**О способах хищения денежных средств граждан с использованием информационно-коммуникационных технологий.**

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели, в том числе, личное обогащение.

В Российской Федерации отмечается ежегодный рост таких преступлений. Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий.

Подавляющее большинство анализируемых хищений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей для общения с потерпевшими (сотовой связи, ресурсов сети Интернет). Технология основана на использовании психологических слабостей человека и является достаточно эффективной. Например, преступник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке.

Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками органа правопорядка.

Дистанционные хищения совершаются посредством размещения на открытых сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица.

Денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны с установленными на них банковскими сервисами. То же самое касается и банковских карт: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – деньги снимаются в банкоматах.

Так называемый фишинг - тоже техника «социальной инженерии», направленная на получение конфиденциальной информации. Обычно злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо – от банка или платежной системы – требующее «проверки» определенной информации, или совершения определенных действий. Это письмо, как правило, содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.

Социальная инженерия используется также для распространения троянских коней: эксплуатируется любопытство, либо алчность объекта атаки. Злоумышленник направляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Также это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Такая техника остается эффективной, поскольку многие пользователи, не раздумывая кликают по любым вложениям или гиперсылкам. Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей, испытывающих сложности при освоении современной техники, а также страдающих излишней доверчивостью.

Преступники реализуют множество других способов и инструментов для завладения чужими деньгами: используют дубликаты сим-карт потерпевших, а также устройства-скиммеры, считывающие информацию, содержащуюся на магнитной полосе банковской карты для последующего изготовления ее дубликата. Рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами одолжить деньги, внедряют вредоносные ПО в системы юридических лиц, похищают электронные ключи и учетные записи к нему в офисах организации и т.д.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные IT-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети.

Для создания препятствий правоохранительным органам для раскрытия подобных преступлений злоумышленники: меняют сотовые телефоны, места своего нахождения; оформляют сим-карты и открывают счета в банках на подставных лиц; используют анонимные электронные кошельки и предоплаченные банковские карты, Proxy-серверы и различные программы, скрывающие фактические IP-адрес и место нахождения, привлекают лиц, не осведомленных о противоправности их действий, применяют другие способы конспирации. Это касается не только хищений, но и преступлений в сфере компьютерной информации. При этом данные преступления носят скоротечный, многоэпизодный (серийный), и трансграничный характер.

В целях пресечения указанных видов преступлений просим всех быть предельно внимательными при осуществлении банковских операций с использованием сети «Интернет» и мобильных телефонов. Не поддавайтесь на уловки мошенников и всегда перепроверяйте полученную информацию.

О.Н. Еланкова