze grzywny na mocy prawa o świadczeniu usług drogą elektroniczną, obowiązującego od 2002 roku.

Cyberprzestępcy oczywiście nie płacą za swoje bazy, a po prostu je kradną, niespecjalnie też przejmując się ustawami. Każda zarejestrowana i zhackowana skrzynka e-mailowa to baza nowych kontaktów. Dzięki nowym możliwościom społecznościowym kierowanie wysyłek z wirusem zaszytym w pliku mp3 do osób zainteresowanych np. muzyką stało się dziecinnie proste.

Cyberprzestępcy delegalizują marketing?

Ustawa z 2002 roku, która uregulowała zasady masowego rozsyłania e-maili, znacznie utrudniła pracę marketerom, niewiele bardziej powstrzymując cyberprzestępców. Prawo nie nadało za rozwojem technologii i problem ten ma zasięg globalny. Administratorom serwisów internetowych będzie zawsze zależało na przyciąganiu jak największej liczby reklamodawców, stąd ułatwiają użytkownikom szybki import list kontaktów np. ze skrzynek e-mail, stosują też coraz bardziej liberalne zasady prywatności. Wydaje się, że jedynie technologia jest w stanie gonić samą siebie. Firmy zajmujące się bezpieczeństwem w sieci oferują obecnie najskuteczniejsze metody walki z zagrożeniami płynącymi z Internetu.

Prywatność zaczyna się w domu

„Uświadomienie ryzyka jest antidotum w każdej dziedzinie. Od momentu uzyskania świadomości zaczynamy postępować ostrożniej – mówi Tomasz Zamarlik z firmy G Data Software – Udostępniamy dane masowo, logując się na naszą ulubioną społeczność, w profilach, robiąc zakupy, komunikując w opisie na GG «Jestem na uczelni». Marząc o anonimowości nie powinniśmy ograniczać się do myślenia tylko o danych udostępnianych poza naszym komputerem – w sieci – ale również do tego co archiwizujemy lokalnie. Skuteczne zabezpieczanie zdjęć, dokumentów takich jak CV czy plików, w których przechowujemy ważne informacje jest konieczne”.

Szukając złotego środka na anonimowość warto zatem myśleć i lokalnie i globalnie. Warto np. dać się znaleźć w Internecie potencjalnemu pracodawcy czy kontrahentowi. Warto podtrzymywać relacje ze znajomymi i dalszą rodziną. Warto też stosować oprogramowanie, które zabezpiecza komputer przed podejrzaną aktywnością z zewnątrz. To, co najważniejsze pozostaje w kwestii samego użytkownika – świadomość i decyzja o działaniu.

Someday Interactive