OUCH! | октомври, 2017 г.

Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

Да помогнем на другите в сигурността

Преглед

Много от нас се чувстват комфортно с технологиите, което включва и това как да ги ползват безопасно и сигурно. Въпреки това, приятели или членове на семейството може да не се чувстват толкова комфортно в тази сфера. Всъщност те могат да се чувстват объркани, стреснати или дори уплашени от технологиите. Това ги прави много уязвими за днешните кибер атакуващи. Кибер сигурността не е задължително страшно нещо, всъщност е доста проста сама по себе си след като веднъж сте наясно с основните положения. Такива хора най-вероятно просто се нуждаят от лидер като вас, който да им помогне да разберат основните неща.

Гост-редактор

Ранди Марчани (Twitter: **@randymarchany**) е Главен директор по Информационна сигурност (CISO) във Virginia Tech и сертифициран инструктор на SANS Institute.

Пет лесни стъпки

Ето пет прости стъпки, които можете да предприемете, за да помогнете на другите да преодолеят тези страхове и безопасно да се възползват максимално от съвременните технологии. За повече информация по всяка от тези точки, вижте раздела Ресурси в края на този бюлетин.

1. **Социално инженерство**: Социалното инженерство е често срещана техника, използвана от кибер атакуващите за подвеждане или заблуждаване на хората, за да направят нещо, което не трябва да правят, като споделяне на своята парола, заразяването на компютъра си или споделяне на чувствителна информация. Това не е нищо ново, измами и измамници са съществували от хиляди години насам. Единствената разлика сега е, че злосторниците прилагат същите тези понятия в интернет. Можете да помогнете на другите като им обясните най-често срещаните признаци на атака от типа социално инженерство, като например, когато някой създава силно чувство за спешност, когато нещо е прекалено хубаво, за да е истина, или когато един кибер атакуващ се представя за някого, когото познавате, но посланията им не звучат като идващи от приятел. Споделяйте примери за често срещани атаки от типа социално инженерство, като например фишинг имейли или известните телефонни обаждания на Microsoft за техническа поддръжка. Ако не друго, се уверете, че членовете на семейството ви разбират, че никога не трябва да дават своята парола на никого или да позволяват отдалечен достъп до компютъра си.
2. **Паролите**: Силните пароли са ключови за защита както на устройствата, така и за всички онлайн акаунти. Научете членовете на вашето семейство как да създават силни пароли. Препоръчваме фрази за достъп, тъй като те са най-лесни и за изписване и за запомняне. Фразите за достъп са нищо повече от пароли, съставени от няколко думи. Освен това им помогнете да инсталират и използват мениджър на пароли. Важно е да има уникална парола

Да помогнем на другите в сигурността

за всяко един от вашите устройства и акаунти. Ако мениджъра на пароли в твърде сложен за употреба, научете ги поне да записват паролите си, а след това да ги съхраняват на сигурно място. И накрая, помогнете им да активират удостоверяването в две стъпки за най-важните пароли (често наричано двуфакторно удостоверяване). Удостоверяването в две стъпки е една от най-ефективните мерки, които можете да предприемете, за да се направите всяка сметка сигурна.

3. **Обновяване**: Поддържането на системите обновени и напълно в крак с времето е ключова стъпка, която всеки може да предприеме за сигурността на устройствата си. Това се отнася не само за вашите компютри и мобилни устройства, но и за всичко, свързано с Интернет, като игрови конзоли, термометри или дори светлини или високоговорители. Най-лесният начин да се гарантира, че всички устройства са актуални е да се даде възможност за автоматично актуализиране винаги, когато е възможно.
4. **Анти-вирусни програми**: Хората правят грешки, понякога кликваме върху нещо или инсталираме неща, които може би не трябва да имаме, и които могат да заразят нашите системи. Анти-вирусната програма е предназначена да ни предпази от тези грешки. Въпреки че анти-вирусната програма не може да спре всички злонамерени програми, тя помага да се открият и спрат най-често срещаните атаки. Постарайте се всеки домашен компютър да има инсталирана анти-вирусна програма, както и тя да е актуална и активна. Освен това, много от днешните анти-вирусни решения включват други технологии за сигурност, като защитни стени и защита на браузъра.
5. **Архивиране**: Когато всичко друго се провали, архивирането често е единственият начин, по който може да се възстанови информация загубена или поради грешка, като изтриване на погрешни файлове, или поради кибер-атака от типа „откуп“. Уверете се, че семейството и приятелите ви разполагат с автоматизирана система за архивиране на файлове. Често най-простите решения са базирани на облачна услуга, която архивира вашите устройства на всеки час или всеки път, когато направите промяна във файл. Тези решения улесняват не само архивирането на данните, но и възстановяването им.

Помагайте на другите безопасно да се възползват максимално от технологиите, като споделите с тях тези пет прости стъпки.

Сигурност на децата при пътувания

Ако се чувствате комфортно с технологиите, най-вероятно се грижите не само за собствената си сигурност, но и за тази на децата си. Въпреки това, когато децата посещават роднина, който не разбира много от технологии, като баба и дядо, тези приятели или роднини може да не знаят как да защитят най-добре децата онлайн и да не разбират вашите очаквания. Ето някои стъпки, които можете да предприемете, за да защитите децата, когато посещават други хора, особено от семейството:

Да помогнем на другите в сигурността

- **Правила**. Уверете се, че ако има някакви правила или очаквания, които имате за сигурността на децата, то другите знаят за тях. Например, има ли някакви правила за това колко дълго децата могат да бъдат онлайн, с кого могат да говорят или какви игри могат или не могат да играят? Повярвайте ни, не бива да очаквате от децата да обясняват какви са правилата на други членове на семейството. Една от идеите е да се създаде "списък с правила", който да споделяте с всички роднини на детето ви, които то посещава често.
- **Контрол**: Ако едно дете разбира от технологии по-добре от възрастните, то може да се възползва от това. Например, децата могат да поискат или да получат администраторски права за компютъра на баба и дядо, а след това да си правят каквото си искат, като например да инсталират тази игра, която вие не искате да им позволите да играят. Уверете се, че родниците разбират, че не трябва да дават на децата никакъв допълнителен достъп освен това, което е било установено.

И накрая, предложете на хората да се абонират за различни ресурси, като например този бюлетин - OUCH!, за да могат да продължат да учат сами. Този бюлетин се публикува всеки месец безплатно на над 20 езика. Регистрирайте се на адрес https://securingthehuman.sans.org/ouch.

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

Социално инженерство:	https://securingthehuman.sans.org/ouch/2017#january2017
Парола:	https://securingthehuman.sans.org/ouch/2017#april2017
Мениджър на пароли:	https://securingthehuman.sans.org/ouch/2017#september2017
Удостоверяване в две стъпки:	https://securingthehuman.sans.org/ouch/2015#september2015
Архивиране и възстановяване:	https://securingthehuman.sans.org/ouch/2017#august2017
Сигурността на днешните онлайн деца:	https://securingthehuman.sans.org/ouch/2017#may2017

Редакторски колектив: Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли
Превод: Николай Дачев и Радослава Несторова

