В рамках профилактики преступлений, совершаемых с использованием методов социальной инженерии, необходимо постоянно повышать уровень киберкультуры как одного из важнейших элементов противодействия хищению персональных данных и денежных средств.

Эффективным инструментом повышения уровня киберкультуры противодействия хищениям денежных средств является информирование о новых способах мошенничеств и правилах «финансовой безопасности».

К наиболее распространенным видам дистанционного мошенничества относятся:

– **«фишинг» –** вид дистанционного мошенничества, при совершении которого злоумышленники (в ходе телефонного разговора, посредством направления электронного письма или смс-сообщения) получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств. Жертвами указанного вида мошенничества зачастую становятся незащищенные, малообразованные, доверчивые слои населения.

Представляясь зачастую сотрудниками кредитных организаций, преступники вводят в заблуждение граждан относительно совершаемых несанкционированных списаний денежных средств, осуществляемых покупках, после чего просят назвать конфиденциальные сведения с целью пресечения возможного совершения преступления. Граждане, доверяя полученной информации, желая обезопасить свои денежные средства от преступных посягательств, сообщают запрашиваемую информацию, в результате чего злоумышленники похищают принадлежащие им денежные средства.

«Фарминг» – процедура скрытого направления на ложный IP-адрес, то есть направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг (ozon.ru, avito.ru, aliexpress.ru, joom, biglion, купинатор, кассир.ру, билетер, сайты по продаже билетов на ж/д и авиатранспорт).

«**Двойная транзакция»** (при оплате товаров и услуг продавец сообщает об ошибке и предлагает повторить операцию, а в дальнейшем денежные средства списываются дважды по каждой из проведенных операций).

«Траппинг» (манипуляции с картридером банкоматов, позволяющие либо не возвращать карту владельцу, либо списывать все данные карты для дальнейшего их использования).

Основные схемы телефонного мошенничества

1. Обман по телефону

Мошенник звонит с незнакомого номера и представляется родственником (знакомым) и взволнованным голосом сообщает, что задержан сотрудниками правоохранительных органов и обвиняется в совершении того или иного преступления (это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство). Далее в разговор вступает якобы сотрудник правоохранительных органов, который уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует перевести на определенный расчетный

счет или передать какому-либо человеку. В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам, но нередко человек, которому звонит мошенник, сам случайно подсказывает имя того, кому нужна помощь.

Аналогичным образом могут звонить мошенники сотрудникам государственных органов, либо предпринимателям и, представляясь, например, руководителем какого-либо государственного органа (правоохранительного, надзорного, контролирующего), под предлогом приезда комиссии проверяющих и требуют организовать либо «теплый прием» в форме бесплатного предоставления услуг (питание, подарки, организация отдыха и т. д.), либо перечислить определенную сумму денежных средств на указанный расчетный счет для организации досуга проверяющих или достижения необходимых положительных результатов проверки.

КАК ПОСТУПИТЬ В ТАКОЙ СИТУАЦИИ

Прервать разговор и перезвонить тому, о ком идет речь (либо в указанный государственный орган). Если телефон отключен, нужно связаться с его коллегами, друзьями и родственниками для уточнения информации.

2. SMS-просьба о помощи

SMS-сообщения позволяют упростить схему обмана по телефону. Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие. На SMS-сообщения с незнакомых номеров реагировать нельзя. Это могут быть мошенники.

3. Телефонный номер-грабитель

На телефон приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь – и оказывается, что с Вашего счета списаны крупные суммы. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок. Единственный способ обезопасить себя от телефонных мошенников – не звонить по незнакомым номерам.

4. Телефонные вирусы

Очень часто используется форма мошенничества с использование телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке…». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств. Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после

перевода денег на фальшивый счет они снимаются с телефона. Не следует звонить по номеру, с которого отправлено SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

5. Выигрыш в лотерее или какого-либо приза

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют это для своей деятельности и обмана людей. На Ваш мобильный телефон, как правило, в ночное время – приходит SMS-сообщения, в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль. Чаще всего, упоминаются известные иностранные модели, марки. Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из вышеуказанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного денежную сумму, а затем набрать определенную комбинацию цифр и символов, якобы для проверки и получения «кода регистрации». Комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому, злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

6. Простой код от оператора связи

Поступает звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи, с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ

Перезвонить своему мобильному оператору для уточнения условий, а также узнать, какая сумма спишется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

7. Ошибочный перевод средств

Абоненту поступает SMS-сообщение о поступлении средств на его счет с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности, деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ

Если Вас просят перевести, якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

1. Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда Вы звоните по указанному телефону, то Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации. Злоумышленникам нужен лишь номер Вашей карты и ПИН-код, как только Вы их сообщите, деньги будут сняты с Вашего счета. Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.
2. Если Вы утратили карту немедленно ее блокируйте.
3. При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной.
4. Совершая операции пластиковой картой, следите, чтобы рядом не было посторонних людей. Набирая ПИН-код, прикрывайте клавиатуру рукой.
5. Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нем телефону.
6. Если банкомат долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь, от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.
7. Хищение с карт, подключенных к опции бесконтактных платежей. Для проведения оплаты бесконтактной картой рекомендуется просто приложить её к терминалу. Ввод ПИН-кода не требуется, если сумма не превышает 1000 рублей. При этом количество расходных транзакций не ограничено.

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ

1. Установить на телефон (компьютер) современное лицензированное антивирусное программное обеспечение.
2. Не устанавливаете и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).
3. используйте пароли не связанные с Вашими персональными данными.
4. Не сообщать данные карты, пароли и другую персональную информацию.
5. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.
6. По всем возникающим вопросам обращаться в банк, выдавший карту.

7. Не выполнять никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.
8. Не перезванивать по номерам и не переходить ни по каким ссылкам, которые приходят на e-mail или по SMS.
9. Обращать на все сообщения от банка (например, если они содержат грамматические ошибки.

БУДЬТЕ БДИТЕЛЬНЫ!