Способы преступлений, совершаемых с использованием информационно-телекоммуникационных технологий».

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно-телекоммуникационных технологий стремительно набирают силу.

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрыть информацию о себе либо совершать те или иные действия, используют человеческие слабости, чувства в своих корыстных интересах.

Основные и самые распространенные схемы телефонного мошенничества:

1. *Взлом «Госуслуг».*

На телефон абонента поступает звонок, где неустановленные лица представляются сотрудниками Пенсионного Фонда, НЭСК, сотовой компании, Федеральной налоговой службы, Почты России, банковских учреждений и под предлогом оказания соответствующих услуг просят назвать код, поступивший в смс-уведомлениях. Таким образом, злоумышленник получает доступ к персональным данным.

2. *Ошибочный перевод денежных средств.*

Абоненту поступает смс-сообщение о поступлении на его счет переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок, и злоумышленник сообщает, что ошибочно перевел деньги на его счет, 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 этому номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все денежные средства.

3. *Покупка товара в интернет-магазинах, сервиса по продаже («Авито», «Юла» и пр.)*

Результатам отправки денежных средств «продавцу» может явиться либо непоступление покупки, либо поступление другого товара (менее ценной вещи, муляжа). Уменьшить риски приобретения товара у мошенников поможет изучение отзывов о продавце.

4. *Перевод денежных средств на «безопасный счет».*

«Безопасных счетов» не существует. Преступление совершается от лица «представителя банка» либо «сотрудника правоохранительных органов», сообщающего жертве о действиях неких злоумышленников, которые посягают на имеющиеся на лицевых счетах денежных средствах, которые необходимо перевести на другой, безопасный счет. Дальнейшее манипулирование может включать «помощь» в установке специального

программного обеспечения на мобильный телефон, переход по отправленной в смс-уведомлении ссылке, опосредованном сопровождении в ближайший банкомат.

5. *«Инвестирование».*

Граждане находят в сети Интернет различные «зарубежные» финансовые организации, которые предлагают под их управлением инвестировать деньги в валюту, криптовалюту, акции, металлы и т.п., обещая при этом доходы, существенно превышающие действительные биржевые курсы. Злоумышленники просят установить приложение, скачанное с их сайта, на котором отображаются биржевые котировки (стоимость актива, определенная в ходе торгов), создать личный кабинет и специальный счет для участия в торгах. В итоге потерпевший переводит денежные средства не на специальный счет, а на обычные электронные средства платежа мошенников. Все время потерпевшего сопровождает «персональный менеджер», цель которого заставить гражданина под различными предлогами постоянно «инвестировать». Однако вывести деньги со специального счета невозможно.

6. *«APK- файл».*

APK – формат архивного файла, который содержит все необходимые компоненты для установки и работы приложения. Данные файлы могут содержать вирусы и трояны. Мошенники часто рассылают APK-файлы, маскируя их под фото или приглашения на мероприятия. Например, Вам могут прислать файл с названием «фото». В сообщении может быть вопрос «Привет, это ты на фото?». Если открыть файл такого формата, смартфон заразится вирусом, который может украсть личные данные.

Как не стать жертвой мошенников:

- Оформляйте на свое имя только банковские карты, в которых имеется необходимость;
- Помните, что сотрудники банка, правоохранительных органов никогда не спрашивают данные о Вашей банковской карте, тем более не запрашивают коды для подтверждения, не просят оформить кредит и не звонят посредством мессенджеров «Вотсап». Если поступил сомнительный звонок из банка, необходимо самостоятельно обратиться в банковское учреждение для подтверждения каких-либо операций;
- Никому не передавайте реквизиты своих банковских карт;
- Не переходите по незнакомым ссылкам, направляемым Вам незнакомыми лицами или «друзей», «знакомых»;
- Приобретайте товары в проверенных Интернет-магазинах, предварительно ознакомившись с отзывами. При покупке у частного лица воздержаться от внесения предоплаты.