Профилактика преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Развитие современного общества, основанного на использовании огромного массива разнообразной информации, немыслимо без широкого внедрения компьютерной техники.

Она служит для хранения и обработки информации, используется как средство связи и коммуникаций.

За последние 4 года произошел резкий рост преступлений, совершенных с применением информационно-коммуникационных технологий или в сфере компьютерной информации – более, чем в 6 раз. Более половины преступлений совершено с использованием сети «Интернет», значительное количество – с применением средств мобильной связи, расчетных (пластиковых) карт.

К социальным причинам роста преступности в сфере ИКТ относится:

- всеобщая компьютеризация, которая создает необходимую среду для деятельности компьютерных преступников;
- противоречия между потребностями населения и возможностью их удовлетворения легальными способами в силу низкого уровня жизни;
- легкомысленное отношение российского общества к компьютерной преступности;
- доверчивость граждан при онлайн-покупке товаров и услуг (оплата до их получения, особенно через интернет-кошелек, а не через расчетный счет банка, помощь по объявлениям от благотворительных организаций через сайты-дублеры со сторонними реквизитами для перечисления денег).

Профилактика особенно важна в отношении несовершеннолетних пользователей сети «Интернет». Учитывая, что значительную группу лиц, совершающих преступления в сети Интернет, составляют ранее не судимые учащиеся, в том числе и несовершеннолетние, с целью профилактического воздействия на них необходимо проводить профилактические мероприятия в школах, высших учебных заведениях, публиковать статьи на эту тему.

Анализ данных уголовно-правовой статистики свидетельствует о росте числа таких преступных деяний.

Так, за 2020 год на территории Мурманской области с использованием информационно-телекоммуникационных технологий совершено более 4200 преступлений, что на 75% больше, чем в 2019 году. Из них 2189 – это мошенничества, совершенные, в том числе с использованием электронных средств платежа и в сфере компьютерной информации.

Только за январь текущего года жертвами действующих дистанционно злоумышленников стали 308 жителей региона.

К наиболее типичным способам совершения преступлений с использованием информационно-телекоммуникационных технологий можно отнести следующие.

Злоумышленники звонят гражданам, представляясь сотрудниками банков, называя их по имени, отчеству, просят сообщить данные банковских карт (номер, CVC(CVV), PIN-коды и т.п.) для предотвращения якобы несанкционированного списания денежных средств либо оформления кредита. Используя эти сведения, получают удаленный доступ к личному кабинету клиента банка и переводят деньги без ведома собственника. При этом, преступники могут использовать программы подмены телефонных номеров, в связи с чем номер входящего звонка определяется у клиента как номер банка. Зачастую введенные в заблуждение граждане сами переводят денежные средства на счета, указанные мошенниками.

Распространены хищения с использованием преступниками сервиса «Avito». Вводя гражданина в заблуждение относительно своего намерения приобрести или продать товар, в ходе телефонных разговоров злоумышленники узнают реквизиты банковской карты потерпевшего, при помощи которых списывают денежные средства со счета. В ряде случаев предлагается перейти по ссылкам для перевода денежных средств, после чего «продавец» не предоставляет оплаченный товар и не выходит на связь.

Кроме этого, преступники массово рассылают SMS-сообщения следующего содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру…». Большинство граждан, вместо того, чтобы сразу обратиться в свой банк для проверки поступившей информации, перезванивают по указанному в SMS-сообщении номеру и в ходе разговора передают злоумышленникам информацию о банковских реквизитах, после чего осуществляется незаконное списание денежных средств. Зачастую граждане сами переводят денежные средства на указанные преступниками «защищенные» счета якобы для их сохранения. Фактически денежные средства выбывают из законного владения, и собственник не имеет к ним доступа.

Хищения денежных средств у граждан совершаются также путем направления SMS-сообщений о выигрыше, для получения которого необходимо перевести денежные средства на указанный абонентский номер.

Распространены факты, когда преступники представляются родственниками либо знакомыми потерпевших, рассказывают, что попали в беседу (стали виновником дорожно-транспортного происшествия, задержаны сотрудниками полиции, срочно требуются деньги на операцию и т.п.) и просят предоставить им денежные средства.

Злоумышленники взламывают электронную почту, аккаунты в социальных сетях, после чего от имени пользователя рассылают гражданам, сведения о которых имеются в контактах данного лица, просьбы о займе денежных средств. В результате деньги поступают на счет мошенника.

Чтобы не стать жертвой преступников, необходимо следовать определенным правилам:

1. Если получен звонок или сообщение в социальной сети с просьбой о срочной денежной помощи для знакомого или родственника, не стоит

принимать решение сразу. Необходимо проверить полученную информацию, связавшись со своими родными и знакомыми.

2. Никогда и никому не сообщайте трёхзначный код на обратной стороне Вашей банковской карты (CVV), это ключ к Вашим деньгам.

3. Нельзя сообщать никому личные сведения, данные банковских карт и СМС-пароли, которые могут быть использованы злоумышленниками для неправомерных действий.

4. Если по телефону Вас просят набрать комбинацию цифр в банкомате, прекратите разговор. Никогда не выполняйте действия с банкоматом «под диктовку» другого человека.

Необходимо помнить, что злоумышленники могут представиться сотрудниками банка, правоохранительного органа, учреждения здравоохранения и обращаться к Вам по имени и отчеству. Однако только мошенники будут просить сообщить реквизиты банковской карты, смс-пароль (код), CVV-код Вашей карты. В каждом таком случае необходимо завершить разговор.

Сотрудники банка также не предлагают:

- установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, для удаления вирусов с мобильного устройства);

- перевести денежные средства на «защищенный счет»;

- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк.

Если Вы стали жертвой преступника, необходимо незамедлительно обратиться в органы внутренних дел с соответствующим заявлением лично либо позвонить по телефонам 102 или 112. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Также следует принять меры к блокировке банковской карты.