Что представляет собой преступность в сфере информационно-телекоммуникационных технологий (далее – ИТТ)?

В современном обществе банковская система все больше уделяет внимание упрощающим жизнь человека высоким технологиям, активно внедряя их в различные операционные процессы для взаимодействия финансового учреждения с многочисленными клиентами. Наиболее популярны телефонные приложения «СбербанкОнлайн», «ВТБОнлайн» и прочие, с помощью которых можно в любое время суток осуществлять банковские операции, оплатив, например, через личный кабинет с помощью банковской карты любой товар в интернет-магазинах.

С развитием и внедрением в повседневную жизнь информационно-телекоммуникационных сетей и технологий, целью которых является обеспечение эффективного процесса сбора, обработки, хранения, предоставления и распространения информации по линиям связи, различные банки, осуществляющие операции на территории Российской Федерации, стали активно применять дистанционную систему обслуживания клиентов. Данные нововведения, с одной стороны, облегчили обмен полезной и значимой информацией, доступ клиентов к банковским услугам и операциям, с другой – стали использоваться в преступной деятельности, в том числе и в хищении денежных средств с банковских счетов граждан.

Злоумышленники, в свою очередь, не стоят на месте.

Что нужно знать и как действовать, чтобы не стать жертвой преступления, совершенного дистанционно с помощью ИТТ?

Применяйте эти простые правила:

- не сообщайте свои персональные данные, а также банковских карт и счетов третьим лицам, даже если неустановленное лицо представилось сотрудником банка, прекратите разговор и обратитесь в банк лично либо по телефону горячей линии;
- не выполняйте указания неизвестных лиц по вводу каких-либо команд и символов в телефонном режиме, а также с использованием банкомата;
- не перечисляйте денежные средства неизвестным лицам, представляющимся знакомыми ваших родных, сотрудниками правоохранительных органов (положите трубку и позвоните лицу, который по словам неизвестного попал в беду или нуждается в помощи);
- прежде чем приобретать какой-либо товар или услугу с использованием сети Интернет, ознакомьтесь с отзывами, оставленными ранее покупателями/клиентами;
- при вводе пин-кода банковской карты закрывайте его рукой, не стесняйтесь это делать, не храните пин-код совместно с банковской картой.

В современном обществе одним из самых распространенных видов преступлений является мошенничество, то есть хищение чужого имущества путем обмана или злоупотребления доверием, в том числе совершенное дистанционным способом с использованием информационно-коммуникационных технологий. Данный вид мошенничества совершается, как правило без физического контакта с потерпевшим.

Способы совершения хищения с использованием информационно-коммуникационных технологий постоянно совершенствуются, что создает определенные сложности для правоохранительных органов в раскрытии преступлений указанной категории.

Одним из самых распространенных видов хищения является телефонное мошенничество. Как правило, от имени сотрудников банков России, мошенники сообщают потерпевшему о несанкционированных списаниях денежных средств с банковских карт или сообщают о необходимой блокировке банковской карты. Далее, мошенники, войдя в доверие, просят предоставить определенные данные карты владельца или сообщить смс-код, поступивший на его телефон. В результате чего, как правило, происходит списание денежных средств с банковского счета.

Нужно помнить, что сотрудники банка при общении с клиентом банка никогда не просят сообщить ему реквизиты банковской карты.

Зачастую мошенники могут представиться сотрудниками полиции и сообщают о том, что близкие родственники задержаны за совершение преступления либо стали виновниками дорожно-транспортного происшествия, в результате которого погибли люди. Для того, чтобы родственник избежал наказания мошенник предлагает заплатить определенную сумму денег. В последнее время участились случаи, когда за денежными средствами приезжают курьеры, либо мошенники просят перевести денежные средства через платежный терминал.

Также, довольно распространенным способом мошенничества на сегодняшний день является мошенничество в социальных сетях. В данном случае мошенники с помощью взлома персональной страницы в социальных сетях обращаются от лица потерпевшего с просьбой о помощи, а именно о переводе денежных средств на банковский счет, либо просят реквизиты карт, чтобы перевести деньги.

Мошенничество через «Интернет-магазин» – еще один способ обмана. Преступники берут с будущей жертвы предоплату или полную сумму за определенный товар, но не исполняют своих обязательств. Благодаря фальшивых интернет-сайтов, мошенники собирают реквизиты банковских карт потерпевших и далее используют для операций по обналичиванию денежных средств.

Будьте внимательны и осторожны при общении с посторонними лицами.

Ускоренное внедрение цифровых технологий в жизни общества помимо положительных аспектов, имеет и негативную (криминогенную) сторону.

Информационно-телекоммуникационные технологии преимущественно используются при совершении преступлений против собственности, а также в сфере незаконного оборота наркотических средств и психотропных веществ. Уязвимость внедряемых в финансово-кредитную сферу инновационных технологий и их активное применение на практике эксплуатируют мошенники, совершая посягательства на имущество граждан и организаций на принципиально новой высокотехнологичной основе.

Какие существуют меры в борьбе с преступностью в сфере ИТТ?

Государство на законодательном уровне реагирует на сложившуюся обстановку. Усилено наказание за хищение денежных средств с банковского счета или электронных денежных средств до 6 лет лишения свободы. При этом уголовная

ответственность наступает не только за совершение хищений с использованием банковских карт (их реквизитов и контрольной информации), но и иных электронных средств платежа («электронные кошельки», другие платежные сервисы).

Принятие Федерального закона от 27 июня 2018 г. № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» и запуск автоматизированных систем Банка России расширили возможности кредитных организаций по выявлению и блокированию транзакций, имеющих признаки перевода денежных средств без согласия клиента, и возмещению ущерба от них.

В интегрированный банк данных федерального уровня (ИБД-Ф) Главного информационно-аналитического центра МВД России введен в эксплуатацию модуль «Дистанционное мошенничество». Анализ содержащейся в базе данных информации свидетельствует о возможности установить сведения о причастности уличенного в совершении преступления лица к совершению иных преступлений в сфере ИТТ с использованием им тех же номеров телефонов, банковских карт, адресов используемых сайтов и т.д. Таким образом, при установлении лица, совершившего хотя бы один преступный эпизод с использованием тех же средств, возможно отследить и иные совершенные им преступления в любом регионе страны.

Что стоит учитывать?

В ходе противодействия данному виду преступности органы внутренних дел сталкиваются с рядом проблем. К ним, во-первых, следует отнести длительные сроки исполнения запросов по предоставлению информации со стороны операторов сотовой связи и IT-телефонии, кредитно-финансовых учреждений, администраций социальных сетей, что затрудняет проведение расследования и получения данных, способствующих раскрытию преступлений. Во-вторых, использование злоумышленниками IP-телефонии, программного обеспечения, позволяющего избежать или существенно затруднить идентификацию абонента – VPN, TOR и технологий, позволяющих создавать динамические или нераспознаваемые IP-адреса. А также использование значительного количества транзакций похищенных денежных средств и различных схем их вывода. Кроме того, зачастую при совершении преступлений используются банковские карты, эмитентом которых являются иностранные финансовые организации, что затрудняет получение сведений о держателе карты и движении денежных средств по ней.

Иногда банки дают ответы о невозможности предоставления информации о перечислении денежных средств с расчётного счёта потерпевшего, в связи с тем, что банк предоставляет держателям карт услугу «Перевод с карты на карту» посредством сайта банка в сети Интернет и может предоставить только данные о первых шести и последних четырёх цифрах карт, осуществляющих переводы. Некоторые кредитные учреждения указывают на то, что банк не располагает сведениями о владельце карты и о движении денежных средств по ней, так как данная информация банку не предоставлена и неизвестна.

Таким образом, чтобы совершить преступление, злоумышленник, используя современные технологии, в среднем затрачивает около пяти минут, а чтобы

сотрудникам правоохранительных органов получить необходимую информацию в целях раскрытия преступления и возмещения ущерба потерпевшему, затрачивается времени от месяца и более.

Например, до месяца может длиться процедура наложения ареста на счета подозреваемых (обвиняемых).

Таким образом, результативность противодействия хищениям, совершённым дистанционным способом, зависит не только от способности правоохранительных органов раскрывать уже совершённые преступления, но и от профилактических мер общего и индивидуального характера.

Поэтому важно помнить – предупрежден, значит защищен. Нужно стараться не давать возможности мошенникам воспользоваться финансовой неграмотностью населения.