

«Станьте инвестором!», «Ваши счета подвергнуты атаке!» способы совершения хищений денежных средств с банковских счетов граждан становятся все более разнообразными.

Как свидетельствуют материалы уголовных дел, практически каждый из обманутых знал о методах совершения кибермошенничества. Так почему же обладая информацией о применяемых мошенниками уловках, потерпевшие безропотно передавали сведения о пин-кодах карт, паролях к личным кабинетам и переводили деньги на счета посторонних людей.

Основной инструмент мошенников – это социальная инженерия, то есть воздействие на эмоции и чувства людей с целью заставить совершить необходимые для преступников действия.

Мошенники отлично владеют психологическими приемами и навыками, а располагая сведениями о личных данных граждан, которые легко установить благодаря социальным сетям и разнообразным базам данных, входят в доверие и похищают огромные суммы денег.

Кроме того, приемы совершения преступлений постоянно изменяются. Знать о наиболее распространенных способах и своевременно пресекать какой-либо контакт с мошенниками – верный способ защитить свои финансы.

Анализ преступлений, совершенных в отношении жителей Кяхтинского района, позволяет выделить наиболее распространенные схемы.

С «заботой» о Ваших деньгах

Мошенники звонят под видом работников банка, службы безопасности кредитных организаций, правоохранительных органов и сообщают о совершении сомнительных операций по счету либо кибер-атаке. Для обеспечения сохранности денег просят перевести их на безопасный счет, сообщить пароли и пин-коды или установить мобильное приложение.

Как защититься?

Сотрудники банка и работники полиции никогда не просят сообщить по телефону подобную информацию, тем более не используют для осуществления звонков чаты и мессенджеры. Не стоит вступать в перепалку с мошенниками, пытаться самостоятельно их разоблачить. Следует сразу же прервать звонок и обратиться лично в банк или полицию.

Оформление кредита в мобильном приложении

Сомнительные сайты, ссылки, при переходе на которые мошенники могут завладеть информацией о личных данных потерпевших, разнообразные

приложения, которые могут дублировать широко распространенные официальные приложения. Такой вид мошенничества особенно опасен тем, что мошенники могут завладеть не только средствами, находящимися на счете клиента, но и заемными средствами, размер которых может достигать сотни тысяч рублей.

Как защититься?

Никогда не устанавливайте сомнительные мобильные приложения и не сообщайте какие-либо пароли посторонним.

Совершение сделок на интернет-сайтах.

Такой вид мошенничества связан с обещанием совершить определенные действия, например, трудоустроить на вахту, продать какой-то товар, помочь с написанием диплома или курсовой работы.

Намерения мошенников сводятся к одному – убедить потерпевшего в своей благонадежности и возможности возврата денег в любой момент. Кроме того, при совершении таких преступлений злоумышленники зачастую завладеваю персональными данными граждан, которые добровольно пересылают копии паспортов, трудовых книжек, и в дальнейшем используют их для оформления кредитов и займов.

Как защититься?

Проверять добродорядочность объекта, разместившего объявление, например, искать отзывы и комментарии других пользователей.

Выгодное вложение денег, инвестиции и игра на фондовом рынке.

Ежедневно в сети появляются новые предложения о возможности дополнительного заработка, в том числе путем осуществления инвестиций, покупки и продажи акций известных компаний. Мошенники обещают гарантированный заработок, возможность получения пассивного дохода. Более того, злоумышленники в подтверждение будущих гонораров могут даже переводить небольшие суммы денег в виде первоначальной прибыли, тем самым подсаживая на удочку.

Как защититься?

Не забывать, что бесплатный сыр бывает только в мышеловке. Без наличия минимальных познаний в финансовой сфере нельзя полагаться на добрую волю неизвестных брокеров и инвесторов.