Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- **Какво е социален инженеринг**
- **Разпознаване / Спиране на атаки чрез социален инженеринг**

Сигурност, когато сте на път

Преглед

Бихме искали да можете да се възползвате изцяло от технологиите по всяко време, включително когато пътувате. В този бюлетин искаме да обърнем внимание на това как можете да се свързвате към Интернет и да използвате устройствата си сигурно, когато сте на път.

Гост-редактор
Марк Уилямс е Архитектът по сигурността на компанията в BlueCross Blueshield в щата Тенеси. Той е също така и инструктор на SANS и Президент на клона на ISSA (Асоциация на ИТ сигурността) в Читануга. Той има много пътувания зад гърба си и разбира проблемите, които човек среща, докато разнася технологичните си играчки наоколо.

Предварителна проверка

Въпреки че мрежата ви у дома или на работа може да бъде сигурна, докато пътувате трябва да имате презумпцията, че към която и мрежа да се свържете, не можете да й имате доверие. Никога не знаете кой друг е свързан към нея и какво прави. Ето няколко прости стъпки, които могат да предпазят вас и данните ви доста добре преди да пътувате.

- Най-сигурната информация е информацията, която нямате. Определете каква част от информацията не ви е необходима на устройствата, които носите със себе си и изтрийте тази информация. Това може значително да намали щетите, ако устройството ви бъде изгубено, откраднато или отнето от митница или граничен контрол. Ако пътуването ви е свързано с работа, питайте супервайзора си дали организацията ви предоставя устройства, които се използват специално за работа, докато пътувате.
- Защитете мобилните устройства и/или лаптопа със сигурна парола. По този начин, ако те бъдат изгубени или откраднати, никой не може да получи достъп до информацията на тях. В допълнение, активирайте или инсталирайте пълно криптиране на диска на мобилните си устройства или лаптопи. За повечето мобилни устройства, това се активира автоматично, когато използвате ключ за екрана.
- Инсталирайте или активирайте софтуера на устройството си, за да можете да следите отдалечено къде е то, и дори и да изтриете всичко на него от разстояние, ако е било изгубено или откраднато.
- Актуализирайте устройствата, приложенията и антивирусния софтуер преди да тръгнете, за да сте сигурни, че имате последните версии. Много от атаките се базират на системи със стар софтуер.
- Направете пълно архивиране на всичките си устройства. По този начин, ако нещо се случи с тях, докато пътувате, все още имате оригиналните си данни на сигурно място.
- При международни пътувания, проверете при доставчика си на мобилни услуги на какъв план за услуги сте

Сигурност, когато сте на път

за телефона си. Често доставчиците на услуги имат много високи тарифи за международната употреба на данни, така че е вероятно да пожелаете да деактивирате възможностите на телефона си за предаване на клетъчни данни при международни пътувания или да купите местна предплатена SIM карта, за да я използвате на път в чужбина.

За да имате безопасно пътуване, подсигурете устройствата си преди да тръгнете, уверете се, че са физически обезопасени и ползвайте само криптирани онлайн услуги.

Изгубени / Откраднати устройства

При отпътуването започнете с осигуряването на физическата сигурност на устройствата си. Например, никога не оставяйте устройствата си в колата, където хората могат лесно да ги видят, тъй като престъпниците могат просто да счупят прозореца на колата ви и да грабнат всичко ценно, което видят. Въпреки че престъпността винаги е риск, според неотдавнашно проучване на Verizon е 100 пъти по-вероятно да изгубите устройство, отколкото да ви го откраднат. Това означава, че трябва да проверявате по два пъти дали устройствата ви са все още у вас, докато пътувате, особено на места като проверката за сигурност на летището, при напускане на такси или ресторант, при освобождаване на хотелска стая или преди слизане от самолета. Помнете да проверявате в джоба на гърба на седалката пред вас!

Wi-Fi достъп

Достъпът до Интернет, докато пътувате често означава използване на обществени точки за достъп, като онези, които се намират в хотел, местно кафене или на летището. Има два проблема с обществения Wi-Fi достъп: никога не можете да сте сигурни кой го настроил и никога не знаете кой е свързан към него. И в този смисъл този достъп трябва да се смята за несигурен. Всъщност, това е причината поради, която направихте всички стъпки, за да осигурите устройствата си преди да сте тръгнали. В допълнение, Wi-Fi достъпът използва радиовълни, което означава, че някой, който седи близо до вас може потенциално да прихване и следи тези комуникации. Затова, ако използвате обществен Wi-Fi достъп, трябва да сте сигурни, че цялата ви онлайн активност е криптирана. Например, когато сте онлайн през браузъра си, уверете се, че всички сайтове, които посещавате са криптирани. Можете да потвърдите това, като търсите „HTTPS://” и/или изображение на затворен катинар в полето за адрес или URL. В допълнение е възможно да имате нещо наречено VPN (Virtual Private Network /Виртуална Лична Мрежа/), която може да криптира цялата ви онлайн активност, когато бъде активирана. Тя може да ви бъде предоставена от работата ви или можете да си купите VPN за лична употреба. Ако сте загрижени, че няма Wi-Fi достъп на който

Сигурност, когато сте на път

можете да се доверите, обмислете тетъринг към смартфона. Предупреждение: както споменахме по-рано, това може да бъде скъпо при международни пътувания, така че първо проверете при доставчика си на услуги

Обществени ресурси

Не използвайте обществени компютри, като тези в лобитата на хотелите или в кибер кафенетата, за да влизате в каквито и да било акаунти и да получавате достъп до поверителна информация. Нямате представа кой е използвал този компютър преди вас и дали той не е заразил този компютър нарочно или по погрешка. Когато е възможно, използвайте устройства, които контролирате вие и на които имате доверие. В най-добрия случай обществените компютри са добри за публична информация, като проверка на времето или гледане на новини. Влизането в акаунти, като например вашия Google акаунт може да бъде покана за хакерите, които вероятно са на нащрек.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

Пароли:	https://securingthehuman.sans.org/ouch/2015#april2015
Архивиране:	https://securingthehuman.sans.org/ouch/2015#august2015
Зловреден софтуер:	https://securingthehuman.sans.org/ouch/2016#march2016
Криптиране:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH Архиви / Преводи:	https://securingthehuman.sans.org/ouch/archives

Редакторски колектив: Бил Уайман, Уолт Скривенс, Фил Хофман, Боб Рудис
Превод: Николай Дачев и Радослава Несторова

