Ежемесячный информационный бюллетень по безопасности

Весенняя чистка

Обзор

Большинство из нас с нетерпением ждут весны! Картина обретает форму, начинают расцветать цветы, и у многих возникает желание начать весеннюю чистку. Хотя может быть легко увидеть необходимость чистки и наведения порядка. Необходимость в цифровом виде чистке не так очевидна. Вот несколько простых советов, чтобы привести вашу цифровую жизнь в порядок и установить новые цифровые привычки:

РЕЗЕРВНОЕ КОПИРОВАНИЕ: Мы сперва привели этот шаг, потому что, это один из самых важных шагов, которые вы должны сделать, прежде чем переходить к другим. Независимо от того, насколько вы безопасны, в какой-то момент вам, скорее всего, понадобятся резервные копии для восстановления вашей важной информации. Причины могут включать отказ жесткого диска, потерю устройства и заражение вредоносными программами, такими как вымогатели. Создание и планирование автоматических резервных копий гарантирует, что вы сможете восстановить наиболее важную информацию.

УДАЛЕНИЕ: Удалите все неиспользуемые программы или приложения на ваших мобильных устройствах и компьютерах. Некоторым приложениям требуется большой объем памяти, они могут создавать новые уязвимости и даже замедлять работу. Чем меньше у вас приложений, тем выше безопасность вашей системы и информации. Многие устройства показывают, когда последний раз вы использовали приложение - если прошло более нескольких месяцев, скорее всего, вам это приложение ненужно!

ОБНОВЛЕНИЕ: Обновите все устройства и приложения, которые у вас есть, и включите автоматическое обновление, когда это возможно. Таким образом, ваши устройства и приложения остаются актуальными, не только гарантируя, что они будут работать быстрее, но и то, что их будет намного сложнее взломать.

ПАРОЛИ: Пересмотрите свои пароли. Если вы используете одни и те же пароли для нескольких учетных записей, измените их, чтобы у каждой учетной записи был свой уникальный пароль. Не можете запомнить все свои пароли? Подумайте об использовании менеджера паролей. Наконец, если это возможно, включите двухфакторную аутентификацию (2FA), особенно для любой электронной почты или финансовых счетов.

ФИНАНСОВЫЕ СЧЕТА: Убедитесь, что ваши банковские счета, пенсионные счета, а также кредитные карты настроены на оповещение о каждой транзакции, особенно при крупных покупках или денежных переводах. Чем раньше вы заметите мошенническую деятельность, тем раньше вы сможете ее остановить. В зависимости от того, в какой стране вы живете, замораживание кредита может быть одним из наиболее эффективных способов защиты вашей личности.

БРАУЗЕР: Просмотрите все дополнение и плагины, установленные в вашем браузере. Просмотрите настройки разрешений; действительно ли плагинам нужен доступ к вашему местоположению, паролям или спискам контактов? Если вы больше не используете определенные плагины или у вас есть проблемы с конфиденциальностью, удалите их.

СОЦИАЛЬНЫЕ МЕДИА: Проверьте свое присутствие в онлайне и контролируйте его. Проверьте настройки конфиденциальности и удалите все фотографии и видео, к которым больше нет доступа или которые вам не нужны. Вы также можете искать себя в поисковой системе и посмотреть, какая информация о вас там имеется. Помните, что нужно ограничивать объем информации, которой вы делитесь, даже с теми с кем вы решите ею поделиться.

СТОЛ: Очистите ящик стола, пересмотрите все старые жесткие диски и USB-накопители, возможно даже уничтожьте все заметки со слишком большим количеством информации. Подумайте, если у вас его ещё нет, об инвестировании в уничтожитель документов.

Электронная почта: выполните очистку файла электронной почты, удалите то, что вам не нужно, и организуйте то, с чем вы работаете. Обратите особое внимание на любые конфиденциальные документы, которые имеют вашу дату рождения или номер социального страхования и уберите их из своего электронного ящика!

Хотя это может показаться сложной задачей, будьте уверены, ваши устройства и информация будут более защищены. Если вам кажется, что это очень сложно сделать все сразу, рассмотрите возможность выбора нескольких пунктов или попробуйте наметить одну задачу в день или неделю. Помните, каждый маленький шаг защищитит вас.

Приглашенный редактор

Кэти Никелс *(@LiketheCoins) - главный аналитик разведки в Red Canary, а также инструктор SANS для FOR578: анализ киберугроз. Более десяти лет она занималась защитой сетей, реагированием на инциденты и разведкой киберугроз.*

Ресурсы

Резервные копии:	http://www.sans.org/u/ZVr
Простые пароли:	http://www.sans.org/u/ZVw
Поиск себя в онлайне:	http://www.sans.org/u/ZVB
Утилизация ваших мобильных устройств:	http://www.sans.org/u/ZVG