Приёмы мошенничества, направленные на получение доступа к персональным данным

Мы все сталкиваемся с тем, что в различных организациях, при оформлении или покупке билетов, с нас требуют документы и мы не задумываясь даем свои персональные данные. И каково же бывает наше недоумение и возмущение, когда оказывается, что на наш паспорт оформлен кредит, или микрозайм или другое, то, о чем мы даже не подозреваем.

Для начала давайте поймем, кто в принципе имеет доступ к вашим персональными данными (кроме полиции и прочих государственных органов):

контактам, информации паспорта…

Сотрудники банка. Разумеется, когда вы открывали счет, вы заполняли анкету (или сотрудник банка заполнял ее за вас). Может быть, открывали депозит или брали кредит в другом банке и уже забыли о нем, но данные все равно остались в базе.

Сотрудники почты. По доброй российской традиции при получении посылки или заказного письма нужно было заполнять «квиточек». К счастью, эту традицию недавно упразднили.

Сотрудники компании-оператора. Сюда мы включили и сотовых операторов, и интернет-провайдеров.

Сотрудники страховой компании. Ни один полис без предъявления паспорта вам не оформят.

Сотрудники частной клиники. Медицинское обслуживание — дело серьезное, и при заключении договора на оказание услуг тоже нужен паспорт.

Работники отдела кадров вашей компании. Им тоже ваши данные положено знать «по долгу службы».

Персонал отдела размещения гостиниц. Заселяясь в очередной отель, вы всегда предъявляете документы.

Как видите, огромное количество людей может получить доступ даже к вашим паспортным данным — тем более, если у них есть какие-то корыстные планы. Что уж говорить о банальных адресах электронной почту и телефонных номерах.

Гораздо более ценны ФИО и номера телефонов — номера часто запрашивают на сайтах для авторизации, но некоторые пользователи не раздумывая вводят и свои реальные фамилии с именами. Тот же «комплект» может быть скопирован, например, из адресной книги компании.

Утечка базы данных сотрудников с телефонами и электронными адресами может быть использована для проникновения в информационные системы компании или же дальнейшего персонального мошенничества, так как позволяет обратиться к человеку персонифицировано, войти с ним в контакт, заставить открыть заражённую ссылку или же получить другую ценную информацию.

«Фишинг».

Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на "сайт-двойник" такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы. Достаточно распространенным является предложение о работе за границей, уведомление о выигрыше в лотереи, а также сообщения о получении наследства.

Как защитить свои данные от использования?

Прежде всего, воспитать в себе культуру безопасного обращения с сайтами и организациями. Для начала старайтесь следовать этим трем простым советам.
Регистрируясь в онлайн-магазине, вовсе не обязательно делиться своими реальными именем и фамилией — их проверять никто не будет.
Постарайтесь также не держать в открытом доступе (например, в облачном хранилище) сканы и ксерокопии личных документов.
Установите пароль или другой способ идентификации на своем смартфоне. Незащищенный смартфон — это просто кладезь полезной для преступников информации.

Отдел по вопросам законности,
правопорядка и безопасности
администрации Невского района
Санкт-Петербурга