**Правила личной финансовой безопасности**

Редко сейчас можно найти человека, которому не пришлось общаться с мошенником хотя бы по телефону: с лжесотрудником банка, «представителем компетентных органов о родственнике, попавшем в беду» и т.п. Однако кого-то просто заваливают звонками и спамом с «выгодными» предложениями, а кто-то почти не получает странных звонков. Об «утечке» баз персональных данных и правилах цифровой безопасности рассказывает Ольга Дайнеко, эксперт Центра финансовой грамотности НИФИ Минфина России.

**Как «утекают» личные данные**

Сейчас практически невозможно обезопасить себя от «утечки данных» о себе и связано это не только с кражей данных пользователей у компаний (служб доставки, мед.лабораторий и т.п.), но и потому, что о многом личном мы делимся добровольно. Порой, мы даже не замечаем, как часто и кому передаем персональные/личные данные: оплатили покупку в интернете, скачали новую игру на телефон, заключили договор, заполнили анкету для участия в розыгрыше призов или получения дисконтной карты, а также самостоятельно сообщаем подробности о себе через соцсети.

К сожалению, сегодня практически невозможно не попасть в списки к таким-либо аферистам – информацию о человеке в большинстве случаев можно найти в открытом доступе, а мошенникам сделать выводы об его предполагаемом имущественном положении, семье, отдыхе, заработке и многом другом. Мы все живем в цифровой среде и не можем находиться в абсолютном информационном вакууме. Так почему же одних мошенники атакуют чаще, а других – только по редкому случаю.

**Что интересует мошенников?**

Прежде всего потому, что базы персональных данных – это товар, стоимость которого определяется его полнотой. Мошеннику интереснее приобретать не только базу номеров телефонов с ФИО, но и иметь своеобразный «скоринговый балл» потенциальной жертвы-иметь дополнительные сведения не только в виде документов (паспорта и места жительства, например), но и оценочную характеристику внушаемости и доверчивости человека, индивидуальные маркеры для психологической манипуляции конкретным человеком. Просто база (слитая или похищенная) из миллионов «строк» мобильного оператора, службы доставки, маркетплейча и т.п. стоит недорого-ее отработка потребует от мошенников значительных трудовременных затрат. Самая важная часть-это то, что нельзя найти в сети (личностные характеристики человека).

Если к звонкам, смс и электронным письмам с запросами (в том числе-электронно) люди стали относиться более настороженно при любом упоминании данных банковского счета в запросе, то на разного рода «социологические опросы», «исследования потребителей» готовы общаться охотнее. Использование методов социальной инженерии позволяет мошенникам и собирателям данных получить эти сведения из простой беседы (или онлайн-опроса) и сделать предварительные выводы о психологическом портрете человека и его «привлекательности» для дальнейшего обмана. Чем больше в базе перспективных жертв, тем дороже она стоит, над чем и трудится немалая армия таких «собирателей». Базы кочуют и корректируются.

В сфере мошенничества (в том числе и цифрового) именно человек намного более уязвим, нежели любая программа или система. Выявленные уязвимости человека могут быть использованы не раз в разных мошеннических сценариях, поэтому некоторые люди попадают на удочку мошенника не раз. «Старые грабли» не всегда видятся старыми: для этого могут использоваться различные тактики, направленные на эмоции, слабости или иные особенности личности: сочувствие и жалость, жадность и желание быстро получить желаемое, страх (например, за ребенка, родственника), неопытность и доверчивость, лень и многое другое. Если банковскую карту, удостоверение личности, внешность можно поменять, то особенности личности меняются с меньшей легкостью.

Зная эти особенности потенциальной жертвы, мошенник, используя опыт «коллег», может просчитать, как именно войти в доверие во время общения, как ввести в заблуждение.

**Базовые правила**

А вот реже всего атакуют (а порой и вовсе перестают) тех, кто абсолютно бесперспективен: не отвечает вовсе, нарочито ассоциален, не идет на контакт, грубит/троллит, говорит односложно и категорично. Но не все готовы грубить или троллить, поэтому можно просто прервать разговор и внести абонента в черный список блокировки, поскольку чем меньше человек идет на контакт, тем реже его будут беспокоить.

Помимо правил цифровой безопасности (не передавать банковские данные, не переходить по сторонним ссылкам, не загружать программы/игры из непроверенных источников и т.п), важно помнить о безопасности социальной: не делиться личным с посторонними, не предоставлять дополнительную информацию о себе или близких без прямой необходимости (в том числе, под видом соцопросов). Передавая свои персональные данные, нужно оценивать целесообразность их передачи/обработки организацией, а предавать только в том объеме, который необходим для оказания услуги, а после-отзывать такие разрешения.