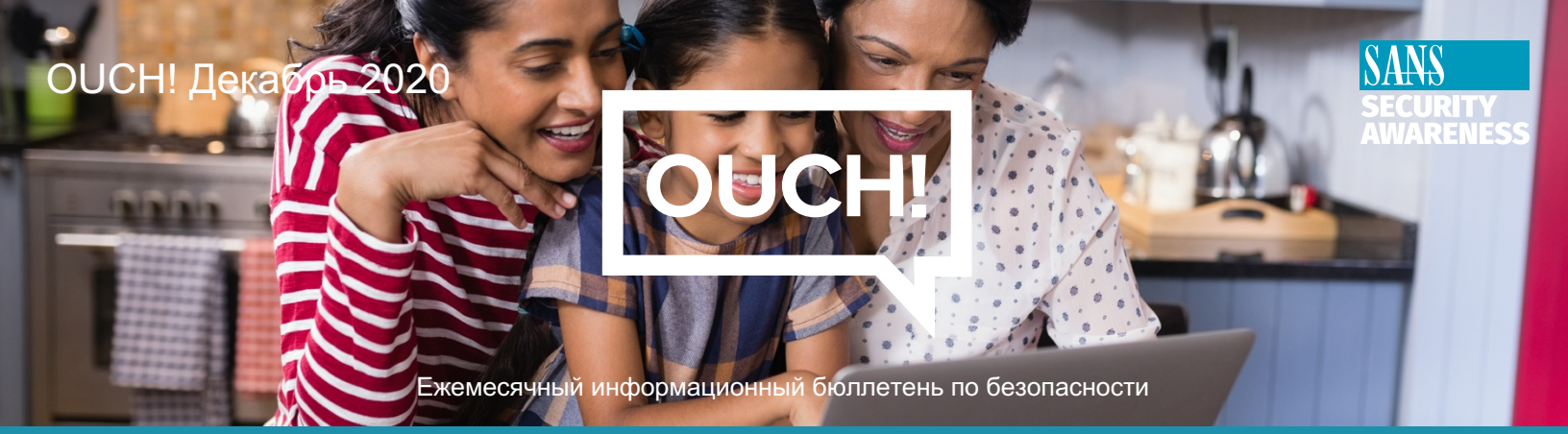
OUCH! Декабрь 2020



Ежемесячный информационный бюллетень по безопасности

Безопасность для разных поколений

Обзор

Попытки безопасно использовать современные технологии могут быть непосильными почти для нас всех, но особенно сложно для членов семьи, которые не привыкли к технологиям или не настолько знакомы с ними. Поэтому мы хотели поделиться некоторыми ключевыми шагами, которые помогут обезопасить членов семьи, которые могут испытывать трудности с технологиями и неправильно понимать риски, связанные с их использованием.

Сосредоточьтесь на основах

Часто лучший способ защитить других - это сделать безопасность как можно более простой для них. Сосредоточьтесь на минимальном количестве шагов, которые окажут наибольшее влияние.

1. **Социальная инженерия:** Атаки социальной инженерии - один из основных способов нападения на большинство из нас. Объясните что мошенники и аферисты действовали на протяжении тысячелетий, единственная разница сейчас в том, что плохие парни используют Интернет, чтобы нас обмануть. Приведите примеры, например, фишинговые электронные письма, выдаваемые за ваш банк или посылку, или мошенники, называющие себя службой технической поддержки или правительством. Убедитесь, что члены семьи понимают, что они никогда не должны никому сообщать свой пароль, кредитную карту, личную информацию или доступ к своему компьютеру. Напомните им, чем сильнее ощущение срочности, тем больше вероятность, что это атака. Некоторые преступники охотятся на наших близких, жаждущих любви, и притворяются их желанной мечтой. Наконец, убедитесь, что они знают, если они чувствуют себя некомфортно или у них есть вопросы по электронной почте или кому-то звонящему, что они в первую очередь позвонят вам.
2. **Домашняя сеть Wi-Fi:** Найдите время, чтобы убедиться, что их домашняя сеть Wi-Fi защищена паролем и что пароль администратора по умолчанию изменен. Вы также можете подумать о настройке сети Wi-Fi для использования безопасной формы DNS, такой как бесплатный https://www.opendns.com. Службы безопасного DNS не только помогают предотвратить посещение зараженных веб-сайтов, но и дают вам контроль над веб-сайтами, которые люди могут или не могут посещать, что может быть особенно ценно, если их посещают дети.
3. **Обновление:** выделите, что постоянное обновление систем, программного обеспечения и устройств значительно затрудняет их взлом злоумышленниками. Самый простой способ гарантировать это - включить автоматическое обновление там где это возможно. Если у вас

© SANS Institute 2020

есть устройство или система, которые настолько стары, что вы не можете их обновить, мы рекомендуем вам заменить их новым устройством, которое поддерживает обновление.

4. **Пароли:** сильные и надежные пароли являются ключом к защите как устройств, так и любых учетных записей в Интернете. Расскажите членам вашей семьи, как создавать длинные парольные фразы. Парольные фразы возможно могут быть самыми простыми для их использования и запоминания. Другой пример - установить менеджер паролей и научить им пользоваться. Это может позволить вашим близким пользоваться Интернетом простым и безопасным способом, достаточно запомнить только один пароль, чтобы разблокировать хранилище. В зависимости от решения вы можете даже виртуально управлять им. Если это не сработает, попросите их записать свои пароли в записной книжке, а затем хранить ее в удобном и безопасном месте. Для любых критически важных онлайн-аккаунтов, таких как их финансовые счета, вы также можете настроить двухэтапную проверку. Убедитесь, что у вас есть план для любых онлайн-аккаунтов, точно так же, как вы готовили бы завещание для физических активов.
5. **Резервные копии:** когда ничего не помогает, резервное копирование может спасти положение. Убедитесь, что у членов семьи есть простые и надежные резервные копии. Для многих подход на основе облака, чаще самый простой.

Если члены вашей семьи чувствуют себя подавленными, помогите им, сосредоточившись на основах, стараясь обеспечивать безопасность как можно проще. Кроме того, проявите терпение, дайте время и место для ошибок и помогите им не повторять их. Наконец, подумайте о том, чтобы они подписались на OUCH! информационный бюллетень.

Приглашенный редактор

Крис Дейл (Twitter @chrisadale) - главный консультант в River Security, европейской консалтинговой фирме по вопросам безопасности, и сертифицированный инструктор SANS (https://www.sans.org/profiles/chris-dale/).
Найдите Криса в LinkedIn здесь: https://www.linkedin.com/in/chrisad/

Ресурсы

Социальный инжиниринг: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Менеджеры паролей: https://www.sans.org/security-awareness-training/resources/password-managers-0
Обновление: https://www.sans.org/security-awareness-training/resources/power-updating
Резервные копии: https://www.sans.org/security-awareness-training/resources/got-backups
Цифровое наследование: https://www.sans.org/security-awareness-training/resources/digital-inheritance

Переведено для сообщества: Роман Поляков

OUCH! публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0 license. Вы можете поделиться или распространить этот бюллетень, если вы не продаете или не изменяете его. Редакция журнала: Уолт Скривенс, Фил Хоффман, Алан Ваггонер, Шерил Конли