**Телефонное мошенничество**

Телефонная связь, ее возможности и особенности зачастую используются злоумышленниками для незаконного обогащения. Телефонное мошенничество – это очень распространенный в настоящее время вид мошеннических действий, направленный на обогащение путем обмана телефонного собеседника без визуального контакта с ним. Как правило, мошенники представляются своим жертвам родственниками или обманным путем действуют от имени банка.

Действия телефонных мошенников квалифицируются по ст. 159 УК РФ как мошенничество, т.е. умышленные действия, направленные на хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях, направленных на введение владельца имущества или иного лица в заблуждение. Злоупотребление доверием при мошенничестве заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам. Согласно разъяснениям пункта 3 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (далее – постановление Пленума № 48) доверие может быть обусловлено различными обстоятельствами, например служебным положением лица либо его личными отношениями с потерпевшим.

Мошенничество признается оконченным с момента, когда имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность пользоваться или распорядиться им по своему усмотрению.

В пункте 5 постановления Пленума № 48 установлено, что если предметом преступления являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу [п. 1 примечаний к ст. 158](consultantplus://offline/ref=54B46AE0779B7050834C7E216A973DE93777936E90D5918CBDC7EAD4739DEAC6CEB4E1DC2043A27E41116F135FE92056E81BB281602AB2044Du5J) УК РФ и [ст. 128](consultantplus://offline/ref=54B46AE0779B7050834C7E216A973DE93774916893D4918CBDC7EAD4739DEAC6CEB4E1D82545AC23165E6E4F1BBB3357EF1BB1817C42uAJ) ГК РФ содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб.

Телефонное мошенничество в зависимости от размера похищенного и других обстоятельств деяния (например, имеются или отсутствуют признаки преступления) может повлечь административную или уголовную ответственность.

В Кодексе об административных правонарушениях РФ предусмотрена ответственность за мелкое хищение: от наложения административного штрафа в размере до пятикратной стоимости похищенного имущества, но не менее одной тысячи рублей до административного ареста на срок от десяти до пятнадцати суток.

Кроме того, на основании ст. 7.27.1 КоАП РФ причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием при отсутствии признаков уголовно наказуемого деяния влечет наложение административного штрафа в размере до пятикратной стоимости причиненного ущерба, но не менее пяти тысяч рублей.

[Статья 159](consultantplus://offline/ref=54B46AE0779B7050834C7E216A973DE93777936E90D5918CBDC7EAD4739DEAC6CEB4E1DC2043A17746116F135FE92056E81BB281602AB2044Du5J) УК РФ предусматривает различные виды уголовной ответственности за мошенничество в зависимости от конкретных обстоятельств: от штрафа до лишения свободы сроком до десяти лет.

**Действия, которые необходимо предпринять, став жертвой**

**телефонного мошенничества**

Если гражданин предполагает, что стал жертвой телефонного мошенничества, ему необходимо обращаться в органы внутренних дел с соответствующим заявлением. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Кроме этого, следует сообщить о факте телефонного мошенничества в абонентскую службу мобильного оператора, который обслуживает номер преступника. Если гражданин, к примеру, совершил перевод денежной суммы по мобильной сети, то принятие оператором экстренных мер может позволить заблокировать перевод и вернуть деньги.

Для того чтобы не стать такой жертвой, необходимо следовать определенным правилам. Например:

- если получен звонок с просьбой о срочной денежной помощи для известного гражданину лица (знакомого, родственника и т.п.), следует не принимать решение сразу, идя на поводу у позвонившего, а проверить полученную от него информацию, перезвонив вышеуказанным лицам, или связаться с ними иными способами;

- нельзя сообщать по телефону личные сведения или данные банковских карт, которые могут быть использованы злоумышленниками для неправомерных действий;

- нельзя перезванивать на номер, если он не знаком.

**Кибермошенничество**

Кибермошенничество – один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).

Наиболее распространенным видом кибермошенничества является так называемый «скимминг». С помощью технических средств преступники копируют магнитную полосу карты и считывают ее пин-код. На основе полученных данных они изготавливают поддельную пластиковую карту, при использовании которой деньги списываются с оригинала.

Другой способ – «фишинг», когда преступники получают информацию о карте дистанционно. Для этого они присылают гражданину SMS с просьбой сообщить пин-код и cvv-код, представляясь сотрудниками банка.

Фарминг – очередной метод хищения, суть которого сводится к автоматическому перенаправлению пользователей на фальшивые сайты. В отличие от фишинга новый метод хищения данных почти не требует участия потенциальной жертвы.

Пользователи могут стать жертвой фарминга в силу уязвимостей браузеров, которые позволяют размещать в адресной строке фальшивые адреса сайтов, уязвимостей операционных систем и уязвимостей DNS-серверов (это специализированный компьютер (или группа), который хранит IP-адреса сайтов).

Согласно поправкам, за мошенничество с банковскими картами с применением высоких технологий преступникам грозят принудительные работы на срок до 5 лет или лишение свободы сроком до 6 лет. При этом осужденному придется заплатить штраф - от 100 до 300 тысяч рублей или в размере его дохода за период от одного года до двух лет. Если же преступление совершено организованной группой, срок лишения свободы увеличивается до 7 лет, а размер штрафа - до 1 миллиона рублей.

Чтобы обезопасить себя:

1. Не открывайте электронные письма от незнакомых отправителей.

2. Нажимайте на ссылку внутри электронного письма только в том случае, если вы точно знаете, куда она ведет.

3. Получив письмо от сомнительного отправителя, перейдите по прилагаемой ссылке вручную – введите адрес законного веб-сайта в адресную строку браузера с помощью клавиатуры, так Вы обеспечите для себя еще один уровень безопасности.

4. Проверяйте цифровые сертификаты веб-сайтов.

5. Если Вас просят раскрыть конфиденциальные данные, убедитесь, что URL-адрес (URL это адрес, который выдан уникальному ресурсу в интернете) веб-страницы начинается с «https», а не просто с «http». Буква «S» обозначает «secure» (безопасно), то есть подключение с таким адресом является защищенным.