Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Что следует копировать и когда
- Как делать резервные копии
- Восстановление
- Ключевые моменты

Резервное копирование и восстановление данных

Обзор

Рано или поздно, при неудачном стечение обстоятельств, вы можете потерять личные файлы, документы или фото. Примеры могут быть разные: случайное удаление файлов, сбой системы, потеря ноутбука или заражение компьютера. В этих случаях возможно восстановление данных только из резервной копии. В этом выпуске мы поговорим о резервном копировании, как это правильно делать и для чего.

Об авторе

Хизер Махалик – известный эксперт в сфере расследования киберпреступлений. Она специализируется на безопасности смартфонов. Хизер является соавтором книги Practical Mobile Forensics, техническим редактором книги Learning Android Forensics и соавтором курсов Института SANS FOR585 Advanced Smartphone Forensics и FOR518 Macintosh Forensics. Она ведёт сайт **Smarterforensics.com** и Twitter: **@heathermahalik**.

Что следует копировать и когда

Резервные копии – это копии вашей информации для хранения отдельно от оригинала информации. Если вы потеряете важную информацию, вы сможете её восстановить из этой копии. Проблема заключается в том, что большинство людей не делает резервных копий, несмотря на то, что это просто и доступно. Вот два подхода к решению проблемы, что именно копировать: (1) конкретные данные, которые важны для вас; или (2) абсолютно всё, включая операционную систему. Первый подход наиболее простой, позволяет экономить пространство на жёстком диске, но второй подход тоже довольно простой, но более эффективный. Если вы не уверены, что следует копировать, советуем копировать абсолютно всё.

Затем, вам нужно решить, как часто делать резервное копирование. Широко используется подход, при котором резервные копии делаются каждый час, ежедневно, раз в неделю и т.д. Для домашнего пользования есть специальные программы, например, Apple's Time Machine, Microsoft's Windows Backup или Restore, позволяющие настраивать автоматическое, так называемое «установи и забудь», расписание резервного копирования. Эти программы делают резервные копии автоматически, даже когда вы на работе или вдали от компьютера. Есть и другой подход, так называемая «непрерывная защита», которая делает копии всех новых или изменённых файлов при их закрытии. Мы рекомендуем делать резервное копирование каждый день. В конечном счете, следует задать себе вопрос: «как много информации я могу себе позволить потерять, если я должен восстановить резервную копию?»

Как делать резервные копии

Есть два способа хранения резервных копий: на физических носителях или на «облаке». Физические носители – это любой тип устройств, например, DVD диски, USB носители или съемные жесткие диски. Какой бы тип носителя вы не выбрали, никогда не храните копии на том же устройстве, где хранятся оригиналы. Недостаток физических

Резервное копирование и восстановление данных

носителей в том, что в случае бедствия (пожара или кражи) вы потеряете не только само устройство, но и резервные копии вместе с ним. Поэтому вы должны выбрать безопасное место для хранения копий вне дома или офиса. Не забудьте пометить дату и содержание устройства или диска. Для дополнительной безопасности используйте шифрование данных.

автоматическое, регулярное резервное копирование может стать единственной возможностью сохранения ваших данных.

Облачное хранение данных заключается в том, что ваша информация хранится в Интернете. Условия хранения зависят от объёма информации: в некоторых случаях услуги могут быть платными. Вам следует установить на компьютер программу, которая будет делать резервные копии автоматически. Преимущества этого решения в том, что в случае несчастья с вашим домом, копии будут в безопасности. Кроме того, вы можете получить доступ к копии или даже отдельным файлам из любого места, например, путешествия. Недостаток данного решения заключается в том, что восстановление данных из резервных копий происходит намного медленней, особенно при больших объёмах информации. Если вы не можете выбрать наиболее подходящее решение (физические носители или «облако»), используйте оба.

Наконец, мобильные устройства. Их преимущества в том, что большинство данных уже хранится на «облаке», например, ваша электронная почта, события в календаре или контакты. Однако, не вся информация может попасть на «облако», например, настройки приложений, последние фото или настройки системы. Создание резервных копий мобильных устройств не только предотвратит потерю данных, но и облегчит восстановление системы при покупке нового устройства. iPhone/iPad автоматически отправляют данные на iCloud компании Apple. Возможности устройств на базе Android и других устройств зависят от производителя или провайдера услуг. В некоторых случаях вам придется приобрести мобильное приложение, которое будет делать резервные копии автоматически.

Восстановление

Создание резервных копий – это только полдела; вы должны быть уверены, что сможете восстановить систему из них. Рекомендуем ежемесячно проверять, насколько копия рабочая путем восстановления файлов и их содержимого. Кроме того, перед серьёзной модернизацией (например, переходом на новое устройство), или капитальным ремонтом (например, заменой старого жёсткого диска), убедитесь, что сделали полную копию системы и она рабочая.

Резервное копирование и восстановление данных

Ключевые моменты

- Автоматизируйте, по возможности, резервное копирование и регулярно его проверяйте.
- При восстановлении системы из копии, убедитесь, что переустановили последние программы безопасности и обновили их перед использованием системы.
- Устаревшие или неиспользуемые копии следует уничтожить для предотвращения несанкционированного использования.
- Если вы храните данные на «Облаке», ознакомьтесь с правилами поставщика услуг и его репутацией, чтобы убедиться в правильности выбора. Узнайте, шифруются ли данные при хранении? Кто имеет к ним доступ? Использует ли провайдер надёжную аутентификацию, например, двухступенчатую верификацию?

Общественные ресурсы

Не пользуйтесь общественными компьютерами, например, в лобби отелей, библиотеках или интернет-кафе. Вы же не знаете, кто пользовался этим компьютером до вас, компьютеры могут быть заражены вирусами случайно или специально. По возможности, используйте только свое устройство для соединения с Интернетом.
Если возникнет необходимость воспользоваться публичным компьютером, то постарайтесь не пользоваться сервисами, требующими вводить логин и пароль.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Ресурсы

Паролевые фразы: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_ru.pdf

Двухступенчатая верификация: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_ru.pdf

Правила безопасной работы с «облаком»: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_ru.pdf

Шифрование: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_ru.pdf

Ежедневные советы по информационной безопасности: SANS: Security Awareness Tip

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова


securingthehuman.org/blog


/securethehuman


@securethehuman


securingthehuman.org/gplus