**Как обезопасить себя от мошенничества в сфере информационных и телекоммуникационных технологий?**

**Разъясняет помощник прокурора Волжского района Самарской области Тарасова Юлия Рафиковна**

На территории Российской Федерации на протяжении последних лет отмечается рост числа атак на клиентов банков, которые осуществляются ежедневно посредством информационных и телекоммуникационных технологий. Например, в форме многочисленных звонков гражданам с незнакомых номеров.

Наиболее распространенным видом мошенничества с использованием информационных и телекоммуникационных технологий являются звонки злоумышленников, представляющихся сотрудниками банков или правоохранительных органов, с предупреждением граждан об атаке на банковский счет гражданина либо об оформлении якобы мошенниками на имя гражданина кредита. Злоумышленники убеждают граждан в необходимости в связи с этим перевести денежные средства со счета гражданина на якобы безопасный счет банка.

Желание гражданина избежать негативных последствий приводит к вовлечению его в контакт с мошенником, в рамках которого по указанию последнего введенный в заблуждение гражданин сообщает злоумышленнику необходимые для совершения мошенничества коды, пароли, номера банковских карт и счетов, кодовые слова, самостоятельно под контролем мошенников оформляет на свое имя кредиты на крупные суммы, переводя денежные средства на счета, указанные неизвестными.

Чтобы обезопасить себя и своих близких и не стать жертвой мошенников, необходимо соблюдать правила цифровой или компьютерной безопасности, а именно: не использовать подозрительные интернет-сайты, не сообщать незнакомым лицам (банковским служащим, сотрудникам правоохранительных органов), в том числе по телефону, данные своих банковских карт и паролей от Интернет-банка; использовать при входе в Интернет-Банк сложные пароли, затрудняющие злоумышленникам доступ к информации.

Гражданам при поступлении посредством сотовой связи просьб незнакомых лиц об оказании помощи в связи с непредвиденными обстоятельствами, связанными с их родственниками, переводе крупных сумм денег с банковских счетов, нужно сохранять бдительность и в каждом случае прежде, чем перечислять денежные средства, принять меры к проверке поступившей информации, не реагировать на требования злоумышленников, создающих во время телефонных переговоров напряженную атмосферу и торопящих гражданина с принятием решения.

В связи с тем, что мошенничества с использованием электронных средств обладают повышенной общественной опасностью, законодателем за совершение указанных преступных действий предусмотрена уголовная ответственность.

Так, статьей 159.3 УК РФ установлена уголовная ответственность за мошенничество с использованием электронных средств платежа (платежных карт, иных технических средств).

За мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей уголовная ответственность предусмотрена ст. 159.6 УК РФ.

В зависимости от тяжести совершенного преступления Уголовным кодексом Российской Федерации за преступления, связанные с указанными видами мошенничества, предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы на срок до 6 лет.

При обнаружении неправомерного снятия денежных средств с банковских счетов (электронных карт и кошельков) необходимо незамедлительно обращаться в правоохранительные органы.