Новые способы дистанционных мошенничеств.

Несмотря на принимаемые правоохранительными органами Старооскольского городского округа меры, количество дистанционных хищений с использованием информационно-телекоммуникационных технологий продолжают расти, а жители нашего округа продолжают подвергаться уловкам мошенников. За 3 месяца 2024 года на территории округа уже зарегистрировано более 200 таких преступлений.

Мошенники умело используют всю доступную информацию и современные технологии, прекрасно разбираются в психологии людей, умело используют в своих корыстных целях человеческие слабости (страх, алчность) и чувства (сострадание, обеспокоенность за близких, жалость).

В настоящее время практически каждый человек знает, что банковские работники не звонят на сотовые телефоны гражданам, и что никому нельзя сообщать коды доступа, поступившие на мобильные телефоны. Однако, мошенники не стоят на месте и придумывают новые способы обмана граждан, о которых необходимо знать каждому, чтобы не стать жертвой преступления.

Самыми распространенными в 2024 году способами совершения дистанционных мошенничеств являются следующие.

Наиболее частым в текущем году является **звонок от «оператора сотовой связи» (взлом портала Госуслуг).** При этом способе мошенник звонит на сотовый телефон потерпевшего и представляется оператором сотовой связи, поясняет о том, что якобы у потерпевшего заканчивается срок действия работы его сим-карты (или предлагает сменить тариф), после чего потерпевшему предлагают «онлайн» продлить срок действия сим-карты, на что люди зачастую соглашаются. После чего им приходит СМС сообщение с кодом, однако люди по собственной невнимательности не обращают внимание на то, что СМС сообщение пришло с портала «Гос. услуг», и диктуют данный код мошеннику, тем самым предоставляют доступ к своему личному кабинету. Необходимо знать, что сим-карты не имеют срока давности. Не стоить звонить по номерам 8-800…, которые приходят в СМС сообщениях гражданам. Также стоить отметить, что сотрудники портала Госуслуг НИКОГДА не звонят гражданам, а при подозрительной активности личного кабинета автоматически блокируют его до разбирательств. Стоит также отметить, что кредитные обязательства оформить на гражданина лишь получив доступ к личному кабинету в портале Госуслуг невозможно. Мошенники смогут это сделать, лишь получив от потерпевшего коды, поступившие из кредитной организации.

Из вышесказанного можно сделать вывод о том, что никому нельзя называть коды, которые приходят в СМС сообщениях от различных организаций (банки, Госуслуги, авито, и кабельное телевидение, сотовые операторы и т.д.).

Дополнительный заработок. В последнее время участились случаи мошенничеств, связанные с желанием получить дополнительный заработок в сети «Интернет». Граждане находят «онлайн» работу, где им предлагают оценивать товары на популярных площадках, таких как «Валдберис» «Озон» и тд., за что они будут получать денежные средства на банковские карты.

Данный способ заработка не является действительным, так как после выполнения 1-2 заданий «работодатель» требует пополнить несуществующий личный кабинет на различные суммы от 1000 рублей до 100 000 рублей, чего делать категорически нельзя.

Демонстрация экрана. При разговоре с неизвестными лицами мошенники рекомендуют установить в смартфоне программы удаленного доступа, которые размещены на популярных платформах для IOS u Android, этого делать никоем случае нельзя, так как мошенник получает доступ к конфиденциальной информации (паролям от личных кабинетов и т.д.), с помощью которой совершается хищение.

Родственник попал в ДТП. Старая схема, которая, к сожалению, до сих пор работает. Заключается в том, что мошенники звонят, зачастую, на домашний телефон, и плачущим голосом сообщают о том, что их родственник попал в ДТП, просят передать денежные средства курьеру (водителю, помощнику следователя и т.д.) якобы для освобождения от ответственности их родственника. Никогда в данном случае нельзя передавать неизвестным лицам денежные средства, кем бы они не представились. При этом следует сразу же прервать разговор, связаться со своим родственником и сообщить о данном разговоре, выяснить обстоятельства.

Звонки в мессенджеры (WhatsApp, Viber, Telegram и др.). Сотрудники организаций, таких как Сбербанк, ВТБ и др. банки, ФСБ, полиция НИКОГДА не звонят гражданам в мессенджерах**,** даже если «сотрудник» скинул фотографию своего удостоверения или жетона, это не означает, что он действительно является сотрудником из вышеперечисленных организаций. Разговор нужно сразу прекратить и заблокировать данный номер.

Заем денежных средств от близкого лица. В социальных сетях гражданам поступают сообщения от их близких друзей, родственников, знакомых с просьбой займа денежных средств под различными предлогами. Как правило у этих граждан злоумышленники взломали аккаунт в социальных сетях и разослали от имени владельца аккаунта сообщения с просьбой о помощи. В данном случае необходимо связаться со своим знакомым и уточнить, для какой цели он просит денежные средства, и точно ли не взломали его аккаунт.

Фишинговый сайт (сайт двойник), интернет ссылки. В настоящее время большой популярностью пользуются покупки в интернет-магазинах, в связи с чем появились сайты двойники, которые визуально не отличаются от оригинальных сайтов, где мошенники просят указать ПОЛНЫЕ реквизиты банковской карты, это номер карты, срок действия и CVV код (трехзначный код на обратной стороне), чего ни в коем случае нельзя делать, так как можно лишиться всех денежных средств на банковском счете, а также предоставить мошеннику доступ к личному кабинету банка.

Площадки для покупки и продажи товаров Авито, Юла и др. При продаже (покупке) каких-либо товаров на подобных площадках нельзя переходить по сторонним ссылкам, а также продолжать общение в сторонних мессенджерах, сообщать полные реквизиты банковской карты, номер карты, срок действия и CVV код (трехзначный код на обратной стороне).

Звонок (сообщение) от руководителя организации. Мошенники из источников в свободном доступе получают информацию о руководителе организации, после чего злоумышленник от имени руководителя организации связывается с работниками данной организации (чаще всего используя мессенджеры WhatsApp, Viber, Telegram и др., зачастую применяя способ «подмены номера вызывающего абонента»), и сообщает о том, что якобы с ним связались сотрудники ФСБ (полиции, следственного комитета и т.д.) и рекомендует действовать по их указаниям. После чего с сотрудником организации связывается подельник, и представившись сотрудником правоохранительных органов сообщают о том, что в Центробанке произошла утечка его данных и его банковские счета находятся в «опасности», либо иную легенду для получения доступа к счетам потерпевшего.

Инвестиции (дополнительный заработок). В сети интернет граждане находят различные сайты, зачастую специально созданные мошенниками, где им предлагают инвестировать накопления с высокой доходностью. При этом дизайн мошеннических сайтов похож на известные торговые площадки. После того, как гражданин оставил заявку на участие в инвестициях, с ним связывается мошенник, который сообщает о том, что заявка на участие рассмотрена, а также о том, что в ближайшее время с ним свяжется «брокер», который с ним будет дальше работать. После чего в мессенджерах с потерпевшим связывается «брокер», с помощью которого потерпевший создает «Личный кабинет», и его просят пополнить свой счет, а по факту – перевести деньги, чаще всего на карту физического лица или электронный кошелек. При этом мошенники имитируют фейковый рост депозита, что внушает потерпевшему доверие и побуждает отправить мошенникам еще больше денег. В итоге вернуть свои деньги практически невозможно.

Кража денег со счета чужой банковской карты. Если гражданин нашел банковскую карту любого из банков, то ему необходимо попытаться установить владельца данной банковской карты и сообщить ему о находке. Если же установить владельца не удалось, данную банковскую карту нужно утилизировать (порезать) или отнести в отделение банка, которым выпущена банковская карта, и сообщить о находке, чтобы сотрудники банка связались с собственником карты. Пользоваться чужой банковской картой в категорической форме запрещено, так как это влечет уголовную ответственности за хищение денежных средств с банковского счета по пункту «г» части 3 статьи 158 УК РФ.

Старший помощник
Старооскольского городского прокурора

советник юстиции А.М. Стёпичев