

OUCH!

Ежемесячный информационный бюллетень по безопасности

Цифровое Наследование

Обзор

Вы когда-нибудь задумывались над таким неудобным вопросом: «Что происходит с нашими цифровыми данными, когда мы становимся недееспособными или умираем?» Многие из нас имеют или знают, что у нас должен быть список или воля того, что должны знать близкие в случае нашей кончины. Но как насчет всех наших цифровых данных и онлайн-аккаунтов? Должны ли мы рассмотреть тип цифровой воли? Должны ли мы создать план «Цифрового наследства»?

Задумайтесь о своем цифровом присутствии! Банковские и пенсионные счета, ипотека, семейные фотографии и видео, учетные записи умных домов, электронная почта и социальные сети - вот лишь некоторые из множества примеров, которые составляют наш цифровой след. В случае вашей смерти или смерти близкого члена семьи, семья и близкие могут нуждаться в быстром доступе к этим учетным записям или данным. Кроме того, устаревшие данные и оставленные в сети учетные записи могут со временем стать уязвимыми для хакеров, что может подвергнуть риску семью и друзей.

Создание плана

Хорошая идея, обсудить ваши желания с вашей семьей или друзьями, которым вы доверяете, как и другие детали вашей воли. Помимо этих разговоров, проведите инвентаризацию и документируйте свои цифровые активы и онлайн-аккаунты. Если вы не предоставите членам семьи доступа к своим учетным записям, после вашей смерти им может быть очень трудно получить к ним доступ или закрыть их. Например, хотите ли вы, чтобы члены вашей семьи были заблокированы к доступу семейных фотографий и видео, которые вы хранили в Интернете?

Одной из идей является использование в сети менеджера паролей. Это программа, которая надежно хранит все ваши логины и пароли, кредитные карты и другую конфиденциальную информацию. Менеджер паролей разработан для того, чтобы значительно упростить создание, хранение и доступ к паролям и вопросам безопасности. Во многих отношениях это мощный инструмент для хранения вашего цифрового присутствия. С помощью менеджера паролей вы можете настроить их для совместного использования всех или определенных паролей с другими доверенными членами семьи. Если вам это неудобно, документируйте доступ к своему менеджеру паролей и запечатайте его в

конверте, а затем передайте его доверительному лицу или члену семьи чтобы они смогли его открыть после вашей смерти. Таким образом, они получают доступ к вашему менеджеру паролей и смогут получить доступ к вашим учетным записям и информации, хранящейся там.

Кроме того, некоторые сайты предоставляют возможность идентифицировать устаревшие или доверенные контакты. Например, Facebook позволяет участникам заранее определить, хотели бы они, чтобы их учетная запись была удалена или сохранена в памяти после их смерти. Мемориализация создает пространство, которое видно только существующим друзьям, где можно поделиться воспоминаниями. Наконец, вы можете рассмотреть возможность работы с адвокатом или специалистом по недвижимости, который специализируется на цифровом наследовании.

Наследование цифровых активов

Вы можете оказаться в ситуации, когда вам нужно восстановить или получить доступ к онлайн-счетам недавно умершего друга или члена семьи. Мы рекомендуем вам сначала согласоваться с адвокатом и другими членами семьи, прежде чем предпринимать какие-либо действия. Другие члены семьи могут расстроиться, если увидят, что вы принимаете меры, не посоветовавшись с ними в первую очередь. Затем идентифицируйте любые пароли, которые вы можете найти. Член семьи записал или хранил их где-нибудь? Если это не вариант, можете ли вы получить доступ к компьютерам или мобильным устройствам, которые они использовали и все еще находятся в системе? Если нет, вам, скорее всего, придется обратиться к каждому сайту для доступа к учетной записи умершего участника. Это часто включает в себя предоставление свидетельства о смерти и доказательств того, что вы непосредственно связаны с членом семьи. В некоторых случаях вы не сможете получить доступ к учетной записи или данным, хранящимся в учетной записи, а только их удалите. Каждый сайт обрабатывает эти ситуации по-разному, что может занять много времени.

В сегодняшнем цифровом мире мы должны учитывать не только физические активы, но и цифровые активы при планировании будущего.

Приглашенный редактор

Шерил Конли - эксперт в области фишинга и осведомленности, чей опыт включает помощь в создании и управлении фишинг-программой в Lockheed Martin. В настоящее время она поддерживает команду SANS Security Awareness и имеет сертификат SSAP (SANS Security Awareness Professional).



Ресурсы

Менеджер паролей: <http://www.sans.org/u/Y5Y>

Создание простых паролей: <http://www.sans.org/u/Y63>

OUCH! публикуется SANS Security Awareness и распространяется под лицензией [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). 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