**Профилактика телефонного мошенничества**

Телефонное мошенничество реализуется в настоящее время методами «социальной инженерии», которая определяется как способ обманом заставить кого-либо раскрыть информацию или предоставить доступ к данным. Мошенники манипулируют людьми в своих преступных целях, используя человеческие слабости, низкий уровень финансовой грамотности и отсутствие у населения выработанных способов противодействия. Производится так называемый «взлом» человеческого сознания с использованием психологических приемов.

К наиболее распространенным способам телефонного мошенничества в настоящее время относятся следующие:

- Мошенник представляется сотрудником правоохранительных органов (сотрудником ФСБ РФ, прокуратуры, следственного комитета) и сообщает, что группа лиц использовала лицевой счет клиента для распоряжения денежными средствами, полученными преступным путем; далее снова предлагаются действия по снятию наличных денежных средств или их переводу на «безопасный счет». Один из вариантов войти в доверие к потерпевшему – направить сообщение в мессенджере якобы от руководителя организации с просьбой о содействии сотрудникам ФСБ, «который сейчас перезвонит». Естественно, что аккаунт руководителя является клоном настоящей его страницы с фотографией, либо просто используется его фотография, взятая в сети Интернет.

- Мошенник представляется специалистом портала «Госуслуги» или оператором сотовой связи и под предлогом получения писем, информации, справок (о перерасчете пенсии, о доходах…, штрафах… иной интересующей информации клиента) на электронную почту клиента, а также смены абонентского номера телефона, окончания действия сим-карты (которая зачастую привязана к банковской карте в качестве услуги в мобильном банке) просит граждан сообщить ему код (пароль), который поступит в смс-сообщении на мобильное устройство и, получая данные сведения, в последующем мошенник получает свободный доступ в приложения клиента (оператора связи, банковское приложение), после чего зная персональные данные лица, оформляет от его имени кредиты в различных учреждениях, банках, микрофинансовых организациях.

- Мошенник представляется сотрудником банка и сообщает о том, что некто пытается оформить кредит от лица клиента, либо совершить манипуляции с личными накоплениями на счете последнего, и клиенту настоятельно предлагается для защиты от несанкционированного оформления кредита, как можно быстрее первому оформить кредит или взять кредит на сумму аналогичную той, которая уже оформлена посторонним лицом, обналичить деньги и передать их для сохранения якобы сотрудникам банка или перевести денежные накопления на «безопасный счет» («зеркальный счет», «в безопасную ячейку»), т.е. совершить действия по предупреждению оформления несанкционированного кредита на имя потерпевшего посторонним лицом (самому клиенту вперед быстрее оформить новый кредит, чтобы Банк более не смог выдать иных кредитов на имя клиента посторонним лицам) и тем самым, переведя только что взятые в кредитные денежные средства, аннулировать кредит. Схемы мошенничества являются многоэтапными и растянутыми во времени. Диалог с клиентом может продолжаться в течение нескольких часов или дней. При общении с гражданами используются психологические приемы воздействия путем уговоров, угроз (содействие террористам, вооруженным силам недружественных государств), повышение тона, перекладывания вины и ответственности при потере денежных средств на самого гражданина в случае отказа следовать указаниям звонящих. Зачастую злоумышленники возвращаются к обманутым гражданам, чтобы обмануть их повторно и/или вовлечь их в противоправные антиобщественные действия (совершить поджог отделов полиции, военкоматов, транспортных средств, отделений банков).

Клиенту под угрозой уголовной ответственности предъявляется требование о сохранении всех переговоров в тайне; сообщается, что разглашать информацию нельзя никому, даже соседям или близким родственникам. Мошенники полностью контролируют действия граждан, требуют постоянно находиться с ними в режиме телефонного общения, при направлении гражданина в отделении банка для оформления и получения кредита, указывают лицу при общении с сотрудником банка называть надуманные цели для получения кредита (срочная покупка, медицинское лечение, строительство), якобы для понимания того, кто из сотрудников банка замешан в совершении мошенничества и дальнейшей его поимке.

Появляются и дополнительные способы телефонного мошенничества:

- Махинации со счетами мобильных телефонов. Клиенту поступает сообщение или звонок об ошибочном переводе денег на счёт мобильного телефона и формулируется просьба вернуть их владельцу. При этом могут осуществляться угрозы обращения в полицию или оператору мобильной связи с требованием блокировки телефона.

- Сообщение о попавшем в беду родственнике (чаще это представлено как виновник при совершении ДТП) с просьбой о финансовой помощи «для решения вопроса». Звонок о попавшем в беду родственнике, как правило, поступает на стационарный телефон среди ночи, когда полусонной жертве сообщают об автомобильной аварии, наезде на пешехода, крушении поезда или любых других происшествиях, случившихся с детьми, внуками или просто друзьями. Далее следует просьба о срочной помощи в виде перевода немалой суммы на электронный кошелек или счёт мобильника. Метод крайне жестокий, известны случаи инфарктов от подобных новостей. Потерпевшими выступают чаще всего лица пожилого возраста. Есть примеры, когда телефонные звонки поступали малолетним детям с требованиями найти деньги, так как их родители якобы виновны в совершении дорожно-транспортных происшествий.

- Сообщения о выигрыше в лотерею, получении бонусов в виде денежного приза от банка в честь дня рождения, иного события. Новость сопровождается требованием перевода на покрытие технических издержек самой лотереи, либо сообщении реквизитов банковской карты и кода из смс-сообщения для перевода денежного приза. Мошенники здесь рассчитывают на незнание гражданами законодательства РФ, согласно которому все расходы организаторов лотерей ложатся на них самих, а также отсутствия в банках подобных ситуаций – выплат в качестве призов. Для усыпления бдительности клиентов мошенники используют различные современные технологии и мошеннические схемы.

Также необходимо отметить о новом способе обмана россиян при помощи чат-ботов. Так, по мере того как чат-боты стали набирать популярность у обычных людей, ими стали пользоваться и мошенники. Например, они взламывают легитимные чат-боты различных компаний и организуют рассылку-опрос, с помощью которой собирают личную информацию: номера телефонов, геопозицию и т.д. Также хакеры могут создавать собственные чат-боты, что придает фишинговому сайту большую правдоподобность: люди доверяют чат-ботам и не подозревают, что «сливают» им свои данные.

Распространены факты применения технологии подмены номера, когда в качестве номера звонящего подставляется официальный телефон банка, различных правоохранительных ведомств (сведения о которых в свободном доступе находится в сети Интернет, данные руководителей указанных структур).

Дистанционные мошенники постоянно совершенствуют манипулятивные тактики воздействия на сознание граждан с целью хищения их денежных средств. Преступники изобретательны и циничны. Знание о методах мошенников поможет защититься от финансовых потерь, будет способствовать повышению их психологической устойчивости.