Прокуратура Приволжского района разъясняет, что участились случаи совершения преступлений, совершенных с использованием информационно- телекоммуникационных технологий. Большее количество преступлений составляют мошенничества (ст. 159 УК РФ), кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

Наиболее распространенными способами совершения преступлений на сегодняшний день являются:

**1. СМС от работодателя.**  
Потерпевшему поступает смс сообщение или сообщение в мессенджере от работодателя о том, что с ним в ближайшее время свяжется сотрудник ФСБ или иной организации, следует с ним пообщаться.  
После этого потерпевшему звонит сотрудник с именем указанным руководителем и сообщает о попытках перевода личных сбережений на иностранные счета, финансирование терроризма, Украины и т.п. В целях пресечения преступных операций потерпевшего убеждают прервать транзакции путем перевода денег (личных накоплений или путем взятия кредита) на счет, указанный злоумышленниками.

**2. Злоумышленники продают Вашу квартиру или машину.**  
Звонившие представляются представителями службы безопасности коммерческого банка, Гос. услуг, Центрального банка либо правоохранительного органа. Сообщают о том, что персональные данные с личного кабинета утекли и теперь преступники могут от Вашего имени продать квартиру, машину, используя электронноцифровую подпись. В целях защиты имущества следует срочно его продать, перевести деньги на «защищенный канал», «безопасный счет», «резервную ячейку».

**3. Перевод денег на «безопасный счет».**  
Звонившие представляются либо представителями службы безопасности коммерческого банка, Центрального банка либо правоохранительного органа и сообщают, что мошенники с использованием персональных данных потерпевшего оформляют кредиты в различных банках и для того, чтобы предотвратить хищение денег с банковского счета необходимо личные сбережения срочно перевести на «безопасные счета». В ходе дальнейшего общения потерпевшему сообщают о необходимости оформления кредитов и их перевода. Также зарегистрированы случаи продажи недвижимости и перевода мошенникам вырученных средств. Следует отметить, что общение потерпевшего со злоумышленниками является длительным, в некоторых случаях осуществляется в течение нескольких месяцев, используется как телефонная связь, так и общение посредством мессенджеров (Ватсап, Вайбер, Телеграм и т.д.), Кроме того, следует помнить, что «безопасных счетов» не существует, а представители Центрального Банка не осуществляют работу с физическими лицами.

**4. Звонок злоумышленника под видом мобильных операторов,**которые сообщают, что срок действия вашей сим-карты истек либо истекает, а для его продления необходимо сообщить код, который поступит в смс либо пройти по ссылке, иначе сим-карта будет заблокирована, Важно знать, что у сим-карты нет срока действия, сотовые операторы перевыпускают сим-карты только по просьбе потребителей в случае физического износа, потери, необходимости другого формата. Выполнив требования мошенников и сообщив код из смс, либо пройдя по ссылке Вы отдаете в руки злоумышленников доступ в свой личный кабинет на сайте оператора связи, после чего мошенники имеют возможность устанавливать переадресацию сообщений на нужный им номер, что позволит сменить пароль от мобильного банка и похитить денежные средства. Вторая разновидность таких преступлений - получение в результате сообщения кода из смс доступа к аккаунту «госуслуг», дальнейшее оформление заявок на кредиты в банках, получение к персональным данным, таким как сведения о доходах, наличие банковских счетов и т.д.

**5. Сдача налоговых деклараций и справок о доходах.**  
Звонившие представляются сотрудниками Госуслуг, управления по делам президента, сообщают, что в рамках декларационной компании проверяют персональные данные лиц, сдавших налоговые декларации либо декларации о доходах. Для подтверждения следует назвать паспортные данные и код из смс – сообщения, и как результат, списание денег со счетов, взятие кредита.

**6. Взлом либо копирование аккаунта** пользователя в мессенджерах ватсап, вайбер, телеграмм, социальных сетей вконтакте и дальнейшее  направление сгенерированных искусственным интеллектом (нейросетью) голосовых сообщений от имени потерпевшего, которое полностью копирует его голос, используя при этом ранее отправленные сообщения владельца аккаунта. Далее по типичной схеме — просьба одолжить взаймы, фото банковской карты для перевода денежных средств. В данной ситуации важно убедиться, что общение происходит со знакомым путем звонка по мобильной сети. Сделав это, Вы обезопасите себя и предупредите знакомого о том, что от его имени действуют мошенники. Для того, чтобы не потерять контроль над Вашим аккаунтом никогда не переходите по незнакомым ссылкам, не скачивайте программы из неподтвержденных источников, используйте двухфакторную аутентификацию Ваших аккаунтов. Будьте максимально внимательны, поскольку следующим этапом использования искусственного интеллекта может явиться генерация видеоизображений и рассылка видео сообщений от имени родных, коллег, знакомых и т.д.

**7. Хищение денежных средств через систему быстрых платежей (СБП).**  
Например, покупатель на сайте оставляет заявку на приобретение товара, ему поступает звонок якобы от сотрудника магазина, предлагается скидка на товар, но только при условии оплаты через СБП или QR-код. Далее злоумышленник присылает в мессенджер ссылку, ведущую на страницу с формой оплаты по QR-коду. Покупатель подтверждает платеж и денежные средства поступают на счет мошенника. Важно в такой ситуации связаться со службой поддержки онлайн- магазина, через официальный сайт или приложение. Не сохранять для оплаты в личных кабинетах банковские карты, при возможности заведите отдельную карту для оплаты покупок онлайн.

**8. Заработок на бирже, заманивание прибыльными инвестициями.**  
Преступниками в сети Интернет создается максимальная видимость, что общение происходит с представителями крупных инвестиционных площадок, их сайты имеют видимое сходство с банковскими организациями (например, Газпроминвестиции, РБК-инвестиции, Т-Банкинвестиции и т.д.), назначается личный брокер, общение с которым может осуществляться даже посредством видеозвонков. Под их руководством создается личный кабинет на торговой площадке, в котором отображаются все внесенные денежные средства, и прибыль. Однако их дальнейший вывод невозможен.

**9. Рассылка налоговых писем о выявлении подозрительных транзакций и активности налогоплательщика.**  
В поддельном сообщении предлагается пройти дополнительную проверку и предоставить сведения по запросу налоговой службы. Так, мошенники могут запросить кассовые документы, счета-фактуры, отчетные документы. Далее для прохождения проверки предлагается обратиться к указанному в письме инспектору под угрозой блокировки счетов налогоплательщика, Важно помнить, что ФНС не рассылает такого рода письма и не имеет отношения к ним, такие письма открывать не рекомендуется, как и переходить по ссылкам. Используемые мошенниками схемы постоянно меняются, «подстраиваясь» под общественно политическую обстановку, значимые события в государстве.

**10. Схема «Ваш родственник попал в ДТП».**  
Наиболее подвержены данному виду преступлений пожилые граждане. Злоумышленник представляется либо родственником потерпевшего, либо представителем правоохранительного органа. В ходе разговора с потерпевшим сообщает, что для освобождения от уголовной ответственности и наказания в виде лишения свободы срочно необходимо передать денежные средства. Далее потерпевший, будучи введенным в заблуждении и находясь в стрессовой ситуации, действует по указаниям мошенника, денежные средства переводит либо на указанные счета, либо передает «курьерам». Стоит еще раз обратить внимание, что жертвой кибермошенников может стать каждый, вне зависимости от возраста, образования, социального положения и прочих факторов. Причина в том, что мошенники воздействуют на эмоции человека, а современные технологии позволяют сделать используемые приемы максимально правдоподобными. Чтобы не стать жертвой преступников, необходимо запомнить и соблюдать следующие правила:  
– не сообщать никому данные банковских карт, а также сведения из смс- сообщений для входа в онлайн-банк или совершения финансовой операции;  
– не осуществлять поспешные переводы денежных средств, лицам, представившимся родственниками, без проверки данной информации;  
– не загружать на мобильные устройства приложения и программы из непроверенных источников;  
– приобретать товары только на официальных сайтах организаций;  
– проявлять бдительность при осуществлении онлайн-покупок, не переходить для покупок по ссылкам.

**Если вы все же стали жертвой мошенников, незамедлительно обратитесь в правоохранительные органы и банк. Сообщите им о случившемся.  
Будьте бдительны!**