Цифровой ликбез: как обезопасить себя от киберугроз

Издание: Газета.ru, 21 ноября 2018 г.

Спикер: Михаил Савельев, директор по развитию бизнеса «Информзащиты»

Под цифровой грамотностью подразумеваются знания и умения, позволяющие пользоваться передовыми технологиями: от способности найти кнопку включения компьютера до обнаружения в интернете любимой песни. Цифровая гигиена — набор правил безопасного поведения в цифровом пространстве. Как общаться в соцсетях и не навредить себе излишней откровенностью, не стать жертвой мошенников или чересчур предприимчивых коммерсантов — все это цифровая гигиена, составная часть цифровой грамотности, без которой сейчас не обойтись.

Страна непуганых россиян

Россияне, как показал недавний опрос ВЦИОМ, пока не склонны воспринимать киберугрозы всерьез. Например, почти две трети россиян (62%) пользуются социальными сетями с той или иной периодичностью, при этом почти половина опрошенных (47%) размещала в соцсетях какую-либо информацию о себе за последний год. Но вот дальше россияне проявляют неожиданную беспечность: каждый второй (52%) заявил, что использование персональных данных третьими лицами ничем им не угрожает.

Подобная позиция — заблуждение, причем заблуждение опасное. И распрощаться с ним нужно как можно скорее.

«Самый важный аспект цифровой гигиены — осознать, что любые данные о вас имеют ценность, причем это не зависит от вашего социального статуса или материального положения.

Аргумент «я никому не интересен/мне нечего скрывать» в современном мире не работает. Личные данные, данные, размещенные в соцсетях, информация о вашей активности в интернете — все это представляет интерес как для тех, кто занимается рекламой или кредитным скорингом, так и для мошенников.

Например, чем больше данных о вас у них есть, тем более успешную мошенническую схему можно организовать», — рассказал «Газете.Ru» веб-аналитик «Лаборатории Касперского» Владислав Тушканов.

Беспечность россиян хорошо иллюстрирует скандал вокруг столичных МФЦ. Компьютеры общего доступа в центрах «Мои документы» оказались настоящим кладезем персональных данных россиян — там журналисты нашли сканы паспортов и СНИЛС, анкеты с номерами мобильных телефонов, банковскими реквизитами и другими сведениями. Оказалось, что россияне, успешно загрузив сканы своих документов на портал госуслуг или отправив анкету сотрудникам МФЦ, редко вспоминают о необходимости удалить их с чужих компьютеров. А ведь какой-то ушлый мошенник может загрузить данные на флешку и оформить, например, микрозайм.

В подобной ситуации нередко оказываются и известные люди, хотя уж для них-то необходимость следить за сохранностью персональных данных должна быть очевидна.

После задержания футболиста Павла Мамаева его супруга Алана пожаловалась в Instagram на шантажиста, требующего у нее деньги за полученные в результате взлома данные. Девушка отказалась платить, и в результате интимные кадры Мамаевых появились 28 октября во взломанном аккаунте актрисы Марии Горбань. Фото и видео провисели там недолго, сменившись рекламой хакерских услуг по взлому телефонов «звезд, любимых, врагов».

И этим «врагом» или просто жертвой хакеров может оказаться любой из нас. Например, в Коми в прошлом году мошенники взломали страничку местного жителя и скачали фотографии, которые ему пересылала девушка. Думала — фото только в личке, но нет! Результат — шантаж. Вроде бы всего 10 тыс. рублей, но размах может быть любой.

И интимом тут не ограничится — жертва может вполне заплатить пару тысяч рублей, чтобы фривольные фото не попали на глаза начальнику (например, директору школы) или даже маме.

Основа безопасности

Ситуация с цифровой грамотностью тоже далеко не безоблачная, причем не только в России, но и в других странах мира. Например, многие компании пытаются бороться с безразличием, с которым люди подписывают разнообразные пользовательские соглашения, даже не читая их. Внутри этих тоскливых документов, написанных мелким шрифтом, часто прячут возмутительные требования, которые никто не замечает. В 2010 году британский интернет-магазин GameStation разместил в своем пользовательском соглашении пункт, согласно которому люди обязались отдать коммерсантам «свою бессмертную душу и отказаться от любых претензий на нее». Продать душу согласились 7,5 тыс. пользователей или 88% от общего числа покупателей.

Осенью 2015 года в рамках исследования, проводимого Европолом, пользователям бесплатного Wi-Fi в центре Лондона предлагалось пожертвовать за эту услугу своего первенца. И люди легко нажимали «ОК», не замечая подвоха.

Но не все так плохо — общественная организация РОЦИТ, ежегодно вычисляющая индекс цифровой грамотности, зафиксировала положительную динамику в области накопления знаний россиян. По ее данным, к концу 2017 года этот показатель в целом вырос на 5,7% и достиг 5,99 пт. по десятибалльной шкале, с разбросом от 4,17 до 6,41 пт. между федеральными округами.

Приемы самообороны

Если с обретением цифровой грамотности все более-менее ясно, к тому же и ситуация в этом вопросе обстоит неплохо, то заботы о цифровой гигиене пока мало трогают россиян. «Газета.Ru» поинтересовалась у экспертов, о каких мерах безопасности должен знать любой пользователь современной техники и интернета, чтобы нежданно-негаданно не обнаружить свои персональные данные там, где их быть не должно.

Руководитель группы исследований безопасности банковских систем Positive Technologies Ярослав Бабин отмечает, что сейчас самыми простыми инструментами в арсенале мошенников являются звонки и SMS — по данным компании, во II квартале 2018 года в 25% всех зафиксированных атак злоумышленники использовали именно эти средства. В результате банальное невнимание людей помогло преступникам выведать у них ценную информацию.

«Чтобы защититься от такого рода мошенничества, мы рекомендуем пользователям обращать внимание на номер, с которого пришло SMS или поступил звонок. Если это номер обыкновенного сотового телефона — скорее всего, это мошенники. Однако злоумышленники могут подделать номер отправителя. Поэтому необходимо проверять достоверность контактов через другие источники, например, позвонив по номеру банка, который всегда есть на сайте или обратной стороне пластиковой карты. Также мы советуем не переходить по ссылкам из SMS-сообщений от незнакомцев. Они могут содержать вредоносное ПО, с помощью которого злоумышленники могут заразить гаджет жертвы и похитить ее личные данные», — говорит Бабин.

Многие компании давно осознали важность цифровой гигиены и пытаются делиться своими знаниями не только с сотрудниками, но и с клиентами. «Уже существуют федеральные проекты, которые подсказывают, как не попадаться на удочки мошенников в сети. Например, крупные банки создают подобные видео и публикуют на своих сайтах. Также есть компании, где вводится должность «цифровой куратор». И это, на мой взгляд, правильно», — делится мнением директор по развитию компании «Информзащита» Михаил Савельев.

Веб-аналитик «Лаборатории Касперского» Владислав Тушканов подчеркивает, что необходимо быть более бдительными и при пользовании социальными сетями.

«Для начала можно просмотреть ваши страницы в соцсетях и очистить их от персональных данных, которые могут быть использованы злоумышленниками — адреса, номера телефонов, имена и возраст детей и родителей, информацию о дорогих покупках и так далее.

Еще можно зайти в настройки приватности соцсети — изучите их и сделайте так, чтобы только ваши друзья имели доступ к вашим данным», — советует эксперт.

Все специалисты в области информационной безопасности сходятся в одном — в повышении уровня цифровой гигиены россиян ключевую роль играет информирование, причем речь идет и об уроках в школе в рамках стандартного курса ОБЖ, и о программах и статьях в федеральных СМИ для старшего поколения. «Важно, что основная задача состоит не в том, чтобы пугать людей, а в том, чтобы на примерах действительно происходящих инцидентов демонстрировать им реальные угрозы и одновременно с этим тут же давать практические рекомендации, как не стать жертвой таких злонамеренных активностей», — подчеркивает технический директор Qrator Labs Артем Гавриченков.

Подробнее: http://clc.am/zzg9KA