****

# ПРОКУРАТУРА

# СТАВРОПОЛЬСКОГО КРАЯ

# прокуратура Петровского района

«О мерах по предупреждению хищений денежных средств»

Случаи телефонного мошенничества происходят все чаще, а схемы преступных действий становятся все более продуманными и изощренными, появляются новые и эволюционируют старые. Зачастую мошенники используют психологические манипуляции, в ход идут различные речевые уловки, чтобы усыпить бдительность жертвы и управлять ее действиями.

Это могут быть попытки использовать эффект внезапности, чувство опасности, некоторые мошенники могут высказывать угрозы. Пользователи, в силу свойств нормальной обывательской психологии, чаще всего оказываются готовы слушать тех, кто предлагает им обезопаситься и защитить свои счета. На этом и строят свои схемы мошенники. Для них важно, чтобы лицо было дезориентировано и как можно менее внимательно, поэтому они всегда настойчивы и терпеливы.

Распространены случаи направления сообщений в социальных сетях и мессенджерах с реальных аккаунтов, принадлежащих знакомым адресатов, с просьбой перейти на определенный сайт по прилагаемой ссылке (проголосовать за ребенка либо родственника, участвующего в конкурсе), что в последующем приводит к взлому аккаунта, получению доступа к содержимому телефона или компьютера, данным банковских карт и, как следствие, хищению денежных средств как у владельца телефона (компьютера), так и у лиц, данные и номера телефонов которых содержатся в памяти его электронного устройства. Таким же способом зачастую рассылаются сообщения от знакомых и коллег с просьбами о предоставлении взаймы денежных средств или оказании иной финансовой помощи.

Подобные факты следует рассматривать как потенциальную угрозу хищений личных денежных средств.

Обезопасить себя возможно следующими способами:

– не отвечать на звонки с незнакомых номеров, текстовые сообщения, в особенности с неместными кодами телефонного номера, и «короткие» звонки (когда после нескольких гудков мошенник прекращает вызов в ожидании того, что жертва ему перезвонит сама);

– не поддаваться на провокации, требующие быстрого реагирования, и не совершать необдуманных действий;

– в зависимости от сообщаемых обстоятельств и просьб следует перепроверить достоверность данных или полученной информации: позвонить в банк, мобильному оператору, членам семьи, родственникам, знакомым, руководителям;

– не передавать реквизиты банковских карт, пароли от них; – не отправлять коды из SMS-сообщений, которые приходят на телефон с неизвестных номеров;

– в случае поступления на счет денежных средств от незнакомого лица незамедлительно обратиться в отделение банка для отмены данной транзакции и подать заявление о возвращении поступившей суммы на счет отправителя.