Лаборатория Касперского о приватности данных

Распространение смартфонов, появление социальных сетей и других интернет-сервисов открыло для людей новые возможности: общаться с близкими и друзьями на большом расстоянии, делать покупки не выходя из дома, быстро распространять и получать информацию. В то же время этим пользуются и злоумышленники. Персональная и личная информация, попавшая в Сеть, все чаще используется против её владельцев в форме шантажа, буллинга и мошенничества. Овладение основами цифровой грамотности и знание правил информационной безопасности является неотъемлемой частью жизни современного человека, а умение защитить свою приватность— важный навык 21 века.

Определения

●Информационная безопасность—это процесс обеспечения конфиденциальности, целостности и доступности информации.

●Приватность в Интернете—это право человека на сохранение в секрете своей персональной информации.

●Персональная информация—это та информация, по которой можно определить, кто вы.

●Овершеринг—стремление человека рассказывать окружающим больше, чем стоило бы, заходя слишком далеко с откровенностью и забывая о приватности.

●Цифровой след—вся информация, которая остается о человеке в Интернете.

●Конфиденциальность—доступ к информации имеют только определенные лица.

Приватность данных

Чтобы разобраться, как персональная информация может стать общедоступной, нужно понять, как информация попадает в Интернет. Есть несколько вариантов:

●Заполняем анкету при регистрации на ненадежном сайте.

●Участвуем в сомнительных онлайн-опросах, конкурсах, викторинах.

●Оплачиваем покупки в Сети на фишинговом сайте.

●Публикуем посты или сториз в социальных сетях, где рассказываем что-то о себе, отправляем данные в чатах, мессенджерах.

●Выкладываем фотографии, на которые случайно попадает персональная информация, например, табличка с названием улицы и номером дома. Но это не единственные способы. Перечисленные выше варианты, касаются конкретных действий самого пользователя, но важно понимать, что влиять на приватность может то, что мы не контролируем напрямую, например:

●Публикации других людей о нас. Например, друзья размещают совместную с вами фотографию без разрешения.

●История наших поисковых запросов и посещенных сайтов. Ее обычно собирают поисковые системы, чтобы предложить вам более подходящую рекламу.

●А также установка и использование сомнительных приложений. Например, приложению «Фонарик» нужен доступ только ко вспышке, но если такое приложение просит доступ к контактам и сообщениям, это повод задуматься. Под видом благонадежного приложения, может на самом деле оказаться зловредное программное обеспечение или рекламный софт.

Правила информационной безопасности, которые помогут сохранить приватность:

●Когда регистрируетесь на сайтах, определите, что можно рассказать о себе, а что нет.

●В социальных сетях используйте «Настройки приватности». Ограничьте доступ незнакомых людей к вашей странице.

●Если хотите поделиться какой-то персональной информацией, ограничивайте ее в зависимости от ситуации.

●Не сообщайте персональную информацию незнакомым людям. Мошенники могут маскироваться под знакомых ваших родителей, дальних родственников или сотрудников банка, писать вам в соцсетях или даже позвонить.

●Пользуйтесь защитными решениями определителями номеров, а также VPN, когда подключаетесь к неизвестным общественным Wi-Fi сетям.

●Не переходите по подозрительным ссылкам в социальных сетях, почте или мессенджерах, даже если их прислали знакомые.

●Когда устанавливаете приложения на смартфон, не давайте им доступ к тем функциям, которые им не нужны. Например, приложению «Фонарик» явно не нужен доступ к вашим фотографиям или камере.
●Скачивайте приложения и программы только из официальных магазинов приложений.
●Выходите из ваших аккаунтов после работы за школьными компьютерами или чужими устройствами.
●Если хотите разместить фотографию со своим другом, не забудьте уточнить у него, разрешает он вам это сделать или нет. Тоже самое просите делать и по отношению к вам.
●Используйте двух факторную авторизацию—это способ защитить свой аккаунт от несанкционированного доступа, даже в том случае, если ваш логин и пароль знают злоумышленники. Обычно это выглядит так: первый рубеж—это логин и пароль, второй — специальный код, приходящий по SMS, в push-уведомлении или электронной почте. Также давайте вспомним правила, которые касаются паролей. Пароль—это одна из важнейших составляющих вашей приватности. Чтобы пароль был сложным для взлома, нужно придерживаться следующих правил:
●Если связка логин/пароль «утекла», то как можно скорее поменяйте пароль. Как это узнать? Есть специальные сайты для проверки утечек учетных записей. Обращайте внимание на новости о том, в каких сервисах произошли утечки.
●Меняйте пароль регулярно.
●Пароль должен быть надежным: иметь минимум 12 символов, а также содержать прописные и строчные буквы, цифры, специальные символы.
●В пароле не должно быть общедоступной или личной информации, например, имени вашего питомца или номера телефона.
●Используйте разные уникальные пароли для разных сайтов.
●Не храните пароли на листочках, в текстовых файлах на компьютере. Для этого лучше использовать специальные программы — менеджеры паролей. Если вам интересно узнать больше, про то, как защитить свою приватность в Интернете, заходите в блог «Лаборатории Касперского»(www.kaspersky.ru/blog/и www.kids.kaspersky.ru), там вы найдете много полезных материалов на эту тему. Также в блоге рассказывается про новые виды мошеннических схем и приложения для кражи персональных данных.

Профессии в области информационной безопасности

Консультант по безопасности личного профиля
Проводит проверку активностей и данных клиента в Сети на предмет уязвимостей и помогает обеспечить конфиденциальность и общую безопасность. В том числе помогает настроить приватность профиля в социальных сетях, отредактировать или удалить лишнюю информацию.
Исследователь мобильных угроз
Анализирует работу мобильных приложений и операционных систем в смартфонах и планшетах. Помогает распознать вредоносные программы, которые могут маскироваться под мобильные игры и другие приложения.
Веб-контент аналитик
Изучает сайты и сервисы с точки зрения возможности кражи персональной и платежной информации пользователя. Анализирует и раскрывает мошеннические схемы (мошенничество, фишинг, спам). Помогает улучшить информационную безопасность для банков, интернет-магазинов и многих других компаний.
Эксперт по кибербезопасности
Разрабатывает правила информационной безопасности для частных лиц и компаний. Анализирует возможные киберугрозы и помогает с ними бороться, участвует в совершенствовании защитных решений.