Как защитить персональные данные в интернете

Наказ не разговаривать с незнакомцами на улице и в транспорте мы даем детям задолго до того, как начнем отпускать их от себя. А вот просветить их относительно интернет-опасностей почему-то не торопимся. Но общение в мессенджерах и соцсетях, переписка в электронной почте и оплата покупок онлайн сегодня начинаются рано, в младшей и средней школе. Поэтому родителям предстоит объяснить ребенку, какую информацию о себе нельзя выкладывать в сеть и передавать неизвестным людям. Впрочем, для взрослых эти правила тоже актуальны.

Почему персональные данные важны

Мы живем в смешанном мире, где реальность во многом дополняется виртуальной средой. И чем младше человек, тем более естественна для него эта смешанная среда. В интернете дети и подростки знакомятся, общаются и играют; у них есть друзья, с которыми они никогда не встречались в реале, — да это им и не нужно. Часто таким людям доверяют даже больше, чем близким.

На своих страницах в соцсетях многие дети сообщают о себе больше, чем стоило бы: домашний адрес, номер телефона, номер школы и класса, дату рождения и другие персональные данные.

Персональные данные или личная информация — номер паспорта, номер телефона (ребенка или родственников), ИНН, СНИЛС, домашний адрес, дата рождения, пароли, ПИН- и CVV-коды от банковских карт — желанная добыча для интернет-мошенников. Именно эти сведения чаще всего становятся целью их атак, технологических и психологических.

К чувствительной личной информации также можно отнести фотографии дорогих вещей, документов (дипломов, виз, паспортов), даже статусы в соцсетях — например, о том, что вы всей семьей отправляетесь в путешествие. Для нечестных людей геотеги в инстаграме, селфи на фоне дома, школы или работы — прямые подсказки, где можно найти членов семьи, какие ценные вещи есть в доме и когда там наверняка никого нет.

Схемы хищения личной информации

Изобретательность мошенников растет, методы работы постоянно совершенствуются, но в целом используются одни и те же принципы. Перечислим основные (но далеко не все) способы перехватить персональные данные.

Фишинговые сообщения

Это письма от мошенников, представляющихся банками и другими официальными организациями. Цель таких писем — заставить вас ввести пароль от интернет-банкинга или данные карты в поддельную форму. Злоумышленники запрашивают конфиденциальные данные для подтверждения учетной записи или активации почтового ящика. В результате ваша личная информация оказывается у них. Для того чтобы не стать жертвой таких мошенников, старайтесь не пересылать чувствительную информацию по электронной почте, особенно незнакомым людям.

Поддельные сайты

Подменяя адрес сайта, мошенники незаметно перенаправляют пользователей на поддельные страницы.

Пытаясь зайти на популярный сайт по присланной ссылке, пользователь попадает на сайт-подделку, очень похожий на оригинал. Данные учетной записи, введенные на таком сайте, оказываются у злоумышленников.

Фишинговые страницы могут иметь адрес, очень похожий на настоящий. Чтобы распознать сайт-подделку, обратите внимание на адрес в поисковой строке — он будет хотя бы немного отличаться от официального. В адресной строке слева от адреса вы не найдете значка безопасного соединения (в большинстве браузеров это щит или запертый замок), а размещенные на поддельной странице ссылки, скорее всего, будут нерабочими — кроме той, что призвана выудить ваши данные.

Прежде чем вводить логин и пароль на сайте, убедитесь, что в адресной строке браузера указан верный адрес. Закройте страницу, если в браузере появляется сообщение о переходе на подозрительный сайт. В большинство браузеров встроены реестры для отслеживания мошеннических сайтов.

Телефонное мошенничество

Телефонные мошенники звонят или рассылают SMS от имени банка или платежной системы с просьбой предоставить номер карты или перевести деньги на указанный номер. Причины могут быть разными: истекший срок действия пароля, блокировка карты, крупный выигрыш или даже авария с участием близкого человека.

Они могут попросить перейти по ссылке для восстановления доступа к аккаунту, отправить SMS или позвонить по конкретному номеру. Цель таких сообщений — списать деньги за отправку ответного SMS, подписать на платные услуги или перекинуть на фишинговый сайт, а затем заставить ввести пароль и данные карты.

Если вы получили подозрительное сообщение, звонок или письмо, связанные с финансовыми операциями, позвоните по официальному номеру банка и проверьте информацию.

Как защитить свои данные

Чтобы защитить персональные данные своей семьи, для начала поговорите о том, какие сведения о себе нельзя размещать в интернете, а какие — можно, но только на сайтах, которым есть основания доверять. Старайтесь соблюдать правило: «Если сомневаюсь, можно ли доверить информацию о себе этому сайту, то не буду этого делать».

Договоритесь, о каких событиях в личной жизни и жизни семьи не стоит писать в интернете, и объясните детям, почему.

Например, расскажите ребенку, что даже если он размещает деликатную информацию о себе в закрытом посте «только для друзей», ее могут использовать против него интернет-тролли — после ссоры с другом или если аккаунт кого-то из друзей будет взломан.

Одна из самых популярных сетей среди детей и подростков — YouTube. Научитесь устанавливать безопасный режим на всех устройствах (его нужно устанавливать в каждом браузере отдельно) и не забывайте о настройках конфиденциальности.

Защитить конфиденциальность в Сети поможет понимание принципов работы файлов cookie. Это временные файлы, которые сохраняются в браузере и помогают сайту запоминать информацию о вас: логин и пароль, на каком языке вы просматриваете информацию, ваши интересы и предпочтения. На первый взгляд они не опасны, но в некоторых случаях могут причинить вред пользователям.

Вот еще несколько рекомендаций, которые относятся и к взрослым, и к подросткам.

- Не оставляйте незаблокированными телефоны и компьютеры, не выбрасывайте бумаги и носители данных (жесткие диски, флеш-карты, SIM-карты), на которых хранятся пароли.
- Если компьютером пользуются несколько человек, используйте разные профили операционной системы для разных пользователей.
- Не храните в электронной почте и не выкладывайте в открытый доступ копии паспорта и других документов: если мошенники взломают вашу почту, они смогут воспользоваться личными данными.

Перед работой на чужом компьютере войдите в приватный режим. Если такой возможности нет, очистите кэш и cookie после завершения работы.

- Регулярно проверяйте антивирусом съемные диски, флеш-карты и прочие носители информации, которые вы подключаете к чужим компьютерам.
- Не вводите личную информацию в подозрительные формы, особенно в электронных письмах.
- Не открывайте вложения и не переходите по ссылкам из почты или мессенджеров от сомнительных адресатов. Если адресат кажется вам подозрительным, внесите его в черный список.
- Прежде чем совершать покупки онлайн, проверяйте отзывы и рейтинги магазинов, аккаунты продавцов и условия оплаты; оплачивайте покупки только через известные платежные сервисы и системы — такие платежи надежно защищены.

- По возможности выбирайте сайты с протоколом https, а не http: вероятность взлома последних гораздо выше, чем сайтов https.
- Подключите двухфакторную аутентификацию для всех своих аккаунтов. Так вы максимально надежно защитите свои данные.

Источник:

Благотворительный фонд Сбербанка «Вклад в будущее»
Игорь Александров