

Девять из десяти россиян дорожат своими персональными данными, но ничего не предпринимают для их защиты

Москва, Россия, 19 октября 2017 — Компания Avast, лидер в области цифровых продуктов для безопасности бизнеса и потребителей, провела опрос более 1400 россиян, чтобы выяснить, насколько они ценят и как защищают свои персональные данные, опубликованные в социальных сетях.

У большинства из нас есть много аккаунтов в различных социальных сетях; сами того не осознавая, мы распространяем нашу личную информацию по всему миру. Поэтому мы захотели проанализировать не только отношение людей к тем данным, которые они выкладывают на страницах в своих аккаунтах, но и также узнать, какие средства они используют для их защиты.

Электронная почта — самая важная учетная запись, но учетные записи в онлайн-магазинах ценятся ещё больше

Результаты показывают, что электронная почта по-прежнему наиболее используемый онлайн-сервис в России, именно она представляет наибольшую ценность для большей части россиян. Второе место занимают соцсети (VKontakte и Facebook) — 89,4% россиян заявляют, что ценят свои персональные данные в онлайн-сетях.

Перечь наиболее популярных для взлома онлайн-сервисов:

- 43,7% Amazon
- 42,3% Dropbox (или другой облачный сервис)
- 41,7% Snapchat
- 31,4% Электронная почта
- 30,8% LinkedIn
- 29,8% WhatsApp (или другая служба обмена сообщениями)
- 25,2% Facebook
- 23,2% Twitter

Данные, представляющие для вас наибольшую ценность, наиболее часто могут подвергаться захвату

Хотя большинство из нас считает, что информация, хранящаяся в учётных записях, находится под надёжной защитой, взломщики готовы с этим не согласиться. Хакеры получают такую информацию об учетной записи, как имена пользователей, пароли и данные их кредитных карт и впоследствии продают эти данные в сети Darknet за 2 доллара или менее, в зависимости от обменного курса биткойна. И происходит это потому, что пользователи неосторожно обращались со своей личной информацией и она попала в руки к злоумышленникам.

Учитывая тот факт, что утечка информации происходила даже с таких крупных сервисов, как Yahoo и LinkedIn, не удивительно, что две трети россиян (66,6%) сомневаются в том, что их личная информация надёжно защищена.

Почти четверть (22,2%) респондентов заявила, что им приходилось сталкиваться с захватом персональных данных, и еще у троих из десяти россиян возникают сомнения в неприкосновенности их личной информации.

Необходимо предпринимать новые меры по защите персональных данных

Более трети (35,4%) россиян ни разу не меняли пароль после того, как узнавали о взломе. 81,2% же лишь изменили пароль для взломанного сайта, но не для других сайтов. Это наводит на тревожные мысли, поскольку хакеры часто используют учетные данные, полученные в результате нарушений безопасности, для доступа к другим учетным записям, если они защищены тем же паролем. Базы данных с украденной информацией часто появляются спустя несколько лет после того, как произошло нарушение, и продаются уже другим киберпреступникам для пользования. Вот почему крайне важно регулярно менять пароли и не ждать обнаружения утечки данных.

Проверенные сервисы сохраняют пароли своих клиентов в кэше, что означает появление зашифрованных версий паролей в утерянных базах данных. Это хороший способ защиты, однако, как пользователи, мы несем ответственность за обеспечение безопасности наших учетных записей и данных, которые мы храним там. Если пароль достаточно простой и, например, содержит только буквы, несколько символов и никаких специальных символов или цифр, хакеры могут легко его вычислить; существует даже список наиболее легко угадываемых хакерами паролей.

Менеджер паролей — это полезный инструмент, который можно использовать для создания надежных и уникальных паролей для всех ваших учетных записей, которые вы впоследствии сможете легко изменить. К сожалению, только 4,7% респондентов используют подобное приложение для защиты своих учетных записей.

Ежедневно мы публикуем огромное количество личной информации в интернете. И хотя для мошенников наши данные не представляют такую большую ценность, как для нас, это не означает, что пользователи не должны обеспечивать безопасность своей личной информации. Вы можете думать, что вам нечего скрывать или, может быть, вы не возражаете против того, чтобы кто-то читал ваши личные сообщения, но как бы вы себя чувствовали, если бы эта информация была использована, чтобы шантажировать вас? Собрав достаточное количество информации, хакеры получают возможность украсть ваши личные данные или деньги с ваших онлайн-счетов. Они могут заблокировать ваш аккаунт, удалить информацию из учетной записи или даже общаться с другими людьми, используя ваше имя.

О компании Avast:

Avast (<http://www.avast.com>) — мировой лидер в области решений цифровой безопасности, которые защищают более 400 миллионов интернет-пользователей. Компания предлагает продукты под брендами Avast и AVG, которые обеспечивают пользователей качественной антивирусной защитой от всех типов интернет-угроз и опасностей растущего Интернета вещей. Сеть обнаружения угроз Avast является одной из самых совершенных в мире и использует технологии машинного обучения и искусственного интеллекта для обнаружения и предотвращения угроз в режиме реального времени. Продукты Avast для мобильных устройств, ПК и Mac удостоены сертификатов VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs и др. Avast поддерживают лидирующие глобальные частные инвестиционные компании CVC Capital Partners и Summit Partners.