Методические рекомендации по профилактике мошенничества с использованием методов социальной инженерии

Социальная инженерия (social engineering) или «атака на человека» – совокупность психологических и социологических приемов, методов и технологий, которые позволяют получить конфиденциальную информацию.

Основной целью социальной инженерии является получение доступа к конфиденциальной информации, персональным данным, данным карточек, паролям, банковским данным и другим защищенным системам с последующим осуществлением мошеннических операций. Обезопасить себя от мошенничества с применением социальной инженерии можно, соблюдая простые меры безопасности и проявляя разумную бдительность.

Самые распространенные мошеннические схемы.

1. Взлом

Злоумышленники взламывают страницы в социальных сетях и рассылают от имени владельца аккаунта фишинговые сообщения с просьбой от имени владельца странички занять или перевести некоторую сумму либо с целью выманивания реквизитов банковских платежных карточек, а также паролей для проведения в дальнейшем мошеннических операций.

Способы защиты:

при обращении родственников/друзей/знакомых через социальные сети с просьбами о помощи в переводе денежных средств на карточку/оплаты мобильной связи, билетов и т.д. убедитесь, что лицо, обратившееся через страницу социальной сети, является именно тем, за кого себя выдает;

наряду с номером и сроком действия карточки, логином и паролем от интернет-банкинга, паролем 3-D Secure и SMS-паролем (ключом), также не следует сообщать CVV2/CVC2-код (трехзначное число на обороте карточке), данный код используется исключительно для расходных операций и абсолютно не нужен для перевода денежных средств на Вашу карточку.

в случае, если Ваш аккаунт в социальных сетях был взломан, по возможности оповестите об этом подписчиков Вашей страницы и смените пароль.

2. Вишинг

Злоумышленники используют телефонные звонки с целью выманивания у держателей банковских платежных карточек личной информации, номера карточки, логина и пароля от систем дистанционного банковского обслуживания, SMS-кодов и другого. Мошенники могут представляться работниками банка или Службы сервиса клиентов ОАО «Банковский процессинговый центр», использовать скрытые телефонные номера или программы-анонимайзеры, подменяющие номера телефонов на реальные номера, размещенные на официальных ресурсах организаций.

Способы защиты:

важно помнить, что при звонке работники банков или Службы сервиса клиентов никогда не запрашивают информацию о полном номере банковской платежной карточки, сроке действия, CVC/CVV коде, пароле 3D Secure, одноразовых подтверждающих кодах. Ни под каким предлогом не сообщайте информацию о реквизитах банковской карточки, логинах и паролях, SMS-кодах, сеансовых ключах к Интернет-банкингу и мобильным приложениям!

в случае возникновения звонков с просьбами уточнить Ваши данные незамедлительно обратитесь в банк по номерам телефонов, указанным на официальном сайте.

3. Мошенничество при осуществлении сделок на интернет-площадках

Добросовестный продавец размещает информацию о продаже товара на общедоступной площадке. Чаще всего внимание мошенников привлекают объявления о продаже дорогостоящего имущества (бытовая техника, мебель, автомобили). Мошенники под видом покупателей связываются с продавцом и просят предоставить им реквизиты банковской платежной карточки для осуществления предоплаты либо сами предоставляют мошенническую ссылку для перевода денежных средств.

Используя полученную информацию (зачастую держатели карточек разглашают не только номер карты, но и CVV2/CVC2-код, а также пароли 3D Secure) злоумышленники переводят деньги с карточки жертвы на свои карточки (телефонные счета, электронные кошельки и пр.).

Добросовестный покупатель обращается к продавцу (мошеннику под видом продавца) по вопросу приобретения того или иного товара, после чего мошенники просят произвести предоплату путем перевода средств с карточки на карточку или электронный кошелек. Получив деньги, продавец перестает выходить на связь.

Способы защиты:

при покупке товаров и услуг у незнакомых людей или на интернет-площадках необходимо обращать внимание на форму оплаты, если с Вас требуют предоплату (частичную или полную), то есть основания предполагать, что Вы имеете дело с мошенником;

не следуйте просьбам перевести оплату за предоставляемые по привлекательной цене товар или услугу на банковскую пластиковую карточку продавца или его электронный кошелек. Если Вы это сделаете, то Вы не сможете доказать, что произвели оплату за несуществующий товар или сервис.

4. Сообщения о выигрыше ценных призов

Злоумышленники рассылают сообщения о выигрыше ценных призов и провоцируют потенциальную жертву перевести на счет некую сумму денег для получения «приза» или участия в розыгрыше и объясняют это тем, что ему

нужно оплатить комиссию, таможенную пошлину, налоги либо транспортные расходы для доставки «выигрыша».

Способы защиты:

если Вы решили испытать удачу и связаться с организаторами розыгрыша, постарайтесь получить от них максимально возможную информацию об акции, условиях участия в ней и правилах ее проведения;

помните, что упоминание Вашего имени на интернет-сайте не является подтверждением добропорядочности организаторов акции и гарантией выигрыша. Необходимо задуматься над тем, принимали ли Вы участие в розыгрыше призов, знакома ли Вам организация, направившая уведомление о выигрыше, откуда организаторам акции известны ваши контактные данные? Если Вы не можете ответить хотя бы на один из этих вопросов, рекомендуем Вам проигнорировать поступившее сообщение;

любая просьба перевести денежные средства для получения выигрыша должна насторожить Вас;

помните, что выигрыш в лотерею влечет за собой налоговые обязательства, но порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или электронные кошельки.

Необходимо помнить, что для того чтобы противодействовать необдуманным решениям, минимизировать большую часть рисков, связанных с мошенничеством с применением социальной инженерии нужно выработать привычку брать паузу для анализа ситуации и недопущения перевода денежных средств или выполнения других выгодных злоумышленнику действий.