**Мошенничество с использованием информационно-телекоммуникационных технологий в последние годы набирает обороты и уже становится одним из основных видов, общей массе зарегистрированных преступлений.**

Учитывая, что мобильные телефоны с доступом к сети Интернет имеются у большего числа жителей округа, в том числе у малолетних и граждан пожилого возраста, предполагается, что число мошенничеств будет только расти. Более того, преступниками постоянно разрабатываются и используются все более изощренные способы и схемы хищения денежных средств у граждан.

Актуальные мошеннические схемы можно подразделить на несколько видов:

 1. Сообщения и звонки на телефон и в мессенджерах (Telegram, WhatsApp, Viber).

  Данный способ заключается в том, что сообщения поступают якобы от сотрудников правоохранительных органов (ФСБ, полиции, прокуратуры и т.д.), с предупреждением потерпевших о попытке хищения денежных средств с банковского счета. Мошенники при этом настойчиво и агрессивно, не давая человеку подумать или проконсультироваться с банковскими работниками, убеждают потерпевшего перевести денежные средства на якобы «безопасный счет». После осуществления перевода потерпевший лишается доступа к своим деньгам

 2. Использование личного кабинета «Госуслуги».

Звонящий представляется работником «Госуслуг» или МФЦ и сообщает гражданину, что его личный кабинет пытаются взломать. Мошенник, не давая опомниться, и настаивая, что счет идет на минуты, навязывает помощь в смене учетных данных личного кабинета (логина и пароля), для чего владельцу необходимо продиктовать коды, которые ему придут в смс-сообщениях.

Далее после получения от потерпевшего необходимых кодов, мошенник входит в личный кабинет, запрашивает документы, удостоверяющие личность и сведения о доходах владельца (справка по форме 2-НДФЛ), после чего получает возможность получить онлайн-кредит на подконтрольную банковскую карту в микро финансовых организациях.

3. Фишинг.

Фишинг — это обман пользователя с целью получения его личных данных, таких как логин, пароль, номер телефона или банковской карты. Фишинг больше всего распространён в почтовых системах, социальных сетях, интернет-банкинге и электронных платёжных системах. Мошенники создают поддельные сайты, такие как интернет-магазины, торговые площадки, сайты объявлений и сайты развлекательного контента категории 18+.

 Вводя на сайте данные банковских карт, номера телефона, злоумышленники на основе собранных данных получают возможность создать дубликат банковской карты или оплатить товары в реальных интернет-магазинах на денежные средства потерпевшего. А полученные аутентификационные данные (логин и пароль) вполне могут подойти для доступа к другим интернет-сервисам и интернет-банкингу.

Чтобы защитить свои деньги от преступного посягательства предлагается следовать нижеперечисленным рекомендациям:

– использовать многофакторную аутентификацию. Например, вместо простого запроса имени пользователя или пароля при многофакторной аутентификации запрашивается дополнительная информация (отпечаток пальца, голосовые данные пользователя, контрольный вопрос и т.д.);

– использовать сетевой экран с целью блокирования нежелательного трафика, а также предотвращения заражения компьютера или смартфона вредоносными программами;

– создать надежный пароль, который должен состоять минимум из 12 символов, содержать заглавные и строчные буквы, специальные символы и цифры.

– использовать на устройстве актуальную версию антивирусной программы с обновленной базой;

– соблюдать осторожность при открытии ссылок, поступивших в электронных сообщениях;

– не сообщать кому-либо свои персональные данные, особенно пароли от личного кабинета, номера и ПИН-коды банковских карт;

– не хранить такую информацию о личных паролях на компьютере или смартфоне;

– перед тем как приобрести товар в интернет-магазине необходимо убедиться, что адрес сайта является официальным, изучить отзывы интернет-пользователей об этом магазине;

– критично относиться к сообщениям и звонкам неизвестных, сообщающих о том, что необходимо что-то срочно делать с денежными средствами на банковских счетах. В таких ситуациях для собственного спокойствия целесообразно взять паузу и заблокировать карту (дистанционно или в банке).