Наш дом – смартфон

Сегодня для многих из нас смарфон стал лучшим товарищем, которому мы доверяем все свои секреты. Но время от времени проскальзывает мысль о том, что девайс о нас слишком много знает. Что будет, если он попадёт не в те руки? Как сохранить приватность, «СверхНовой Эре» рассказал доцент кафедры периодической печати и сетевых изданий департамента «Факультет журналистики» УрФУ *Владимир ВОЛКОМОРОВ*.

– Сейчас много говорят о том, что хранить важную информацию в смартфоне небезопасно. Насколько это необходимо?

– Уровень паранойи должен быть здравым. Давайте разумно относиться к своему устройству. Представьте себе комнату. Можно помыть с антисептиком стены, окна, двери – всё будет стерильно, как в больнице. Но зачем это нужно? Здесь так же. Можно пользоваться только зашифрованной почтой, удалить учётные записи из соцсетей, отключить GPS, вытаскивать батарею, когда приходите домой. Вряд ли вы это будете делать. Просто предугадывайте развитие сценариев, по которым вы можете потерять личные данные, совершайте простой набор действий – и всё будет в порядке.

– Что это за меры?

– Стоит создать хотя бы минимальное ограничение доступа к содержимому телефона. Они бывают разные: графический ключ, специальный код, разблокировка по отпечатку пальца. У iPhone эта функция стоит по умолчанию, в других моделях её нужно включать. Многие пренебрегают этой мерой. Конечно, зачем каждый раз набирать пароль, если можно просто провести пальцем по экрану. Но если его не будет, любой человек, который найдёт смартфон, сможет получить доступ к вашим данным. С любопытными одноклассниками это средство, кстати, также отлично справляется. Только помните, что пароль должен быть не «12345», от такой комбинации толку ноль.

Не советую также копить большое количество фотографий на устройстве. Мало того, что они занимают место, так ещё могут рассказать о вас лишнее, особенно, если вы любите снимать яркие моменты своей жизни. Любой, кто возьмёт ваш телефон в руки, может узнать, куда вы ездили, с кем общались, что есть у вас дома.

– Неужели этого достаточно?

– В принципе, да. Но если вы хотите ещё больше обезопасить себя, то можете использовать двухфакторную аутентификацию. Это приложения, которые запрашивают от вас дополнительную информацию. Они бесплатны. Например, этот способ по умолчанию используют банковские программы, они дополнительно запрашивают у вас авторизацию через СМС. С помощью аутентификации вы можете защищать отдельные приложения, например, социальные сети.

Главный антивирус – в голове человека. Если вы моете руки и не едите грязные фрукты, вряд ли у вас будет дизентерия

– С человеческим любопытством всё понятно. А как распознать вредные программы, которые могут за нами «подглядывать»?

– Доверяйте крупным разработчикам, смотрите на количество скачиваний. **Если программу установили, например, пятьсот миллионов человек, то, скорее всего, ей можно доверять.** Когда вы скачиваете приложение, вы даёте ему разрешение на те или иные действия. Оно запрашивает у вас, что ему нужно: доступ к камере, вызовам, чтению СМС. Если обычный фоторедактор предъявляет большой список требований, стоит задуматься, нужно ли пользоваться этим приложением.

Думайте, устанавливая ту или иную программу, действительно ли она вам необходима. Иногда приложение просто засоряет память телефона, а после удаления не до конца «вычищает» за собой данные. Для того чтобы стереть всю информацию о программе, нужно зайти в файловый браузер, и папки, которые не удаляются, просто убрать вручную. Так же можно почистить кэш. Некоторые думают: «У меня памяти на смартфоне 128 гигабайт, места много – не жалко». Не храните на телефоне программы, которыми не пользуетесь. Относитесь к устройству, как к своему дому: периодически там надо прибирать, выкидывать мусор.

– На компьютерах обычно всегда ставят антивирусы. Телефонам они нужны?

«Мне нужен ваш лайк». Рисунок Анастасии Колясниковой

– Главный антивирус – в голове человека. Если вы моете руки и не едите грязные фрукты, вряд ли у вас будет дизентерия. То же самое и здесь. Не открывайте ссылки и файлы от неизвестных отправителей, и всё будет хорошо. Честно говоря, я не пользуюсь антивирусами на своём устройстве. Во-первых, они тормозят аппарат: если у вас не мощный девайс, производительность упадёт. Во-вторых, подобные программы постоянно предлагают какие-то новые услуги, что очень раздражает. Но **у антивирусов есть возможности, о которых мы не задумываемся – функции на случай утери или кражи телефона.** Например, удаление данных или возможность сфотографировать вора.

– Кроме вирусов, есть ещё одна опасность – утечка данных через социальные сети. Как этого избежать?

– Многие думают: «Зачем кому-то мой аккаунт?» Действительно, если вы не политик, не общественный деятель, это, скорее всего, никому не интересно. Обычно странички в сетях воруют для того, чтобы продать на чёрном рынке для каких-нибудь целей. Поэтому придумать сложный пароль и не хранить важные данные на своих страницах всё-таки стоит.

Юлия ШАМРО,
20 лет, Факультет журналистики УрФУ