Информационная справка об основных видах преступлений

На территории Тверской области, как и по всей стране уже на протяжении нескольких лет происходит рост количества преступлений в сфере IT (кражи, мошенничества, неправомерный доступ к компьютерной информации с целью хищения персональных данных).

В 2023 году было совершено 6451 преступление в сфере IT, ущерб от них превысил полмиллиарда рублей.

1). Основным способом, с помощью которого совершаются преступления такой категории, остается звонок от имени сотрудника какой-либо организации:

- от имени сотрудника сотовой связи, который сообщает что скоро обслуживание абонентского номера будет прекращено и нужно срочно продлить договор связи или проверить абонентский номер, для чего пришлют СМС с кодом. При этом потерпевшему приходит СМС от банка или портала «Госуслуги», далее жертва диктует код из СМС преступнику. С помощью кода злоумышленник получает доступ в личный кабинет жертвы и совершает хищение денежных средств, как со счетов в банках (при доступе в личный кабинет банковских приложений), так и через оформление займов в микрофинансовых организациях с использованием «Госуслуг» (через них можно подать заявку), а также совершается хищение персональных данных, которые могут быть использованы преступниками в дальнейшем при совершении мошенничеств;

- «звонок из службы безопасности банка» с сообщением о подозрительной активности на счете и предложением перевести имеющиеся денежные средства на единый безопасный счет с целью их сбережения;

- звонок от «сотрудника полиции», который сообщает, что родственник (сын, дочь и т.п.) попал в ДТП и является виновником. Для невозбуждения уголовного дела в отношении этого родственника нужно передать курьеру или перевести на указанный счет денежные средства;

- новый предлог, который начал активно использоваться в отношении пенсионеров – звонок от сотрудника поликлиники или Пенсионного фонда о том, что необходимо записаться на прием, и для этого нужно продиктовать код из смс-сообщения, который поступит на телефон гражданина. При этом потерпевшему приходит СМС от банка или портала «Госуслуг», далее жертва диктует код из СМС преступнику. В дальнейшем злоумышленник получает доступ в личный кабинет жертвы и совершает хищение денежных средств, как со счетов в банках (при доступе в личный кабинет банковских приложений), так и через оформление займов в микрофинансовых организациях с использованием «Госуслуг» (через них можно подать заявку), а также

совершается хищение персональных данных, которые могут быть использованы преступниками в дальнейшем при совершении мошенничеств;

- звонки сотруднику через мессенджер от имени якобы руководителя организации/предприятия с просьбой (под различными предлогами: в долг, на нужды организации) перевести денежные средства на указанный преступником счет.

Меры предосторожности:

- не диктовать коды из смс; все коды, пароли, которые поступают вам в СМС ТОЛЬКО для вас, это КЛЮЧ к вашим личным данным, деньгам, аккаунтам и т.п.;

- не решать никаких денежных/финансовых вопросов по телефону, сотрудники государственных служб и организаций, банков НИКОГДА не просят переводить куда-либо денежные средства;

- соблюдать «цифровую гигиену», не оставлять в открытых источниках (соцсети, форумы и т.п.) свои персональные данные, личные фотографии и др.

2). Совершение преступлений с использованием сети интернет:

- поддельные сайты онлайн-магазинов, на которых необоснованно низкие цены или большие скидки. Потерпевший переводит денежные средства в качестве оплаты за товар, который не получает;

- преступник размещает ложные объявления на торговых площадках (Авито, Юла и т.п.) и просит внести 100% предоплату, мотивируя тем, что иначе товар продадут другому покупателю. Потерпевший переводит денежные средства в качестве оплаты за товар, который не получает;

- по объявлению, выложенному потерпевшим, преступник звонит или начинает переписку на сайте, в ходе которой просит номер банковской карты, якобы для оплаты товара. Далее преступник сообщает, что сейчас придет смс с кодом для подтверждения оплаты, который нужно назвать ему. Потерпевший получает СМС от банка, далее жертва диктует код из СМС преступнику. С помощью кода злоумышленник получает доступ в личный кабинет жертвы и совершает хищение имеющихся денежных средств на счетах в банках (при доступе в личный кабинет банковских приложений), так и через оформление займов;

- сайты, на которых предлагают осуществлять инвестирование под высокие проценты и обещающие сверхприбыли.

Меры предосторожности:

- внимательно проверять название сайтов в адресной строке;

- ссылки на сайты, на которых часто совершаете покупки, хранить в браузере в закладках, чтобы каждый раз не искать через поисковик заново;

- использовать для покупки-продажи в сети интернет отдельную

банковскую карту, на которую принимать платежи или с которой расплачиваться. Желательно, чтобы данная карты была другого банка, не того, на котором хранятся основные финансовые средства;

- не переходить по ссылкам, которые поступили с неизвестных абонентских номеров или электронных почтовых адресов; при поступлении с известных номеров и адресов, предварительно созвониться с отправителем, чтобы убедиться – действительно ли он вам направлял, и не взломали ли его аккаунт.

В настоящее время активно вовлекают в преступную деятельность несовершеннолетних детей, пользуясь их возрастом и неопытностью. Используют либо «в темную», либо убеждают несовершеннолетнего, что ему «ничего» не будет в силу возраста:

- используют в качестве курьера, то есть лица, которое приезжает и забирает наличные денежные средства у жертв мошенников;

- приобретают у несовершеннолетних банковские карты и сим-карты зарегистрированные на их имя, которые в дальнейшем используются при совершении преступлений и для обналичивания денежных средств, добытых преступным путем;

- несовершеннолетние часто используют найденные банковские карты, которыми расплачиваются в магазине, что в дальнейшем квалифицируется как кража денежных средств со счета.