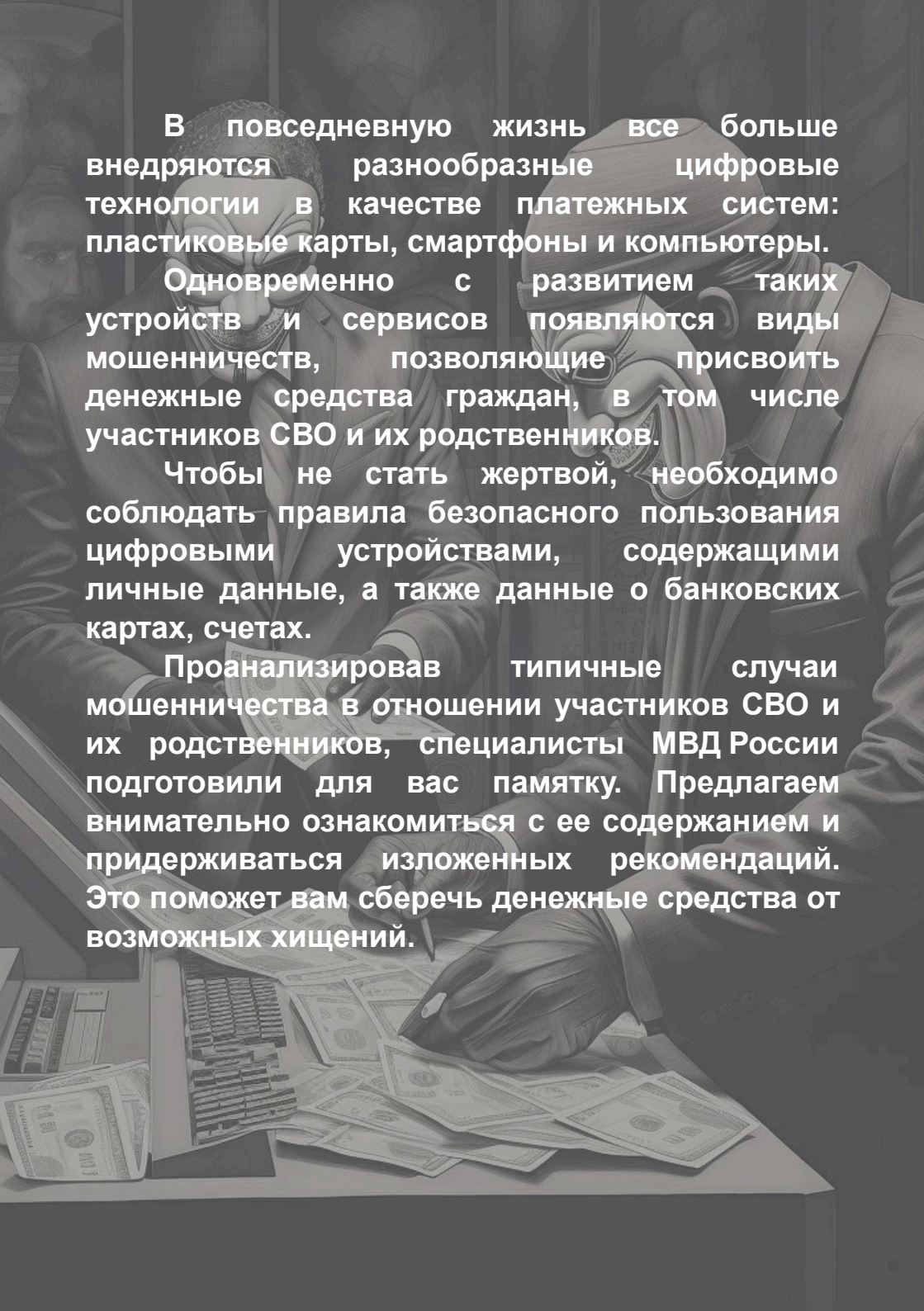


ПАМЯТКА
о возможных видах и способах мошенничества и порядке обеспечения личной финансовой безопасности (для участников СВО)



В повседневную жизнь все больше внедряются разнообразные цифровые технологии в качестве платежных систем: пластиковые карты, смартфоны и компьютеры.

Одновременно с развитием таких устройств и сервисов появляются виды мошенничеств, позволяющие присвоить денежные средства граждан, в том числе участников СВО и их родственников.

Чтобы не стать жертвой, необходимо соблюдать правила безопасного пользования цифровыми устройствами, содержащими личные данные, а также данные о банковских картах, счетах.

Проанализировав типичные случаи мошенничества в отношении участников СВО и их родственников, специалисты МВД России подготовили для вас памятку. Предлагаем внимательно ознакомиться с ее содержанием и придерживаться изложенных рекомендаций. Это поможет вам сберечь денежные средства от возможных хищений.

SMS С ПРОСЬБОЙ О ПОМОЩИ УЧАСТНИКАМ СВО

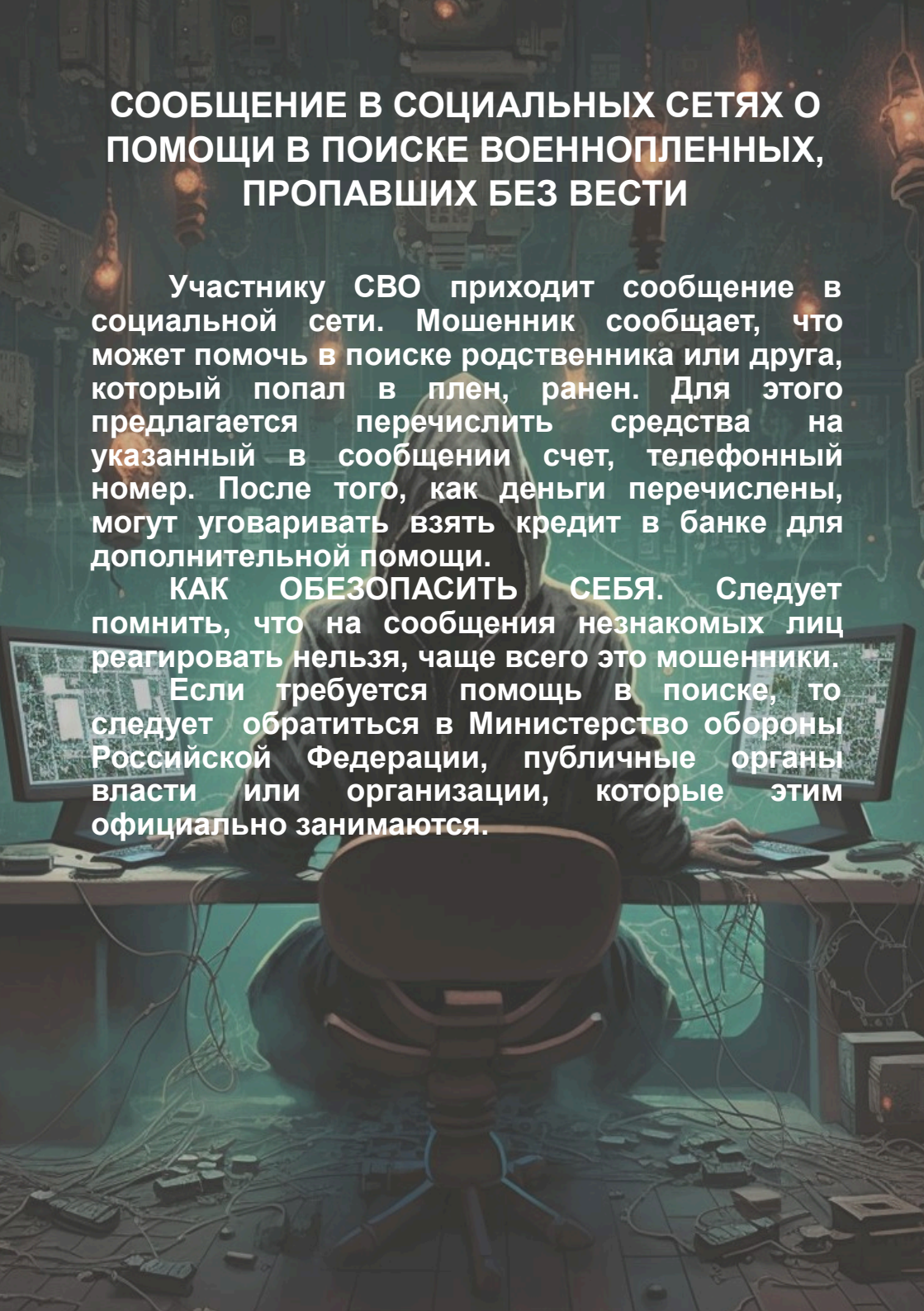
Абонент получает на мобильный телефон сообщение: «Хотите помочь участникам специальной военной операции? Перечислите средства, отправив SMS на короткий номер».

КАК ОБЕЗОПАСИТЬ СЕБЯ. Следует помнить, что по общему правилу на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

Если хотите оказать материальную помощь участникам СВО, то действуйте так:

найдите в официальном источнике – на сайте, на страничке в соцсетях или в телеграм-канале, данные об организации оказывающей помощь участникам СВО;

проверьте подлинность данных о деятельности организации. Для этого ознакомьтесь с отзывами о ее работе, перезвоните по контактному телефону и уточните цели организации, порядок оказания помощи участникам СВО, реквизиты для перечисления денежных средств. Например, на сайте проекта «Все для победы» Народного Фронта указан номер 3030 для абонентов Tele2 и Ростелеком Бизнес, на который можно отправлять СМС с суммой пожертвования.



СООБЩЕНИЕ В СОЦИАЛЬНЫХ СЕТЯХ О ПОМОЩИ В ПОИСКЕ ВОЕННОПЛЕННЫХ, ПРОПАВШИХ БЕЗ ВЕСТИ

Участнику СВО приходит сообщение в социальной сети. Мошенник сообщает, что может помочь в поиске родственника или друга, который попал в плен, ранен. Для этого предлагается перечислить средства на указанный в сообщении счет, телефонный номер. После того, как деньги перечислены, могут уговаривать взять кредит в банке для дополнительной помощи.

КАК ОБЕЗОПАСИТЬ СЕБЯ. Следует помнить, что на сообщения незнакомых лиц реагировать нельзя, чаще всего это мошенники.

Если требуется помощь в поиске, то следует обратиться в Министерство обороны Российской Федерации, публичные органы власти или организации, которые этим официально занимаются.

СООБЩЕНИЕ ОБ ОФОРМЛЕНИИ КРЕДИТА

Участнику СВО поступает звонок от фальшивого сотрудника службы безопасности банка или сотрудника правоохранительных органов с сообщением о том, что мошенники оформили на его имя кредит. Чтобы не платить по чужим долгам, участнику СВО предлагают срочно оформить такой же кредит самому (встречный заем), а денежные средства обналичить и перевести на так называемый безопасный или расчетный счет или передать третьим лицам.

КАК ОБЕЗОПАСИТЬ СЕБЯ. Необходимо помнить, что любой подобный звонок – дело рук мошенников. Службы безопасности банков и сотрудники правоохранительных органов никогда не звонят гражданам с сообщениями о необходимости взять кредит и перевести деньги на «безопасный» или «резервный» счет. При поступлении подобных звонков следует повесить трубку и перезвонить по телефону, указанному на обратной стороне банковской карты. Надо помнить: понятий «безопасный» или «резервный» счет, «встречный заем» не существует.

ПРЕДЛОЖЕНИЕ СКАЧАТЬ НА МОБИЛЬНЫЙ ТЕЛЕФОН (ИСПОЛЬЗУЕМЫЙ ДЛЯ ПОКУПОК ИЛИ ОПЛАТЫ) ПРОГРАММУ ДЛЯ УДАЛЕННОГО ДОСТУПА БАНКА К ГАДЖЕТУ

Участнику СВО поступает телефонный звонок или приходит сообщение от фальшивого сотрудника банка с предложением скачать на мобильный телефон (используемый для покупок или оплаты) программу для удаленного доступа банка к гаджету, чтобы защитить его от взлома, либо для проверки безопасности действующего (установленного) банковского приложения «онлайн -банк». Такая программа предоставляет мошенникам полный доступ к телефонной книге, мобильным банкам и другим личным данным, которые для вашего удобства хранятся в памяти гаджета.

КАК ОБЕЗОПАСИТЬ СЕБЯ. Чтобы не оказаться жертвой мошенников необходимо помнить следующее:

любой подобный звонок должен насторожить. Банк никогда не просит клиента устанавливать программы на телефон;

нельзя устанавливать на телефон неизвестные мобильные приложения!

Среди них могут оказаться как вирусные программы, так и сервисы по удаленному управлению телефоном. Если к нему подключены системы дистанционного управления финансами, данные вредоносные программы получат доступ к ним и к финансовым сбережениям. Чтобы обезопасить себя, не следует переходить по сомнительным ссылкам в SMS и MMS-сообщениях, устанавливать программы, назначение которых не понятно. Следует использовать лицензионное антивирусное программное обеспечение!

ТЕЛЕФОННЫЙ ЗВОНОК ПОКУПАТЕЛЯ

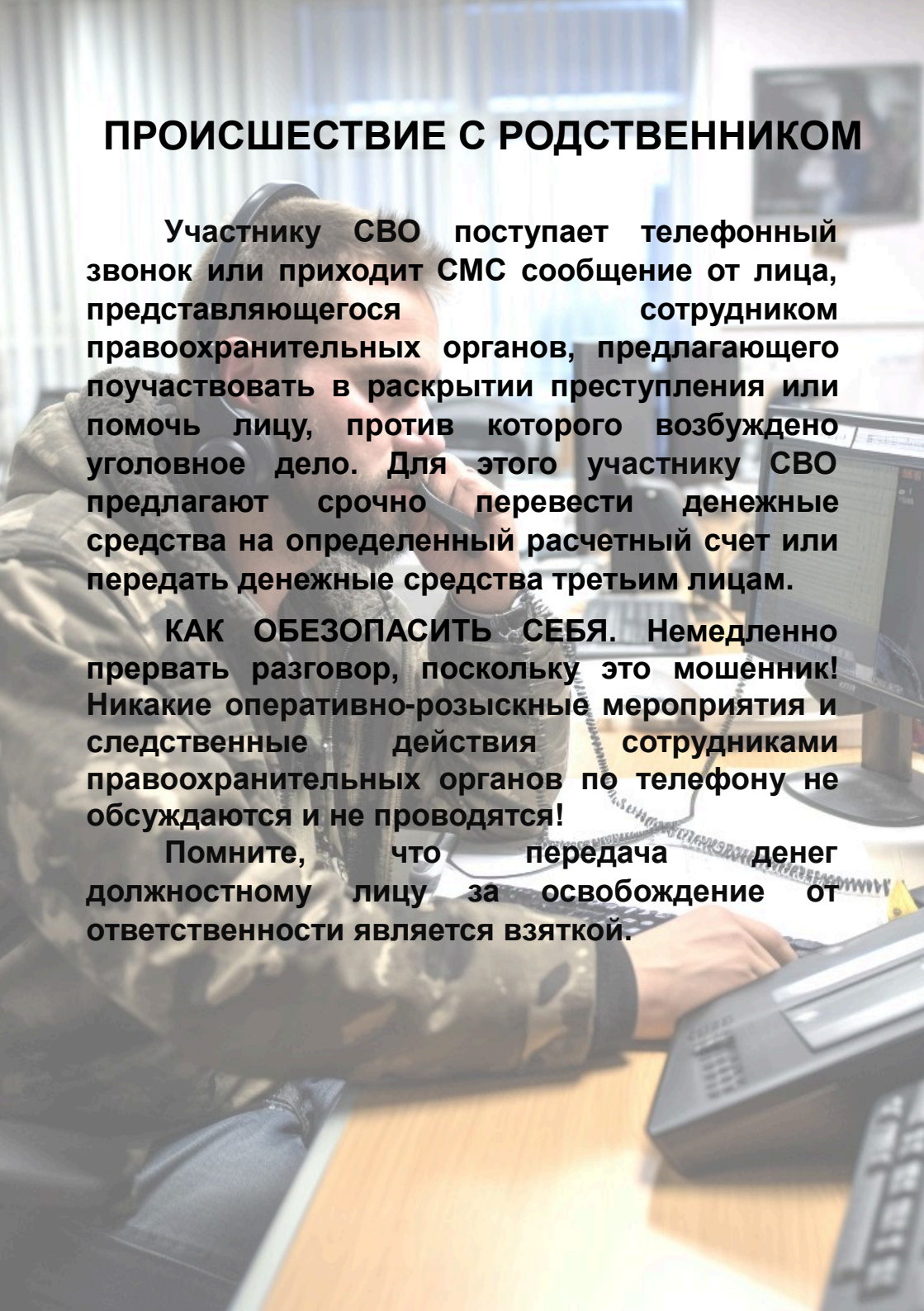
Участник СВО является владельцем объявления, размещенного в сети Интернет о продаже имущества. Ему звонит «потенциальный» покупатель, готовый оплатить товар, не торгуясь, но исключительно на банковскую карту. Для этого он просит сообщить ее номер, срок действия, ПИН-код; пароли, секретные коды из сообщений банка о проведенной операции.

КАК ОБЕЗОПАСИТЬ *СЕБЯ.* Немедленно прервать разговор, поскольку это мошенник! Покупатель не будет интересоваться данными банковской карты и кодами.

SMS ИЛИ ЗВОНОК ИЗ БАНКА О БЛОКИРОВКЕ КАРТЫ

Участнику СВО поступает телефонный звонок или приходит СМС сообщение от имени банка о том, что его банковская карта заблокирована. Участнику СВО сообщают, что для разблокировки банковской карты необходимо перейти по ссылке, указанной в сообщении или назвать звонящему номер банковской карты, ПИН-код, пароли, секретные коды, которые приходили в SMS сообщении от банка.

КАК ОБЕЗОПАСИТЬ СЕБЯ. Не торопиться немедленно выполнять требования лица, представившегося сотрудником банка. Связаться со службой поддержки клиентов самостоятельно, чтобы узнать о состоянии карты.



ПРОИСШЕСТВИЕ С РОДСТВЕННИКОМ

Участнику СВО поступает телефонный звонок или приходит СМС сообщение от лица, представляющегося сотрудником правоохранительных органов, предлагающего поучаствовать в раскрытии преступления или помочь лицу, против которого возбуждено уголовное дело. Для этого участнику СВО предлагают срочно перевести денежные средства на определенный расчетный счет или передать денежные средства третьим лицам.

КАК ОБЕЗОПАСИТЬ СЕБЯ. Немедленно прервать разговор, поскольку это мошенник! Никакие оперативно-розыскные мероприятия и следственные действия сотрудниками правоохранительных органов по телефону не обсуждаются и не проводятся!

Помните, что передача денег должностному лицу за освобождение от ответственности является взяткой.

ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ

Участнику СВО приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат услуг. Сразу после этого поступает звонок и сообщают, что на счет участника СВО ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Если перевести, то такая же сумма списывается со счета участника СВО.

КАК ОБЕЗОПАСИТЬ СЕБЯ. Советуем не поддаваться на обман. Если просят перевести якобы ошибочно переведенную сумму, необходимо напомнить, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

КОМПЕНСАЦИЯ ЗА ЛЕКАРСТВЕННЫЕ ПРЕПАРАТЫ

Через некоторое время после осуществления участником СВО заказа по почте лекарственного препарата поступает звонок по телефону и неизвестный (якобы представитель Министерства здравоохранения, налоговый инспектор либо сотрудник правоохранительных органов) сообщает, что приобретенный препарат якобы оказался подделкой и покупателю положена компенсация в размере от 150 тысяч рублей и выше. Чтобы получить эти деньги необходимо заплатить подоходный налог с суммы, в связи с чем злоумышленник указывает номер счета, на который необходимо перевести деньги.

КАК ОБЕЗОПАСИТЬ СЕБЯ. Немедленно прервать разговор, поскольку это мошенник! Представитель Министерства здравоохранения, налоговый инспектор либо сотрудник правоохранительных органов не будут обращаться с такими предложениями.

СООБЩЕНИЕ ОТ НЕИЗВЕСТНОГО АБОНЕНТА

На телефон участника СВО приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств со счета.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счет они снимаются с телефона.

КАК ОБЕЗОПАСИТЬ СЕБЯ. Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

ЕЩЕ РАЗ НАПОМИНАЕМ!

1. Если звонят подозрительные лица, то немедленно прервите разговор! При длительном разговоре мошенники внушат необходимость исполнить их требования! Для этого разговор будет вестись в темпе «давления» (чтобы Вы не могли прервать разговор), Вас будут запугивать негативными последствиями (денежные средства нужно немедленно обезопасить от похищения), требовать немедленных действий без предоставления возможности обдумать их результаты.

2. Никогда и никому не сообщайте пароли и секретные коды, которые приходят вам в сообщении от банка. Только мошенники спрашивают эти пароли и коды.

Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность! Никто, ни банк, ни правоохранительные органы, не вправе требовать ваш ПИН-код и пароль!

3. Оперативно-розыскные действия, следственные мероприятия по телефону не проводятся!

Службы безопасности банков и сотрудники правоохранительных органов никогда не звонят гражданам с сообщениями о необходимости взять кредит и перевести деньги на «безопасный» или «резервный» счет!

Никогда не совершайте никаких переводов и не передавайте деньги третьим лицам.

4. Не перезванивайте по телефонам и не переходите по подозрительным ссылкам, которые указаны в СМС сообщениях, сообщениях из социальных сетей и электронной почты! Не открывайте сообщения с незнакомых адресатов! Там могут содержаться шпионские программы, помогающие похитить ваши банковские данные!

Отказывайтесь от предложений посторонних лиц, которые предлагают скачать на телефон программы RustDesk и AnyDesk, а затем предоставить коды доступа! Они дают доступ к управлению телефоном и беспрепятственному управлению банковскими счетами! Мошенники могут перевести ваши деньги в другой банк, а доказать это будет невозможно, т.к. с банком взаимодействовал Ваш телефон.

5. Оказывайте помощь или ведите поиск участников СВО через Министерство обороны Российской Федерации, публичные органы власти или организации, которые этим официально занимаются.

6. При получении фото- и видеоматериалов с изображением участников СВО или их родственников не предпринимайте поспешных действий, они могут сгенерированы программным обеспечением.

Постарайтесь связаться с ними или выяснить судьбу через Министерство обороны Российской Федерации.