**Как защитить себя от хищений, совершаемых посредством телекоммуникационных технологий?**

В условиях тенденций развития современных технологий все большее распространение получают хищения, совершаемые с использованием сотовой связи, сети «Интернет» и иных инновационных средств телекоммуникации.

С учетом анализа следственно-судебной практики специалисты в области защиты компьютерной информации рекомендуют соблюдать ряд правил для обеспечения безопасности себя и своих близких от действий злоумышленников.

В первую очередь, никогда и ни при каких обстоятельствах не следует передавать такие конфиденциальные данные, как логин, пароль или реквизиты вашей банковской карты (код безопасности, имя владельца, срок действия) и персональный идентификационный номер (ПИН-код).

Рекомендуется минимизировать или исключить использование «зарплатных» карт для расчетов в магазинах и оплаты интернет-покупок. Для этих целей лучше применять банковские карты с высокой степенью защиты. Деньги целесообразно хранить на лицевом счете либо устанавливать суточные лимиты на все виды совершаемых операций.

Для «обналичивания» и иных финансовых операций брать за правило использовать банкоматы, расположенные внутри банковских отделений или на охраняемых территориях, оборудованных системами видеонаблюдения.

С пристальным вниманием относитесь к сообщениям, в которых вас просят перейти по неизвестной ссылке на электронном ресурсе. Проверьте, нет ли этой страницы в сети «Интернет» в списке подозрительных.

Если на интернет-сайте вам предлагается повторно авторизоваться (подтвердить персональные данные, ввести пароль доступа), обязательно проверяйте адресную строку – на том ли сайте вы находитесь.

Старайтесь пользоваться актуальными версиями программного обеспечения, установленными на вашем устройстве. Не пренебрегайте антивирусными приложениями.

По возможности не заходите в онлайн-банки и другие подобные сервисы через открытые беспроводные локальные сети (Wi-Fi-сети), поскольку увеличивается риск попадания конфиденциальной информации к мошенникам, подменяющим адреса сайтов на уровне подключения и перенаправляющих пользователей на поддельные страницы.

Обнаружив фишинговую операцию (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям), обязательно сообщите о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки социальной сети (если такие ссылки рассылает кто-то из пользователей), а также в правоохранительные органы.

Не забывайте, что кредитные организации не рассылают сообщения о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов.

Будьте предельно осторожны, если кто-то связывается с вами с предложением малорискованных и высокоприбыльных инвестиций. Велика вероятность, что это мошенники, которые, как правило, настаивают на немедленном вложении денег, гарантируют необоснованно высокий доход, обещают отсутствие финансового риска.

С пристальным вниманием относитесь к сообщениям с просьбами предоставить личную или финансовую информацию.

Проверяйте сообщения, которые рекламируют ваши высокие шансы выиграть в лотерею или указывают на то, что вы уже стали победителем. Злоумышленники могут утверждать, что нужно отправить деньги на оплату «налогов», «сборов» или «таможенных платежей», прежде чем выслать вам ваш выигрыш.

Имейте в виду, что фальшивые письма и сайты нередко повторяют дизайн подлинных, но соответствующие ссылки на электронные адреса (гиперссылки), вероятнее всего, являются неправильными и содержат ошибки.

В случае же если вы стали жертвой такого преступления, как можно скорее обратитесь в органы полиции, примите меры к блокированию счета, с которого произошло неправомерное списание денежных средств, и информированию соответствующего кредитного учреждения.

Для надлежащей реализации вашего права на защиту от преступных посягательств следует знать следующее.

Заявления и сообщения о преступлениях подлежат обязательному приему во всех территориальных органах МВД России вне зависимости от места и времени их совершения, а также полноты содержащихся в них сведений и формы представления.

Подать заявление гражданин может в любом удобном для себя виде: письменно или устно, по телефону, в электронной форме по информационным системам общего пользования, в дежурной части или на приеме у руководства территориального подразделения органа внутренних дел.

Вне служебных помещений прием информации о преступлениях и происшествиях обязаны осуществлять все сотрудники полиции, находящиеся при исполнении служебных обязанностей.

При этом они не вправе отказаться от приема заявления по основанию того, что обслуживают другую территорию либо представленные сведения недостаточны для решения вопроса о наличии признаков преступления, а также по иным причинам. Поступившее к ним сообщение о преступлении они обязаны передать в дежурную часть для регистрации.

Любое заявление должно быть подписано и из него четко должно прослеживаться, кто его автор, то есть указаны фамилия заявителя и его почтовый или электронный адрес.

Если сообщение о происшествии поступило в орган внутренних дел при личном обращении заявителя, то оперативный дежурный обязан не только зарегистрировать его, но и, что важно, оформить специальный письменный документ – талон-уведомление.

В нем указываются: сведения о заявителе, краткое содержание сообщения о происшествии, регистрационный номер, фамилия и подпись сотрудника, принявшего сообщение, дата приема. Заявитель расписывается о получении талона-уведомления, с указанием даты и времени.

Особенностью преступлений в сфере информационно-телекоммуникационных технологий является их трансграничный характер. Потерпевший и злоумышленник, как правило, незнакомы, могут проживать и находиться в различных городах и даже странах.

Зачастую это не позволяет своевременно и однозначно определить точное место их совершения, что используют недобросовестные сотрудники правоохранительных органов, которые вместо проведения доследственной проверки, раскрытия преступления и пресечения действий виновного лица, начинают многократно и зачастую необоснованно передавать это заявление от одного территориального органа другому.

Такой подход недопустим, поскольку отрицательно сказывается на соблюдении разумных сроков уголовного судопроизводства, приводит к утрате доказательств и усложняет ход расследования.

В случае подобного отношения к рассмотрению сообщения о преступлении, а также иных фактов бездействия полиции обращайтесь за защитой нарушенных прав в прокуратуру.

Заместитель прокурора

Чердаклинского района В.С. Корухов