Отвечая на поставленные вопросы, следует отметить, что мошенники умело пользуются малой информированностью участников СВО, а также сложной морально-психологической ситуацией родственников, у которых отсутствует прямая связь с военнослужащими.

Высокая концентрация денежных средств и значительность сумм единовременных выплат является привлекательной для злоумышленников мишенью.

Анализ уголовных дел показывает, что ***действия злоумышленников по обману участников СВО и их близких можно разделить на следующие популярные способы:***

1. Злоумышленники создают каналы в мессенджере Telegram, визуально похожие на официальные группы, посвященные помощи семьям военнослужащих, в которых регулярно публикуют сведения о пропавших военнослужащих, их фотографии, а также PDF- и Excel- файлы с персональными данными.

В те же каналы начинают позднее загружать вредоносное программное обеспечение (например APK-файлы, содержащие банковский «троян» Mamont для операционной системы Android).

Используя данный «вредонос» злоумышленники получают полный контроль над устройством жертвы, могут собирать о нем информацию, перехватывать и отправлять СМС, получить доступ к пользовательским контактам и т.д., а также банковским приложениям и мессенджерам.

В целях безопасности необходимо отключить автозагрузку в Telegram, проверять формат документов.

2. Помощь в оформлении выплат, как способ войти в доверие.

Так, в сентябре текущего года возбуждено уголовное дело по факту мошенничества в отношении вдовы участника специальной военной операции.

Инцидент начался с телефонного звонка, в ходе которого неизвестный поинтересовался, получала ли женщина причитающиеся ей выплаты и награду погибшего супруга.

После отрицательного ответа злоумышленник предложил оформить необходимые документы через портал «Госуслуги» и под предлогом оказания помощи запросил у нее код подтверждения из СМС-сообщения.

Впоследствии, лже-сотрудник правоохранительных органов обвинил женщину в соучастии в мошеннической деятельности и пригрозил уголовным преследованием. Под давлением мошенников жертва передала все имеющиеся денежные средства неизвестному курьеру, прибывшему по ее месту жительства.

В целях безопасности:

- никому и никогда не передавайте коды из СМС-сообщений;

- не переходите по ссылкам из сообщений и не устанавливайте программное обеспечение из непроверенных источников;

- разумно подходите к публикации в социальных сетях личной информации, так как она может стать информацией, необходимой мошеннику для создания сценария обмана.

3. Мошенники звонят или пишут своим потенциальным жертвам и сообщают, что из их денежного довольствия будет удержано 195 000 рублей – размер единовременной выплаты, которая причитается военным в соответствии с указом Президента РФ. Причина – дисциплинарное взыскание. Для большей убедительности мошенники направляют в мессенджер «копию выписки» якобы из приказа Департамента финансового обеспечения Минобороны России.

Чтобы денежные средства не были списаны, мошенники предлагают военнослужащему или его родным перевести все накопления якобы на «безопасный счет». Получив деньги жертвы, телефонные аферисты исчезают.

Как себя обезопасить:

- если Вам поступил подозрительный звонок, прервите разговор, положите трубку;

- не забывайте, что «безопасных счетов» не существует;

- по всем вопросам, связанным с денежными средствами, обращайтесь в свой банк самостоятельно.

4. «Хищение денежных средств с банковских счетов военнослужащих, в том числе получивших ранение или погибших в зоне проведения СВО».

Военнослужащие хранят свои банковские карты в открытых местах, сохранность личных вещей ими никак не обеспечена.

В результате этого каждый может получать доступ к их вещам, что ведет в дальнейшем к хищению денежных средств.

Ярким примером может послужить совершенное в декабре 2024 года хищение денежных средств с банковского счета одного из военнослужащих, который погиб в зоне проведения СВО, в общей сумме более 2 млн рублей.

Похищенные денежные средства обналичены неустановленными лицами в декабре 2024 года через банкоматы, расположенные в Луганской Народной Республике. О хищении денежных средств, в том числе суммы единовременной выплаты за гибель, мать погибшего узнала при вступлении в наследство.

Аналогичным способом похищены денежные средства в общей сумме более 1 млн рублей с банковского счета еще одного из военнослужащих, который получил ранение в зоне проведения СВО и находился на лечении.

Во всех этих случаях вывод похищенных денежных средств мошенниками осуществляется путем несанкционированного доступа к банковским счетам военнослужащих посредством утраченных ими мобильных телефонов с установленными в них мобильными приложениями банков и выманенных у жертвы реквизитов карты, CVV-кодов, паролей из SMS и кодов из push-уведомлений.

Как подготовиться к такой ситуации заранее:

- не носите с собой банковские карты, оставьте их в безопасном месте;

- не храните вместе с банковской карты ПИН-код;

- включите все уведомления (СМС и Push- уведомления) на Все операции по карте;

- помните, что мобильный телефон с банковским приложением может быть также Вами утерян;

- установите лимиты на снятие наличных, на безналичную оплату и онлайн-платежи на комфортный для Вас уровень (к примеру, 5 000 рублей в день). Сделать это можно в мобильном приложении банка;

- используйте виртуальную карту для онлайн-платежей.

В целях безопасности после обнаружения утери банковской карты:

- откройте мобильное приложение банка и выберите опцию «Заблокировать карту»;

- если нет доступа к приложению, немедленно позвоните на горячую линию банка по номеру телефона, указанному на официальном сайте.

Подобные преступления находятся на особом контроле у правоохранительных органов. По фактам хищений возбуждаются уголовные дела, и виновные несут суровые наказания. Однако проблема требует комплексного решения, включающего как технические меры защиты, так и повышение финансовой грамотности населения.

Одновременно, в целях противодействия совершения отмеченного вида преступлений, будем признательны за участие в распространении среди военнослужащих и членов их семьи дополнительной информационно-профилактической продукции, наиболее приемлемыми и легкоусвояемыми формами восприятия которой являются просмотр фото и видеоконтента на различных интернет-площадках, социальных сетях и средствах массовой информации, а также проведение очных лекций в коллективах.

Рекомендуется использовать рубрику сайта Следственного департамента МВД России «Профилактика мошенничества». В разделе «Новости» размещено 353 информационных сообщений о дистанционных хищениях.

Также соответствующие профилактические материалы и видеоконтенты содержатся на ресурсах, посвященных недопущению преступлений в отношении граждан, ознакомиться с которыми можно по ссылкам:

https://мвд.рф/вопросы/мошенник и https://мвд.рф/news/rubric/17 *(официальные интернет-сайты МВД России)*;

https://мвд.рф/Videoarhiv/Socialnaja_reklama/вбезопасности/item/55246013/

https://мвд.рф/Videoarhiv/Socialnaja_reklama/вбезопасности/item/54619404/

https://мвд.рф/Videoarhiv/Socialnaja_reklama/вбезопасности/item/5461707

(видеоконтенты: «рекомендации для граждан о навыках безопасности при использовании банковских карт, интернет-банкинга, банкоматов», «звонок от «оператора сотовой связи», «звонки от сотрудников государственных органов», «что такое фейковые QR-коды и как этим пользуются мошенники?»);

https://мвд.рф/mvd/structure1/Upravlenija/убк/информация-для-граждан *(официальный интернет-сайт УБК МВД России)*;

https://t.me/cyberpolice_rus *(официальный телеграм-канал УБК МВД России)*;

https://www.kaspersky.ru/ *(официальный интернет-сайт компании «Лаборатория касперского»)*;

https://www.securitylab.ru/ *(информационный портал по безопасности)*;

https://ligainternet.ru/ (официальный *интернет-сайт компании «Лига безопасного интернета»)*;

https://t.me/internetinsafe *(официальный телеграм-канал компании «Лига безопасного интернета»)*.

Одновременно предоставляются ссылки:

https://okko.tv/serial/na-krjuchke-592260973 *(профилактический российский сериал 204 года «На крючке», который полезно посмотреть даже тем, кто уверен, что никогда не попадется на уловки мошенников)*;

https://www.kinopoisk.ru/film/1316625/ *(корейский фильм «Грязные миллионы» о телефонном мошенничестве)*.

Следственный департамент МВД России