BEZPIECZEŃSTWO I OCHRONA PRYWATNOŚCI W INTERNEICE. ORAZ PODCZAS UŻYWANIA TELEFONÓW KOMÓRKOWYCH. PRAKTYCZNY PRZEWODNIK DLA OBYWATELI KRAJÓW BLISKIEGO WSCHODU I AFRYKI PÓŁNOCNEJ – STAN: LIPIEC 2011

Niniejszy przewodnik został stworzony dla obywateli krajów Bliskiego Wschodu i Afryki Północnej, którzy chcą bezpiecznie porozumiewać się, organizować i wymieniać informacje (wiadomości, multimedia itp.) za pośrednictwem nowoczesnych technologii. Zgromadzone tu wskazówki mogą posłużyć każdemu użytkownikowi Internetu, który chce bardziej zadbać o swoją prywatność i bezpieczeństwo. Przewodnik jest dostosowany dla szerokiego kręgu odbiorców. Nie trzeba być ekspertem, by móc wykorzystać podane wskazówki bezpieczniejszego korzystania z Internetu i telefonu komórkowego. Przewodnik zawiera rady i instrukcje dotyczące ochrony przed nadzorem i monitorowaniem, ochrony prywatności oraz radzenia sobie z internetową cenzurą. Szczegółowo omówione zostaną następujące kwestie:

- bezpieczne korzystanie z poczty elektronicznej i czatów,
- używanie bezpiecznych haseł,
- ochrona komputera przed wirusami i złośliwym oprogramowaniem,
- omijanie internetowej cenzury przy zachowaniu anonimowości,
- bezpieczne sposoby używania telefonów komórkowych.

Tekst zawiera liczne odsyłacze do stron szczegółowo opisujących poszczególne zagadnienia. W przypadku problemów z dostępem do linków opisanych poniżej, pomimo zastosowania serwerów pośredniczących, prosimy o kontakt na adres info@accessnow.org – wszelkie interesujące Państwa materiały prześlemy pocztą elektroniczną.

Informacje zamieszczone w przewodniku są dokładne, precyzyjne i odpowiadają stanowi na lipiec 2011 r.. Ochrona jednostki w Internecie jest skomplikowanym, ciągłym procesem, a zabezpieczenia zmieniają się wraz z powstawaniem nowych technologii. Nie istnieje sposób, który w 100 procentach gwarantowałby bezpieczeństwo i prywatność w sieci, ale opisane poniżej strategie mogą w znacznym stopniu ochronić komputer lub telefon przed ingerencją z zewnątrz.

Niniejszy dokument został sporządzony i zatwierdzony przez liczne organizacje i osoby, będące ekspertami w dziedzinie prywatności elektronicznej. Jeżeli w naszym przewodniku znajdą Państwo nieprawidłowości lub nieścisłości, prosimy o kontakt: info@accessnow.org.

Najważniejsze informacje

Zabezpieczanie poczty elektronicznej

Spośród najpopularniejszych dostawców poczty elektronicznej, Gmail i Hotmail zapewniają bezpieczne przesyłanie informacji między serwerami użytkowników a serwerem poczty przy pomocy protokołu szyfrującego (HTTPS).

Gmail ma domyślnie włączony protokół HTTPS, natomiast w usłudze Hotmail, trzeba go aktywować ręcznie (jeżeli Hotmail już wcześniej nie wyświetlił komunikatu o takiej możliwości). W tym celu należy wybrać: Account > Other Options > Connect Using HTTPS > Use HTTPS Automatically. Z kolei usługa Yahoo Mail nie jest aktualnie dostatecznie zabezpieczona – osobom posiadającym tam konta pocztowe radzimy, aby zadały sobie trud i

przynajmniej tymczasowo założyły konto na serwerze, który stosuje HTTPS. Szczególnie, jeśli przesyłają Państwo drogą mailową poufne informacje. Należy pamiętać, że protokół HTTPS szyfruje jedynie transmisję danych pomiędzy nadawcą a serwerem poczty, natomiast dane przesyłane z serwera do odbiorcy mogą zostać odszyfrowane, jeżeli odbiorca nie używa protokołu HTTPS lub korzysta z usług innego dostawcy poczty elektronicznej. Inne serwery zapewniające bezpieczna komunikację to: Riseup.net czy Vaultletsoft. Ponadto, istnieją dwa skuteczne systemy szyfrowania i elektronicznego podpisywania wiadomości – PGP oraz GPG. Więcej na ten temat można przeczytać w języku polskim angielskim lub arabskim.

Jeśli korzystają Państwo z usługi Gmail i chcieliby się dowiedzieć o innych zabezpieczeniach (dwuetapowa weryfikacja przy logowaniu oraz lista adresów IP, z których logowano się na konto), warto zapoznać się z Listą kontrolną zabezpieczeń Gmail. Klienci usługi Hotmail mogą zasięgnąć szczegółowych informacji na temat zabezpieczeń, jak np. hasła jednorazowe tutaj.

Jak skutecznie zabezpieczyć hasło?

- Hasło powinno składać się z więcej niż jednego słowa;
- Hasło powinno zawierać przynajmniej 12 znaków – trudniej jest je wówczas złamać za pomocą programów hakerskich;
- Hasło powinno zawierać symbole, liczby oraz małe i wielkie litery. Aby łatwiej zapamiętać takie hasło można, zastąpić określone słowa symbolami i cyframi. Hasłem może być np. powiedzenie lub fragment piosenki czy wiersza;
- Nie należy używać tego samego hasła dla wszystkich kont – wystarczy, że użytkownik wpisuje hasło na stronie, która nie jest zabezpieczona protokołem HTTPS, a przechwycone hasło może być wykorzystywane przez osoby trzecie do logowania się w innych miejscach;
- Należy zmieniać hasła mniej więcej raz na 3 miesiące lub częściej jeżeli, regularnie korzystają Państwo z obcych komputerów np. w kawiarenkach internetowych;
- W przypadku problemów z zapamiętywaniem haseł, pomocny może się okazać odpowiednio zabezpieczony program do ich przechowywania, np. KeePass;
- W systemie odzyskiwania hasła należy wprowadzić takie dane, które nie są możliwe do odgadnięcia przez osoby trzecie – wybrane pytania i odpowiedzi nie powinny być oczywiste;

Oprogramowanie antywirusowe i antyszpiegowskie

Instalowanie nielegalnego oprogramowania, w szczególności Windowsa, może okazać się brzemienne w skutkach dla użytkownika. Posiadanie pirackich programów wiąże się wprawdzie z pewną oszczędnością finansową, jednakże często uniemożliwia instalowanie aktualizacji i „łatek" publikowanych przez producentów, co przekłada się na luki i błędy w zabezpieczeniach. Jeśli użytkownik nie posiada legalnych wersji oprogramowania, powinien przynajmniej mieć zainstalowane skuteczne programy antywirusowe i antyszpiegowskie (anti-spyware), aby zminimalizować ryzyko naruszenia prywatności. Dla własnego bezpieczeństwa, warto mimo wszystko zadbać o legalne wersje posiadanych programów.

- Dla użytkowników nieposiadających legalnego oprogramowania, a korzystających z systemu operacyjnego Windows, skutecznym programem antywirusowym jest Avast,

który zapobiega uszkodzeniu i zainfekowaniu danych. Z kolei program Malwarebytes przydaje się wówczas, gdy wiemy już, że komputer jest zawirusowany.

- Równie ważne jest oprogramowanie antyszpiegowskie. Identyfikuje i usuwa ono złośliwe aplikacje, które rejestrują aktywność użytkownika online i offline. Bezpłatnym i skutecznym programem tego typu jest Spybot.
- Aby chronić komputer przed wirusami i oprogramowaniem typu spyware, należy unikać otwierania wiadomości e – mail i załączników z nieznanych lub niezaufanych źródeł. Niepewny link lub stronę można przetestować za pomocą aplikacji VirusTotal lub wysłać odnośnik na adres scan@virustotal.com, umieszczając w temacie wiadomości słowo „SCAN" (lub „SCAN-XML" jeżeli chcą Państwo otrzymać odpowiedź w formacie XML).
- Złośliwe oprogramowanie może się zainstalować w systemie użytkownika za pośrednictwem skryptów, które pojawiają się podczas „surfowania" w Internecie. Doskonałym narzędziem zabezpieczającym jest w tym przypadku NoScript, dodatek do przeglądarki Firefox, który blokuje większość skryptów i tworzy wyjątki dla zaufanych aplikacji.
- Złośliwe oprogramowanie może się zainstalować w systemie użytkownika za pośrednictwem pendrive'ów i innych dysków wymiennych. Nie należy podłączać przenośnych urządzeń, które pochodzą z nieznanego lub niezaufanego źródła. Do skanowania nośników USB, przydają się wspomniane programy Spybot i Avast

Warto rozważyć zmianę systemu operacyjnego na Ubuntu, opartego na Linuksie, chyba, że istnieją ważne powody dla pozostania przy Windowsie. Ubuntu ma domyślnie ustawione szyfrowanie danych, przez co jest w zasadzie wolny od wirusów i złośliwego oprogramowania. Bez względu na rodzaj ataków na system, użytkownik Ubuntu jest znacznie lepiej zabezpieczony niż internauta korzystający z niezaktualizowanej, niepełnej lub nielegalnej wersji Windowsa. Mint jest systemem operacyjnym podobnym do Ubuntu, który umożliwia bezpieczne korzystanie z większej ilości programów.

Bezpieczne posługiwanie się komunikatorami

Jeśli uważają Państwo, że prowadzona przez Państwa korespondencja w sieci nie stanie się celem dla hakerów, możecie Państwo czatować przy użyciu Skype lub Google Chat przy włączonym przez Gmail HTTPS. Znacznie skuteczniejszym rozwiązaniem jest aplikacja Pidgin, która umożliwia bezpieczną komunikację np. poprzez Google Talk. Elementem zabezpieczającym w Pidgin jest wtyczka Off The Record (OTR). Nawet gdyby zostały przechwycone klucze szyfrujące, to zakodowane przez nie informacje nie będą miały żadnej potencjalnej wartości. Szczegółowe informacje na temat ustawień bezpieczeństwa OTR znajdują się tutaj. Off The Record stanowi przykład zabezpieczeń zintegrowanych z usługą on-line już na etapie jej projektowania (tzw. Privacy by Design)

Jak jeszcze można zabezpieczyć się w Internecie?

- Aby zachować anonimowość podczas uczestnictwa w wydarzeniach on-line, np. na portalach społecznościowych i platformach multimedialnych, warto logować się za pomocą tzw. aliasów, czyli alternatywnych nazw użytkownika. Przyjęty zakres anonimowości zależy od potrzeb internauty. Częstą praktyką jest tworzenie anonimowych tożsamości na Twitterze, ale w przypadku takich portali jak Facebook, większość osób loguje się używając swojego faktycznego imienia i nazwiska. Decyzja powinna zależeć od tego, jak bardzo użytkownik boi się, że jego aktywność w sieci będzie szczegółowo monitorowana. Chcąc zachować anonimowość na Facebooku, należy wymyślić sobie

realistycznie brzmiące imię i nazwisko, gdyż zastosowanie jednowyrazowego pseudonimu pozwala łatwo wykryć jego nieautentyczność, jak również stanowi naruszenie regulaminu portalu, w wyniku którego takie konto zostanie usunięte.

- Jeżeli użytkownik decyduje ujawnić na Facebooku swoje dane personalne i przy tym używa zabezpieczenia w postaci HTTPS, ważne jest, by publikować możliwie najmniej osobistych danych, takich jak np. numer telefonu, adres.
- Coraz łatwiejsze staje się wykorzystanie nawigacji GPS do przesyłania do sieci informacji o położeniu geograficznym użytkownika. GPS może być skutecznym medium pomagającym w lokalizacji osób w określonych sytuacjach. Z drugiej strony, te same, poufne informacje na temat położenia i aktywności użytkownika mogą być wykorzystane przez osoby trzecie. Proponujemy wyłączenie opcji monitoringu GPS na takich platformach jak Twitter czy Bambuser, chyba, że funkcja ta z jakiegoś powodu jest niezbędna. Nawet, jeśli funkcja GPS nie jest wyświetlana, bardzo ważne jest, by wyłączyć dostęp do tych informacji w przeglądarce lub innym kanale dostępu.
- Należy pamiętać, że treści poufne jak np e – maile, listy kontaktów czy innego rodzaju przesyłane informacje, mogą być niewystarczająco zabezpieczone, a co za tym idzie, monitorowane przez osoby trzecie. Szczególną ostrożność warto zachować, kiedy nie jesteśmy w stanie zweryfikować tożsamości odbiorcy informacji. Ponadto, wszelkie wiadomości wysyłane bezpośrednio do adresata (znanego lub nieznanego) za pomocą Facebook`a lub Twitter`a mogą być czytane przez osoby trzecie, jeżeli nie zostały należycie zabezpieczone (szczegóły na ten temat znajdują się w sekcji dotyczącej HTTPS oraz omijania cenzury).
- Należy w jak najmniejszym zakresie używać aplikacji zewnętrznych, które wymagają dostępu do kont użytkownika (np. aplikacje skojarzone z Facebook`iem, Twister`em czy Gmail`em). Programy te często posiadają luki w zabezpieczeniach i są używane do włamań na konta zabezpieczone już na inne sposoby.

Bezpieczeństwo on-line

W wielu krajach, takich jak Bahrajn, Kuwejt, Arabia Saudyjska, Oman, Katar, Syria czy Zjednoczone Emiraty Arabskie władze cenzurują Internet w bardzo szerokim zakresie. W wymienionych państwach, aktywność internautów w sieci jest także monitorowana na nieznaną skalę. Nawet jeśli użytkownikowi uda się ominąć cenzurę, to problemem pozostaje zabezpieczenie przed monitorowaniem, co w praktyce jest znacznie trudniejsze. Jednym ze sposobów może być używanie zabezpieczającego serwera proxy, który nie ujawnia tożsamości użytkowników. Co więcej, zdecydowanie odradzamy używania przeglądarki Internet Explorer, gdyż posiada ona liczne luki w zabezpieczeniach, w szczególności w nielicencjonowanej wersji programu. Niezawodną, bezpłatną przeglądarką jest natomiast Mozilla Firefox posiadająca wiele przydatnych wtyczek i dodatków.

Szyfrowanie aktywności w sieci za pomocą HTTPS

Jeżeli biorą Państwo udział w kampaniach społecznych w sieci, warto podkreślić, że bardzo ważne jest, aby chronić dane o tożsamości oraz hasła dostępu do portali wokół których gromadzą się uczestnicy kampanii. Niedawno w Tunezji zorganizowano na bardzo szeroką skalę akcję polegającą na wykorzystaniu błędów w zabezpieczeniach użytkowników Facebook`a, w celu wyłudzenia haseł i informacji o logowaniu. Na szczęście Facebook szybko zareagował, umożliwiając swoim klientom włączanie HTTPS. Warto używać tego protokołu, kiedy tylko jest to możliwe. W przypadku, gdy nie istnieje opcja włączenia HTTPS, należy koniecznie korzystać z usług jednego z zabezpieczonych serwerów proxy.

Jeśli używają Państwo serwera animizującego typu TOR, naruszenie Państwa prywatności przez osobę trzecią będzie bardzo trudne lub wręcz niemożliwe.

HTTPS

Niezawodnym i łatwym w obsłudze dodatkiem do Firefoxa jest protokół HTTPS Everywhere. Aplikacja ta „zmusza" przeglądarkę do używania HTTPS na każdej stronie, która to umożliwia. **Ściągnięcie tej aplikacji powinno być jednym z pierwszych kroków mających na celu obustronnie zabezpieczone korzystanie z takich stron jak np Facebook, Twitter, lub wyszukiwarka Google.** Ten rodzaj zabezpieczenia zmniejsza ryzyko wyłudzania haseł podczas korzystania z publicznie dostępnych sieci internetowych.

- Jeżeli nie posiadają Państwo najnowszej wersji przeglądarki Firefox, należy ją ściągnąć. Kolejnym krokiem jest pobranie dodatku HTTPS Everywhere i/lub Force TLS. Następnie należy ponownie uruchomić przeglądarkę i skonfigurować ustawienia. Uwaga: HTTPS Everywhere posiada wbudowaną już listę stron, przy których będzie się włączał HTTPS. Listę tę można dowolnie edytować. Dodatek Force TLS jest bardziej spersonalizowany i wymaga samodzielnego stworzenia takiej listy.
- Dla użytkowników Google Chrome, polecamy dodatek KB SSL Enforcer Extension (Uwaga: ta aplikacja nie jest tak skuteczna jak wyżej wymienione dodatki do Firefox). Chociaż SSL Enforcer zawiera jeszcze drobne błędy, aplikacja ta jest stale udoskonalana.

Facebook

Pomimo, że opisany powyżej dodatek do Firefox wymusza HTTPS na większości stron, przy częstym używaniu Facebook`a warto ustawić stronę portalu społecznościowego jako automatycznie uruchamiającą się w trybie HTTPS, szczególnie w przypadku, gdy użytkownik loguje się z różnych komputerów.

- Aby włączyć HTTPS dla Facebooka, w prawym górnym rogu, należy kliknąć na Konto – Ustawienia konta. Następnie z lewego menu należy wybrać Bezpieczeństwo. Klikamy Edytuj, przy pierwszej opcji – Bezpieczne przeglądanie, i zaznaczamy włączenie HTTPS.
- Niektóre gry i dodatki Facebooka automatycznie wyłączają HTTPS.
- Facebook posiada również inne zabezpieczenia tj. zdalne wylosowywanie lub powiadomienia dotyczące logowania. Przewodnik dotyczący bezpieczeństwa na Facebooku można znaleźć tutaj po polsku lub tutaj w wersji angielskiej.

Twitter

Mimo, że również w przypadku Twitter`a, wspomniane dodatki do Firefox`a właczają HTTPS na stronach portalu, warto zmienić domyślne ustawienia dla Twitter`a na HTTPS, szczególności, jeśli korzystają Państwo z tych stron na różnych, ogólnodostępnych komputerach.

- Aby włączyć HTTPS dla Twitter`a, w prawym górnym pasku klikamy Settings, na dole strony zaznaczamy pole obok "Always use HTTPS".
- Uwaga: włączenie wspomnianej opcji na dzień dzisiejszy nie działa dla urządzeń przenośnych. Zanim ten problem zostanie naprawiony, należy posługiwać się adresem https://mobile.twitter.com.

Omijanie cenzury, odwiedzanie zablokowanych stron

W wielu krajach, strony sieci Web i blogi są starannie filtrowane. Można stąd wyciągnąć wniosek, że władze intensywnie monitorują Internet, przy czym zakres monitorowania różni się w poszczególnych państwach. Aby odwiedzać zablokowane strony i publikować tam różnego rodzaju materiały, zostały stworzone narzędzia omijające cenzurę. Trzeba przy tym pokreślić różnicę pomiędzy szyfrowaniem, a prywatnością/anonimowością. Narzędzia omijające cenzurę szyfrują przesył danych pomiędzy użytkownikiem, a administratorem narzędzi, ale nie są w stanie zaszyfrować przepływu informacji od administratora do odwiedzanej strony. Dlatego też ważne jest, aby używać HTTPS kiedy tylko to możliwe, gdyż takie rozwiązanie zapewnia całkowite szyfrowanie. Jednakże, sam HTTPS nie umożliwi dostępu do zablokowanych stron, niezbędne są dodatkowe narzędzia. Adres IP użytkownika jest zawsze dostępny dla zdalnego operatora. Można go efektywnie ukryć jedynie za pomocą serwera anonimizującego proxy (jak np. TOR). Wiele usług, z których korzystamy w sieci zawiera opcję „ostatnie logowanie" i w przypadku włamania na konto, osoba trzecia będzie miała dostęp do tych danych.

Omijanie zapory sieciowej

Proste serwery proxy umożliwiają użytkownikom dostęp do zablokowanych stron za pośrednictwem specjalnych formularzy. Na takim formularzu na stronie proxy, użytkownik wpisuje adres strony, którą chce odwiedzić. Serwer odnajdzie i wyświetli żądaną witrynę. Serwery proxy HTTP/SOCKS organizują przepływ danych przy użyciu protokołów, które pomagają ominąć zapory sieciowe. Adresy IP oraz numery portów dostępne na listach serwerów proxy są dodawane do ustawień wyszukiwarki. **Pomimo, że zarówno serwery proxy typu HTTPS / SOCKS, jak i te oparte na sieci spełniają swoje zadanie jako narzędzia do omijania cenzury, nie zapewniają one anonimowości, co oznacza, że ich wykorzystywanie przez użytkownika może być monitorowane. Z reguły nie wiadomo, kto jest właścicielem tych serwerów. Istnieje wiele zagrożeń związanych z ich wykorzystywaniem, dlatego warto używać jednej, sprawdzonej usługi (jak np. TOR), która umożliwia omijanie cenzury, jak również zapewnia anonimowość.**

Innym rozwiązaniem opartym na proxy jest Psiphon – niewielka aplikacja działająca z Windows`em i Linux`em. Po zainstalowaniu programu, komputer użytkownika staje się punktem dostępowym dla innych użytkowników, nie jest on jednak serwerem ogólnodostępnym. Ideą projektu było umożliwienie przeciętnym obywatelom, którzy nie posiadają specjalistycznego sprzętu, stworzenia ze swoich komputerów zaufanych serwerów proxy, które będą służyć małej, zamkniętej grupie „przyjaciół", przebywającym w kraju, gdzie Internet jest cenzurowany. Jest to tzw. „sieć zaufania", w której komputer właściciela prywatnego serwera, stworzonego za pomocą Pshipona rejestruje przepływ danych z komputerów osób korzystających z tego proxy, co oznacza, że relacja pomiędzy właścicielem a użytkownikiem serwera powinna być „zaufana." **Psiphon zapisuje informacje o użytkownikach, przy czym adresy IP pozostają anonimowe**. Psiphon 2 jest „rozwiązaniem chmurowym„ zarządzanym centralnie przez firmę Psiphon Inc, składającym się z serwerów proxy przepisujących linki. Psiphon 1 i 2 mają problemy z ładowaniem stron z włączonym HTTPS lub opartych na Web 2.0. Z tymi przeszkodami skutecznie radzi sobie najnowszy produkt kanadyjskiej firmy – Psiphon X.

TOR. Anonimowość w sieci

TOR jest znakomitym, rozbudowanym programem służącym do omijania filtrów sieciowych i ochrony prywatności. Jego główną wadą jest jednak spowalnianie przeglądania stron. Paczka Tora z Przeglądarką umożliwia używanie aplikacji bez konieczności instalowania. „Mostki" przydają się, kiedy w lokalnym środowisku sieciowym występuje wiele filtrów.

Aplikacji TOR można używać na wiele sposobów. Przede wszystkim, zalecamy pobranie „paczki" Tora z przeglądarką, która umożliwia używanie programu pod Windowsem, Mac OS X i Linuxem bez potrzeby instalowania złożonych aplikacji. Wystarczy uruchomić „paczkę", a automatycznie otworzy się specjalna wersja Firefoxa oraz Vidalia – interfejs dla TORa, domyślnie skonfigurowany do odbierania i wysyłania wszystkich danych. „Paczka" może być uruchamiana z dysku USB, a zatem może być wykorzystywana przy pracy na wielu komputerach. Istnieje również wersja „paczki" z zabezpieczonym komunikatorem w wielu wersjach językowych (można je pobrać np tutaj). Mając na uwadze fakt, że TOR spowalnia pracę w Internecie, zalecamy używanie dwóch przeglądarek – strony, których przeglądanie może stanowić zagrożenie dla bezpieczeństwa użytkownika (np. zablokowane strony), najlepiej jest otwierać w przeglądarce skojarzonej z TORem, natomiast w pozostałych przypadkach można używać innej przeglądarki. Jeżeli nie będziemy wyłączać TORa, z czasem będzie on działał coraz efektywniej i spowolnienie pracy będzie coraz mniej odczuwalne. Jeżeli mimo to uznają Państwo, że przeglądarka współpracująca z TORem działa zbyt wolno, a przeglądane informacje mają format tekstowy, warto wyłączyć ładowanie grafiki oraz skryptów Java. Takie działanie może znacznie przyspieszyć otwieranie stron.

Niestety, w wielu krajach strona projektu TOR jest zablokowana. Oto inne sposoby na zdobycie tego oprogramowania:

- Odwiedzenie strony TORa przy użyciu HTTPS: https://www.torproject.org/
- Odnalezienie obrazu strony torproject.org poprzez wpisanie w Google frazy „tor mirror". Z kolei po „wygooglowaniu" "site:torproject.org mirrors", jako jeden z wyników wyszukiwania wyświetli się oficjalna lista dostępnych obrazów TORa – należy wówczas kliknąć na link „Kopia" (wyświetlony na niebiesko obok adresu).
- Można również zamówić Paczkę wysyłając email na adres gettor@torproject.org. Uwaga, dla bezpieczeństwa i w celu osiągnięcia jak najlepszej efektywności, warto używać konta Gmail zabezpieczonego za pomocą HTTPS. W dowolnym miejscu w treści wiadomości należy wpisać nazwę programu.
  - Jeżeli pracujemy używając systemu Windows, w e – mailu należy wpisać „tor-im-browser-bundle" (otrzymamy Tor wraz z komunikatorem).
  - Jeżeli pracujemy pod Windowsem, OR Intel, Mac OS X lub Linuxem, w emailu należy wpisać „tor-browser-bundle" (otrzymamy Paczkę Tora z Przeglądarką).

Wkrótce po wysłaniu e-maila, automat wygeneruje odpowiedź – będzie to email od „Gettor" z programem w załączniku w formacie archiwum zip. W razie pytań dotyczących TORa, prosimy o kontakt na adres tor-assistants@torproject.org .

Uwaga: TOR jest również dostępny dla telefonów z Androidem, występuje tam pod nazwą „Orbot." Aplikację można znaleźć na stronie Android Market lub pobrać bezpośrednio ze strony TORa bądź jego obrazów.

Inną formą omijania filtrów sieciowych zapewniającą anonimowość są sieci VPN. Informacje na temat zakładania takiej sieci można znaleźć tutaj. Pomocną aplikację – VPN Hotspot Shield można pobrać tutaj, można też wysłać email na adres hss-

sesawe@anchorfree.com (temat wiadomości powinien zawierać jedno ze słów: „has", „seasawe" lub „hotspot").

Kolejnym sposobem radzenia sobie z cenzurą są sieci Ultrasurf oraz Freegate. Stanowią one przydatne narzędzia do przeglądania zablokowanych stron. Warto jednak pamiętać, że podobnie jak proste serwery sieciowe proxy czy proxy typu HTTPS/ SOCKS, nie anonimizują one użytkownika, tzn. nie ukrywają jego tożsamości podczas ich używania. Ponadto, właściciele tych aplikacji blokują strony, które uznają za stosowne. Co więcej, Ultrasurf i Freegate rejestrują dane wszystkich użytkowników. Usługi te mają charakter komercyjny i czerpią dochód z wysyłania do użytkowników spersonalizowanych reklam na podstawie ich danych, takich jak odwiedzane strony, słowa wpisywane w wyszukiwarkach itd. Ta informacja może mieć decydujące znaczenie dla osób, które chcą zagwarantować sobie anonimowość w sieci lub po prostu chcą „dyskretnie" używać oprogramowania omijającego filtry.

Ważne: Jeżeli rząd danego kraju ma możliwość kontrolowania dostarczanych usług internetowych, może stosować wiele innych metod celem ograniczenia anonimowości i prywatności internautów np. poprzez wprowadzenie certyfikatów bezpieczeństwa. Opisane powyżej zabezpieczenia mogą uchronić użytkowników przed penetracją danych, które pozostawiają w sieci. Warto również zwracać uwagę na ostrzeżenia od innych działaczy społecznych *on – line*, którzy mogą być dobrym źródłem informacji o technikach infiltracji stosowanych przez władze.

Dodatkowe źródła informacji: Warto obejrzeć Videolekcje dotyczące omijania filtrów sieciowych itp. (tzw. „12 pm Tutorials"). Podobne filmy w języku polskim, choć uboższe w treść, można obejrzeć tutaj lub tutaj, informacje o konfigurowaniu sieci VPN znajdziemy tutaj lub tutaj.

Urządzenia mobilne

Wiele osób aktywnych społecznie, szczególnie w krajach arabskich, jest obserwowanych za pośrednictwem ich własnych telefonów komórkowych. Aktywiści działający w Egipcie doświadczyli tego na bardzo szeroką skalę. Władze w Kairze były w stanie uczynić z telefonów osób im niesprzyjających urządzenia monitorujące, nawet jeśli „śledzone" aparaty były czasowo wyłączone. Należy więc rozsądnie ocenić, czy aktywność, którą podejmujemy naraża nas na inwigilację ze strony władz – zależy to głównie od sytuacji politycznej w kraju, w którym znajduje się użytkownik. Operatorzy GSM są w stanie zlokalizować użytkownika na podstawie jego telefonu, dysponują oni również innymi informacjami na temat jego korzystania z aparatu. W wielu krajach, operatorzy przechowują oraz udostępniają te informacje władzom.

Istnieje również możliwość zainstalowania w telefonie oprogramowania monitorującego bez wiedzy użytkownika. Ryzyko takie istnieje, jeżeli użytkownik przez pewien czas nie będzie fizycznie korzystał z swojego aparatu.

Nawet kiedy telefon jest włączony, przesyła nieustannie następujące informacje do lokalnej wieży transmisyjnej:

- IMEI – unikalny numer identyfikacyjny telefonu
- IMSI - unikalny numer identyfikacyjny karty SIM

- TMSI – tymczasowy numer identyfikacyjny przydzielany użytkownikowi sieci przy każdym logowaniu na podstawie lokalizacji. Numer ten jest rozpoznawalny dla komercyjnie dostępnych urządzeń podsłuchowych
- Komórka – jednostka przestrzenna, w której aktualnie znajduje się telefon. Taka komórka może mieć różną powierzchnię – od kilku metrów do kilku kilometrów kwadratowych. Jednostki w miastach są statystycznie znacznie mniejsze. Zdarza się, że w jednym budynku kilka mini-komórek pokrywa się na tym samym obszarze, by zwiększyć jakość sygnału.
- Położenie użytkownika w danej komórce – sygnał nawet z trzech masztów pozwala dokładnie określić lokalizację. Dokładność pomiaru zależy od wielkości komórki – im więcej masztów w okolicy, tym precyzyjniejsze informacje można uzyskać na podstawie telefonu.

Biorąc pod uwagę ilość informacji przesyłanych z włączonego telefonu użytkownika, urządzenie mobilne może być sposobem monitorowania jego właściciela. Na tej podstawie, osoba trzecia może uzyskać następujące dane:

- Połączenia przychodzące i wychodzące
- Wysłane i odebrane wiadomości SMS, informacje o odbiorcach lub nadawcach wiadomości
- Wszelkiego rodzaju usługi, z których korzysta właściciel telefonu – przeszukiwanie Internetu bez HTTPS, niezabezpieczona wymiana informacji przez komunikator oraz rozmiar przesłanych danych, jeśli np użytkownik opublikował coś na Youtube.
- Przybliżone położenie (z dokładnością co do kilku metrów lub kilometrów, w zależności od ilości wież przekaźnikowych).

Uwaga: Jeżeli użytkownik telefonu komórkowego ma podejrzenie, że jest monitorowany, zmiana karty SIM nie zawsze wystarcza, gdyż numer telefonu (IMEI) lub sama obudowa umożliwia przybliżone określenie położenia właściciela.

Telefon może być również źródłem wielu informacji o użytkowniku, jeżeli zostanie odebrany lub skonfiskowany. Wszystkie telefony komórkowe posiadają pewną ilość pamięci na karcie SIM, jak również wewnętrznej pamięci telefonu (ponadto, niektóre urządzenia mobilne posiadają karty pamięci SD i micro SD dla plików multimedialnych). **Zazwyczaj lepiej jest przechowywać dane na karcie SIM lub SD, niż w pamięci telefonu, gdyż w razie potrzeby, łatwiej można usunąć lub zniszczyć zgromadzone tam dane.**

W pamięci telefonu, karcie SIM i SD znajdują się następujące informacje:

- Książka adresowa: kontakty i numery telefonów
- Historia połączeń: połączenia odebrane, nieodebrane, wybierane numery, godziny rozmów
- SMS-y wysłane i odebrane
- Dane z aplikacji jak np. kalendarz czy terminarz.
- Zdjęcia i filmy zrobione aparatem lub kamerą telefonu. Większość telefonów (posiadających aparaty fotograficzne) rejestruje dokładną datę i godzinę, a czasem także miejsce gdzie zostało zrobione zdjęcie).

Użytkownicy surfujący po Internecie przy użyciu telefonów komórkowych powinni wiedzieć, jaka część historii przeglądania stron www jest zapisywana w pamięci. W miarę możliwości,

należy całkowicie usuwać informacje na temat odwiedzanych wcześniej stron. Osoba, która uzyska dostęp do telefonu lub karty SIM użytkownika może mieć również dostęp do jego skrzynki mailowej, jeżeli użytkownik posługiwał się pocztą elektroniczną przez telefon.

Podobnie jak w przypadku dysku twardego na komputerze, pamięć karty SIM gromadzi wszystkie informacje do momentu, kiedy się zapełni – wówczas stare informacje są „nadpisywane" nowymi. Oznacza to, że nawet usunięty SMS, jak również informacje o kontaktach i połączeniach mogą być odzyskane z karty SIM. Istnieje darmowa aplikacja służąca do tego celu (inny program z polskojęzycznej strony można pobrać tutaj). Podobna zasada obowiązuje przy telefonach posiadających dodatkową przestrzeń pamięci lub inne karty pamięci. Zazwyczaj, im więcej informacji można zapisać w telefonie, tym dłużej można odzyskać dane po ich skasowaniu.

Co to oznacza dla użytkownika?

Telefony komórkowe mogą być pomocnymi narzędziami dla osób aktywnych w przestrzeni społeczno-politycznej. Z drugiej strony, mogą być źródłem poważnych problemów, w przypadku, gdy osoby trzecie, np. władze współpracują z operatorami GSM w celu monitorowania użytkowników. **Jeżeli użytkownik znajduje się w kraju, co do którego istnieje podejrzenie, że władze wykorzystują sieci komórkowe do kontrolowania obywateli, w szczególności jeśli użytkownik obawia się, że sam jest w ten sposób zdalnie śledzony, warto zrezygnować z używania telefonów komórkowych do komunikacji i ograniczyć się do osobistych spotkań.**

Od użytkownika zależy, jakie ryzyko jest gotowy podjąć. Czasem nie ma większych obaw, że jego działalność nie jest przedmiotem nadzoru, np. w ramach rozbudowanego systemu kontroli obywateli. W takim przypadku można dalej rozmawiać, robić zdjęcia, nagrywać filmy i przesyłać informacje przez telefon, przy zachowaniu pewnych środków ostrożności:

- Do komunikacji z innymi zaangażowanymi społecznie osobami warto stworzyć system szyfrów i haseł.
- Sposobem komunikacji może być wysyłanie sygnałów – można umówić się wcześniej, że jedno- lub dwukrotny sygnał oznacza np, że użytkownik dotarł na miejsce, jest bezpieczny itd.
- Nie należy używać prawdziwych imion i nazwisk w książce adresowej. Zamiast tego, można wymyślić dla nich numery lub pseudonimy. Dzięki temu, nawet, jeżeli służby bezpieczeństwa skonfiskują telefon użytkownika, nie będą w posiadaniu siatki jego kontaktów.
- Podczas uczestnictwa w protestach lub wiecach, dobrze jest mieć ze sobą zapasowe kopie kart SIM, szczególnie jeżeli wiadomo, że policja konfiskuje karty podczas tego typu wydarzeń. Warto też mieć ze sobą dodatkowy, działający telefon komórkowy. W momencie, kiedy użytkownik musi oddać kartę SIM, będzie mógł ją fizycznie zniszczyć.
- Warto, jeśli to możliwe, zabezpieczyć telefon hasłem. Takim hasłem może być numer PIN karty SIM. (Niektóre telefony mają domyślnie wyłączoną opcję zabezpieczenia poprzez PIN). Kupując telefon, otrzymujemy fabryczny numer PIN – należy go zmienić.
- Jeżeli istnieje obawa, że protesty spotkają się z masową reakcją sił bezpieczeństwa, warto przełączyć telefon na tryb samolotowy –funkcja ta uniemożliwia przesyłanie informacji, przy czym w dalszym ciągu można robić zdjęcia, nagrywać filmy, by później opublikować je w sieci. Ta metoda sprawdza się również, gdy siły bezpieczeństwa namierzają

wszystkich uczestników demonstracji, którzy posiadają przy sobie telefony. Władze mogą uzyskać dostęp do wszystkich informacji wysłanych i odebranych przez uczestnika demonstracji, co może być pretekstem do masowych aresztowań.

- Należy wyłączyć nawigację GPS, geotagging oraz skojarzone z nimi aplikacje, chyba że funkcje te są niezbędne do przeprowadzenia planowanych działań. Aplikacje lokalizujące należy bezwzględnie wyłączyć, jeśli chcemy przeprowadzić wideotransmisję na żywo. Jedną z platform internetowych, gdzie można przesyłać wideo w wersji lifestream - jest Bambuser
- Przeszukiwanie Internetu, rozmowy, SMS-y i korzystanie z komunikatorów przy użyciu telefonu działającego pod Androidem da się zaszyfrować na wiele sposobów – są to np. rozwiązania dostępne na stronach Guardian Project czy Whispersys. (informacje w języku polskim na temat tych projektów są dostępne tutaj i tutaj).
- Podczas surfowania po Internecie przez telefon, zawsze należy używać HTTPS

Informacja dla użytkowników Blackberry

Firma Research In Morion (RIM), która jest producentem Blackberry oferuje dwa rodzaje usług, odpowiednio na dwóch różnych poziomach szyfrowania. Jak do tej pory, zwykli użytkownicy jeszcze nie mogli cieszyć się całkowitymi zabezpieczeniami (typu end-to-end) – Firma RIM lub operator sieci komórkowej mają wgląd w dane dotyczące połączeń, aktywności w Internecie, SMS-y i e- maile. Z kolei klienci komercyjni, których firma korzysta z serwera Blackberry (BES) mogą liczyć na całkowite szyfrowanie informacji (e-maile, komunikatory - BBM i przeglądanie stron).Użytkownik komercyjny powinien przy tym pamiętać, że administrator lokalnego serwera w firmie może odkodować zaszyfrowane już dane, a rządy często są w stanie znaleźć stosowne zapisy prawne, które umożliwią mu pozyskanie tych informacji.

Niedawno władze Zjednoczonych Emiratów Arabskich próbowały wymusić na Research In Morion, aby firma umożliwiła im odszyfrowywanie wszystkich informacji. Producent Blackberry nie ugiął się jednak pod tymi żądaniami. Użytkownicy „jeżynek" powinni śledzić doniesienia na temat negocjacji władz ich krajów z RIM dotyczących udostępnienia powyższych informacji.

Władze używają również różnych forteli by odszyfrować informacje wymieniane pomiędzy posiadaczami Blackberry. W roku 2009 Etisalat, operator telefonii komórkowej w Zjednoczonych Emiratach Arabskich przesłał użytkownikom Blackberry „nieoficjalną" aktualizację oprogramowania. Każdy abonent, który zainstalował tę aktualizację (nieświadomie) udostępniał tym samym Etisalatowi kopie wszystkich przesyłanych wiadomości. Wkrótce potem RIM przekazał swoim klientom uaktualnienie, które usuwało szpiegowską aplikację, co nie zmienia faktu, że właściciele „jeżynek" powinni zachować ostrożność w stosunku do wszelkiego rodzaju oprogramowania nie pochodzącego bezpośrednio od RIM.

Przydatne strony:
Strona projektu Tactical Technology Collectiva Mobiles in a Box (wersja anglojęzyczna)
Artykuł na stronie MobileActive.org: Mobile Security Risks Primer (wersja anglojęzyczna)

Inne:

Prowadzenie blogów
Jeżeli użytkownik prowadzi bloga lub zamierza go założyć, istnieje wiele sposobów na zabezpieczenie publikowanych informacji i własnej osoby oraz na stworzenie internautom dostępu do strony, w wypadku gdy zostanie ona zablokowana. Poniżej znajdują się linki do stron zawierających instrukcję, w jaki sposób można skutecznie obejść problem zablokowanego bloga (w języku angielskim).

Anonymous blogging with wordpress and Tor (Global Voices)
Mirroring a censored wordpress blog (Global Voices)
Tips on how to blog safely (EFF)
Handbook for Bloggers (Reporters Without Borders)

Nagrywanie video
Instrukcja: Video for Change

Inne źródła dotyczące bezpieczeństwa i cyfrowego aktywizmu:
Tactical Tech & FrontLine – Bezpieczeństwo w pigułce: Arabski Angielski
Fundacja The Electronic Frontier – szczegółowy przewodnik: Surveillance Self-Defense & ogólnie informacje: International edition of SSD (strony anglojęzyczne)

Tłumaczenie: Maciej Małaj

Moje uwagi (TŁUMACZA – przyp. dg)

Inne strony, które znalazłem, polski Internet jest ubogi w takie przewodniki jak poniżej, znalazłem kilka artykułów:
http://www.freecellphonespying.com/pl/cell-phone-spying-that-allows-gps-tracking/
https://www.upc.pl/internet/bezpieczenstwo-w-sieci/
http://www.uczdziecko.pl/mlodszy-uczen/artykuly/artykul/zobacz/bezpieczenstwo-w-sieci.html