**ПРОКУРАТУРА РАЗЪЯСНЯЕТ:**

**«О мерах по предупреждению хищений денежных средств»**

Развитие информационных технологий и сервисов мобильной связи, направленные на облегчение повседневной жизни, в то же время упрощают способы обмана и хищения денежных средств. От пользователей требуется принятие более надежных способов защиты от мошенничества.

Основным источником опасности по-прежнему остаются вредоносные программы - вирусы, которые с развитием сетевых технологий получили новую среду для своего распространения.

В последнее время развитие получил вирус «Mamont», который рассылается пользователям мессенджера Telegram под видом различных фалов, как правило видео (фото) с подписью «Это ты?». После перехода по ссылке (открытии соответствующего файла) происходит хищение личных данных пользователя и рассылка аналогичных спам-сообщений от имени владельца телефона.

Так, в текущем году после перехода работником прокуратуры по подобной ссылке мошенники завладели его персональными данными, в том числе получили доступ к его личному кабинету в автоматизированном портале государственных услуг (Госуслуги). В дальнейшем злоумышленники от имени работника заключили кредитный договор с микрокредитной организацией, в результате чего совершили хищение денежных средств.

С учетом изложенного, необходимо принять меры по недопущению подобных фактов, не переходить по ссылкам, полученным из различных подозрительных источников, независимо от уровня доверия к ним. Как правило, такие ссылки содержат недосказанные сообщения, которые провоцируют интерес и любопытство.

Кроме того, рекомендую принять меры по обеспечению безопасности своих персональных данных, содержащихся в личном кабинете Госуслуг:

- отключить доступ к сервисам Госуслуг иных установленных на телефоне приложений и программ; Руководителям структурных подразделений аппарата прокуратуры области Городским, районным, специализированным прокурорам - не использовать функцию автосохранения паролей и при каждом запуске сервиса самостоятельно вводить пароль;

- во вкладке «Безопасность» приложения настройте вход с дополнительным способом подтверждения - кодом из СМС. Такой вход позволяет защитить ваши данные на всех сайтах, куда можно войти по логину и паролю от Госуслуг;

- по вышеуказанному пути подключите уведомления о входе на электронную почту. Вы будете получать письмо каждый раз, когда кто-то входит в вашу учётную запись, в том числе вы сами. Это позволит быстро узнать о взломе, если он произошёл без вашего участия.