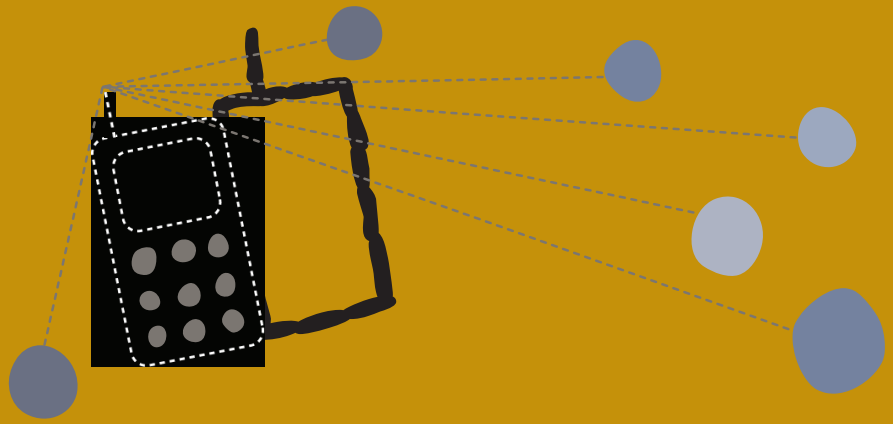
Безпека та конфіденційність при користуванні інтернетом та мобільним зв'язком



НОВІ ТЕХНОЛОГІЇ, ЗОКРЕМА МОБІЛЬНИЙ ТЕЛЕФОН ТА ІНТЕРНЕТ, Є ПОТУЖНИМ ІНСТРУМЕНТОМ ДЛЯ ЗАХИСТУ ПРАВ ЛЮДИНИ, АЛЕ ЇХНЄ ВИКОРИСТАННЯ У ВИПАДКУ ОБМІНУ ОСОБИСТОЮ ІНФОРМАЦІЄЮ МОЖЕ БУТИ РИЗИКОВАНИМ ДЛЯ ВАС, ВАШИХ СПІВРОЗМОВНИКІВ, ДРУЗІВ ТА КОЛЕГ. ЦЯ КАРТА ДОПОМОЖЕ ВАМ ОТРИМАТИ БЕЗПЕЧНИЙ ДОСТУП ДО ІНФОРМАЦІЇ ТА ЗАХИСТИТЬ ВАШІ ДАНІ ПРИ ВИКОРИСТАННІ МОБІЛЬНИХ ТЕЛЕФОНІВ ТА ІНТЕРНЕТУ.

ШО ТАКЕ ЦИФРОВА БЕЗПЕКА ТА СЕКРЕТНІСТЬ?

Ось список ознак, після виявлення яких вам варто почати турбуватися про безпеку та конфіденційність інформації:

- Паролі, які дивним чином самі змінюються
- Приватні повідомлення, які раптово стають прочитаними у ваші скриньці ще кимось, окрім вас.
- Сайти, які раптом стали недоступними з території певних країн.
- Інші особи, які невідомо звідки дізнаються інформацію з особистого листування, включно з датами, іменами чи темою листування.
- Підозра прослуховування мобільного телефону.

ЧИ ЦЕ СТОСУЄТЬСЯ МЕНЕ?

Якщо такий розвиток подій може скомпрометувати ваш проект чи, можливо, поставить під ризик вас і ваших прихильників, тоді це вас точно стосується. Знання та програмне забезпечення, потрібне для здійснення таких атак на ваш приватний простір, зазвичай доступні в інтернеті. Якщо особа, яка хоче здійснити атаку, має вільний доступ до

інтернету чи мобільного телефону, то зробити задумане для неї легко. Державні установи, інтернет-провайдери та мобільні оператори мають привілейований доступ до такої інфраструктури, але офісні працівники, сусід та адміністратори інтернет-кафе також можуть отримати цей доступ..

ЯКІ ПИТАННЯ БЕЗПЕКИ РОЗГЛЯДАТИМУТЬСЯ У ЦІЙ КАРТІ?

У цій карті увагу приділено тим інструментам, які основані на інтернеті та мобільних телефонах. Однак, існує низка інших технологій, які також можуть зробити вас вразливим до цензури, спостереження чи переслідування. І хоча тут ми їх не обговорюємо, регулярне оновлення операційної системи вашого комп'ютера, надійне антивірусне програмне забезпечення, а також супутні процедури є найважливішими базовими засобами захисту. Якщо у вас є підозра, що ваш комп'ютер чи пристрій для зберігання інформації, включно з резервними копіями, можуть бути втрачені, вкрадені чи конфісковані, або ж ваша організація може потрапити в поле цільового стеження в інтернеті (або ж навіть якщо це загальнопоширена практика в регіоні, де ви проживаєте), тоді ви повинні звернутися до керівництва Security in-a-Box, Tactical Tech.

Інструменти захисту прав людини, основані на інтернеті

Використовуючи загальнодоступні інтернет-інструменти, зокрема Blogger, Facebook та Twitter для мобілізації чи координації, пам'ятайте, що інформація, яку ви зберігаєте на цих платформах, стає в певній мірі власністю провайдера чи адміністратора сервісу, і що більшість з цих сервісів насправді розкриває набагато більше інформації, аніж ви думаєте.

Якщо ви вирішили довірити делікатну інформацію з вашого проекту подібним інтернет-платформам - насамперед прочитайте їхні правила про конфіденційність інформації або ж договір з користувачем. Пам'ятайте, що навіть найкращі правила конфіденційності все одно залишають вашу інформацію під прямим контролем адміністратора платформи, який може без вашого на те відома оприлюднити, продати чи використати у своїх інтересах цю інформацію. Навіть якщо ви видалите свій профіль, більшість з таких сервісів насправді не витирають інформацію, яку ви розташували у цьому профілі чи особисту інформацію, яку ви надали при реєстрації. В результаті, якщо вам не принципово, яким сервісом користуватися, подумайте про деякі альтернативні ресурси, які більше поважають права людини: Blip.tv замість YouTube, riseup.net, а не Gmail. Якщо ви маєте достатньо ресурсів, то краще буде створити свої власні аналогічні сервіси й служби, основані на інтернеті.

Якщо ви все ж так користуєтеся комерційними платформами, зробіть усе можливе, щоб захистити себе від зловмисників, які знають, як переглянути приватну інформацію на таких ресурсах. Це, зокрема, стосується соціальних мереж, на зразок Facebook та MySpace. Розберіться детально в принципах зберігання приватної інформації на цих сервісах і після цього виділіть для себе ту інформацію, яку ви можете мимоволі оприлюднити про себе чи про вашу організацію; наприклад, ваше справжнє ім'я, місце проживання, місця подорожей, деталі запланованих подій та зустрічей. Якщо цю інформацію відслідковувати протягом тривалого часу, на її основі можна описати всі ваші звички, вашу роботу.

Однією з корисних фішок є можливість створення кількох профілів в будь-якому онлайн-сервісі, яким ви користуєтесь, що дозволить вам використовувати різні акаунти для різних проектів, а також оперувати тестовими акаунтами, які ви можете використовувати, щоб «шпигувати» за самим собою. Ваш особистий простір набагато краще захищений, якщо ви у стані перевірити, що саме можна дізнатися про ваш профіль, наприклад, через онлайн-пошук чи через профілі людей, які мають право особливого доступу.

ПАРОЛІ

Більшість інтернет-ресурсів залежать від звичайного паролю, який потрібен для захисту вашого акаунта. Якщо зловмисник чи ворожа структура дізнається цей пароль, не має значення ні довіра до адміністрації сервісу, ні ваші старанні тестування секретності профілю:

ви все одно втратите свою конфіденційність та анонімність.
Менш вядомыя спосабы ўзлому паролю: нехта можа інсталяваць на вашым кампутары шкодную праграму, якую вы выкарыстоўваеце для ўваходу на бяспечны сайт. Альбо нехта можа назіраць за вашым Інтэрнэт-злучэннем, калі вы ўваходзіце на небяспечны вэб-сайт.

Менш відомі методи викрадення паролю: хтось міг встановити антивірус на комп'ютер, який ви використовуєте для авторизації на безпечному сайті. Або ж хтось міг відстежити ваше інтернет-з'єднання під час авторизації на небезпечному сайті.

Щоб захиститися від першого типу атаки, використовуйте свій власний комп'ютер чи комп'ютер людини, якій ви довіряєте і переконайтесь, що його операційна система та антивірусне програмне забезпечення мають найсвіжіше оновлення. Щоб захистити себе від другого типу атаки - використовуйте безпечне з'єднання HTTPS, який пропонують більшість популярних поштових сервісів, соціальних мереж, блогів, відео-хостингів. Ви можете перевірити безпечність вашого з'єднання ввівши в поле адреси «https://» замість «http://». Проте все ще є багато інтернет-сервісів, які не використовують HTTPS для захисту всієї інформації, окрім паролю. В результаті, якщо хтось відслідковує ваше з'єднання протягом тривалого часу, він зможе дізнатися всю інформацію, яку ви завантажили на сайт. Найкращим захистом від цього є використання виключно тих інструментів, які мають HTTPS-захист на всіх сторінках.

ЯК ОБІЙТИ ЦЕНЗУРУ

Ви можете використовувати захищені проксі-сервери, інструменти для подолання цензури чи для підтримки анонімності в інтернеті, такі як Tor, для приховування персональної інформації від сайтів, які ви відвідуєте, чи для подолання інтернет-фільтрів. Ці інструменти корисні у випадку, коли вам потрібно отримати доступ до заблокованих сайтів; наприклад, для дослідження чи щоб завантажити оновлену інформацію на інтернет-платформи, такі як Facebook.

АНОНІМНІСТЬ ОНЛАЙН

Програмне забезпечення для підтримки анонімності, таке як Tor, корисне, коли ви не хочете розкривати свою особисту інформацію на сайтах, які відвідуєте. Tor перекидає ваші інтернет-з'єднання через послідовність випадкових добровільних комп'ютерів, щоб не дозволити навіть вашому інтернет-провайдеру чи спостерігачеві державного рівня знати, що ви робите в інтернеті. Однак не використовуйте Tor при передачі чи отриманні делікатної інформації з небезпечних сайтів. Якщо ви не з'єднані з сайтом через HTTPS, то один з добровільних комп'ютерів стає доступним для відстежування відповідно до того, як ви отримуєте інформацію з цього сайту. Tor доволі безпечний, проте він дещо зменшує швидкість вашого інтернет-з'єднання.

Мобільні телефони

Мобільні телефони використовуються правозахисниками у цілому світі. Але часто телефони зберігають велику кількість інформації, яку варто тримати засекреченою. Разом зі списком контактів, мобільний телефон може містити історію викликів, календарі, текстові повідомлення чи електронні листи.

Подумайте про ту інформацію, яку зберігаєте на своєму телефоні, адже телефон доволі легко можуть конфіскувати. Наприклад, вам, швидше за все, не потрібно зберігати всі ваші контакти у своєму мобільнику, якщо ви займаєтесь делікатною роботою, пов'язаною з правами людини. Вам варто видаляти інформацію з вашого телефону чи SIM-картки кожного разу, коли це можливо. Під час організації акцій чи мобілізації мережі добре користуватися анонімною, оплаченою SIM-карткою або ж періодично їх змінювати. Оскільки текстові повідомлення можна легко відслідкувати, вам варто утриматися від небезпечних ключових слів при відправленні повідомлень. Допоки телефон увімкнено, його можна використовувати для стеження за вашим місцем перебування. Люди, які відвідують небезпечний захід, повинні вимкнути свої телефони та вийняти батареї. Мобільні оператори мають доступ до списку всіх ваших дзвінків: кому, коли і де ви телефонували. Оператора можна

юридично зобов'язати передавати цю інформацію офіційним державним особам, крім того оператори можуть зберігати цю інформацію протягом декількох років.

ДІЇ: ВИЗНАЧЕННЯ РИЗИКУ ВАШІЙ КОНФІДЕНЦІЙНОСТІ

Використовуйте нижчезазначені питання для оцінки ризику вашій конфіденційності та обрання потрібних інструментів для зниження цих ризиків.

1. **Я маю справу з делікатною інформацією**. Важливо знати та розуміти, чи маєте ви справу з делікатною інформацію, яка може спокусити інших осіб. Чи залучені ви до діяльності, яку можна розцінити як делікатну чи яка дискредитує владу, правоохоронні органи, збройні сили чи приватні компанії? Якщо так, то ви можете піддати ризику себе чи інших, якщо не вжити хоча б якихось засобів безпеки.
2. **Я працюю з людьми, інформація про яких повинна зберігатися в таємниці**. Можливо, ми отримуєте особисту інформацію від людей, яких підтримуєте, наприклад, інформацію про домашнє насильство, примусову працю чи зґвалтування. Якщо люди надають вам інформацію, оприлюднення якої може завдати їм шкоди, ви повинні вжити заходів, щоб переконатися, що вона зберігатиметься в таємниці.
3. **Я інколи спілкуюсь онлайн з людьми, які мають справу з делікатною інформацією**. Навіть якщо ви відчуваєте, що особисто не ризикуєте своєю безпекою, ви можете спілкуватися онлайн з людьми, які перебувають в зоні ризику і вже самі можете стати мішенню для їхніх опонентів. Такі випадки можливі тоді, коли хтось захоче використати вас, щоб отримати особисту інформацію про інших.
4. **Я переглядаю чи завантажую контент, який можна розглядати як делікатний**. Можливо, ви ставити матеріали на сайтах з прав людини чи пересилаєте статті, спрямовані проти окремих груп людей, що не поважають права людини. Звичайний візит на небезпечний сайт в інтернеті може перетворити вас на мішень.

Інтернет-ресурси для безпеки та секретності

Щоб дізнатися більше та завантажити інструменти з безпеки:

1. Security in-a-box був створений Tactical Tech та Front Line для того, щоб відповідати потребам, які стосуються цифрової безпеки та секретності інформації правозахисників та адвокатів. http://security.ngoinabox.org/
2. Digital Security and Privacy for Human Rights Defenders, створений Front Line, надає корисну інформацію про оцінку та поведінку з різними типами цифрової небезпеки. http://bit.ly/1aCkSs (forntlinedefenders.org)
3. Mobiles in-a-box, створений Tactical Tech, відрізняється цілим розділом, який стосується безпеки та секретності мобільних телефонів. http://mobiles.tacticaltech.org/security
4. Anonymous Blogging with Wordpress & Tor. Global Voices створили цю інструкцію для підтримки правозахисників, які хочуть оприлюднювати правду та висловлюватися онлайн, але від цього можуть постраждати. http://advocacy.globalvoicesonline.org/projects/guide/
5. Залишайтесь анонімними та обходьте цензуру. Tor створений, щоб покращити вашу анонімність та анонімність ваших дій в інтернеті, а також може бути використаний для подолання фільтрів в інтернеті. Ви можете завантажити його на свій комп'ютер чи запускати з USB-носія. http://torproject.org/

TACTICAL TECHNOLOGY COLLECTIVE