МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по противодействию телефонным мошенничествам, мошенничествам с пластиковыми картами и в социальных сетях интернета.

Содержание

1. Введение.

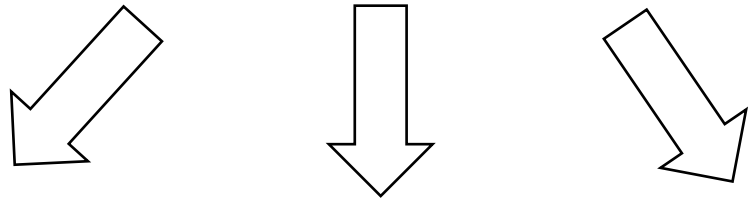
Сегодня в повседневной жизни используется множество разнообразных высокотехнологичных устройств – пластиковых карт, мобильных телефонов и компьютеров.

Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определённых навыков и знаний.

Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила пользования мобильными телефонами, пластиковыми картами и компьютерами.

Проанализировав все случаи такого мошенничества, специалисты УМВД России разработало для следующую памятку. Предлагаем внимательно ознакомиться с содержанием этой брошюры и следовать данным рекомендациям. Они защитят Вас от действий мошенников и сберегут Ваши средства.

В данных рекомендациях подробно будут описаны следующие виды мошеннических действий.



Телефонное мошенничество	Мошенничество с банковскими картами	Мошенничество с помощью социальных сетей

2. Телефонное мошенничество, его основные схемы.

Обман по телефону: требование выкупа.

КАК ЭТО ОРГАНИЗОВАНО:

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления.

Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Далее в разговор вступает «якобы сотрудник полиции».

Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Первое и самое главное правило — прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации.

Хотя беспокойство за родственника или близкого человека мешает мыслить здраво, следует понимать: если незнакомый человек звонит Вам и требует привезти на некий адрес денежную сумму – это мошенник.

Если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела, и если звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба.

Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

МВД России обращает ваше внимание на то, что требование взятки является преступлением.

SMS-просьба о помощи

SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

Телефонный номер-грабитель

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, *проблемы со связью или с Вашей банковской картой* и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь – и оказывается, что с Вашего счёта списаны крупные суммы.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД России настоятельно советует не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

Телефонные вирусы

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента 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 с вашего 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 счёт они снимаются с телефона.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

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

Выигрыш в лотерее

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют их для прикрытия своей деятельности и обмана людей.

«Вы победили, сообщите код карты экспресс-оплаты»

Карточки экспресс-оплаты упростили процедуру зачисления денежных средств на счёт, но одновременно и открыли новые возможности для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

На Ваш мобильный телефон звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерее, организованной радиостанцией и оператором мобильной связи. Это может быть телефон, ноутбук или даже автомобиль. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию.

Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры:

- просит представиться и назвать год рождения;
- грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.);
- спрашивает, может ли абонент перевести на свой номер денежные средства с карты экспресс-оплаты на определенную сумму (от 300 долларов и выше);
- объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя, сообщает номер, куда надо перезвонить;
- поясняет порядок последующих действий для получения приза: с 10.00 до 20.00 такого-то числа абоненту необходимо с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления радостного события.

Если по каким-то причинам абонент не сможет в течение часа купить экспресс-карту, то все равно должен позвонить для согласования дальнейших действий.

Затем мошенник объясняет порядок активации карт: стереть защитный слой; позвонить в призовой отдел; при переключении на оператора – сообщить свои коды. Якобы оператор их активирует на номер абонента, а призовой отдел контролирует правильность его действий, после чего присваивает ему персональный номер, с которым «победитель» должен ехать за призом.

Но если Вы предложите самостоятельно активировать карты на свой номер и приехать с доказательными документами из сотовой компании, то это объявят нарушением правил рекламой акции.

Используются и другие варианты мошенничества

Вам может поступить звонок от якобы представителя вашей сотовой компании, который предложит пополнить счет карточкой экспресс-оплаты. Но прежде чем совершить

оплату, Вы должны будете сообщить оператору личный ПИН-код, перезвонив на определенный номер.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД России напоминает, что активировать карточки экспресс-оплаты следует исключительно через специальный короткий номер, указанный на карточке, а личный код никому никогда не сообщается.

Всё это указано на карте экспресс-оплаты – и в первую очередь надо следовать этим правилам.

Если Вам поступило предложение от радиостанции активировать карточки экспересс-оплаты – не верьте.

Радиостанции никогда не требуют активировать карточки экспресс-оплаты при проведении лотереи. «Вы выиграли машину, нужны деньги для её оформления». Выигрыш приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.

Простой код от оператора связи

КАК ЭТО ОРГАНИЗОВАНО:

Вам поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки Вашего оператора мобильной связи.

Обоснования этого звонка или SMS могут быть самыми разными:

- предложение подключить новую эксклюзивную услугу;
- для перерегистрации во избежание отключения связи из-за технического сбоя;
- для улучшения качества связи;
- для защиты от СПАМ-рассылки;
- предложение принять участие в акции от вашего сотового оператора.

Вам предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД России обращает Ваше внимание, что любая упрощённая процедура изменения тарифных планов выглядит подозрительно. Не ленитесь перезванивать своему мобильному оператору для уточнения условий. SMS-сообщения могут быть самыми разными. Советуем Вам критически относиться к таким сообщениям и не спешить выполнить то, о чем просят. Лучше позвоните оператору связи, узнайте, какая сумма спишется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

Штрафные санкции и угроза отключения номера

КАК ЭТО ОРГАНИЗОВАНО:

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что произошло нарушение условий договора:

- абонент сменил тарифный план, не оповестив оператора;
- не внес своевременно оплату;
- воспользовался услугами роуминга без предупреждения и так далее.

Чтобы предотвратить отключение номера, Вам предлагается:

- купить карты экспресс-оплаты и сообщить их коды;
- перевести на свой номер сумму штрафа и набрать код;

- перевести средства на указанный номер.

После этого Вы якобы сможете доказать свою невиновность и при этом сохраните свой номер.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД России рекомендует перезванивать своему мобильному оператору для уточнения условий.

Помните, что у Вас, как у потребителя услуг связи, есть права, которые защищаются законом. Никакой оператор связи не может требовать выплачивать ему штрафы до тех пор, пока Ваша вина не будет доказана.

Ошибочный перевод средств

КАК ЭТО ОРГАНИЗОВАНО:

Вам 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 Вам сообщают, что на Ваш счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД России советует Вам не поддаваться на обман. Если Вас просят перевести якобы ошибочно переведённую сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян» скорее всего свидетельствует о том, что с Вами общается мошенник.

3. Мошенничество с банковскими картами

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит сообщение о том, что «Ваша банковская карта заблокирована». Предлагается бесплатно позвонить на определенный номер для получения подробной информации.

Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД России предупреждает: не торопитесь сообщать реквизиты вашей карты! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.

4. Правила безопасного использования банковских карт

ПИН-КОД – КЛЮЧ К ВАШИМ ДЕНЬГАМ

- Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами.

- Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери. ВАША КАРТА – ТОЛЬКО ВАША.

- Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.

НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД

- Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ ПРИ ЕЕ УТЕРЕ

- Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

- Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком – он обязан предоставить консультационные услуги по работе с картой.

НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

- В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

5. Мошенничество с помощью социальных сетей. Актуальны схемы мошенничества. Примеры.

Схема мошенничества в мессенджерах в отношении сотрудников и работников органов исполнительной власти города Москвы и подведомственных им организациям (далее – работник).

Работник получает сообщение от лица руководителя организации (поддельный аккаунт) с поручением провести диалог с внешней службой безопасности.

Для повышения доверия к сообщению преступник использует реальные фамилию, имя, отчество руководителя и его официальное фото на аватарке.

Используется давление на человека через авторитет его непосредственного руководителя и репутацию ФСБ России. Часто дополнительно разыгрываются роли с участием фиктивных Центробанка и МВД России.

Продолжение переписки может привести к финансовым потерям, хищению личной и конфиденциальной информации и подрыву репутации Вашей, Ваших коллег или организации в целом.

Примеры реальных атак злоумышленников:

• на левом рисунке сообщение от якобы председателя Комитета ветеринарии города Москвы;

• на правом рисунке сообщение от якобы директора ГКУ «Московский центр развития социальных технологий».

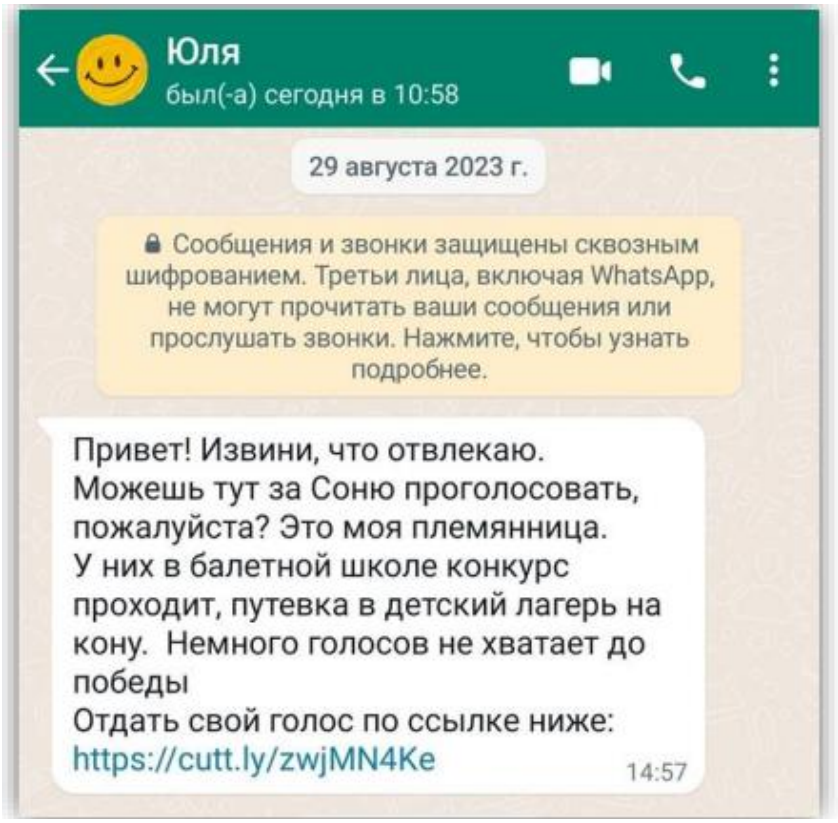
Еще одна распространенная схема мошенничества, когда работник получает сообщение от своего коллеги, аккаунт которого взломали.

Злоумышленник делает рассылку фишингового сообщения с вредоносной ссылкой или вложением всем контактам из телефонной книги взломанного аккаунта. При этом, его владелец этого даже не замечает и не видит этой переписки.

В сообщении описывается проблема и просьба о помощи (в данном случае идет давление через жалость или желание помочь), любопытный факт или новость с предложением перейти по ссылке или скачать файл (в данном случае преступник надеется на любопытство собеседника или пытается вызвать страх и т.д.).

Переход по ссылке или открытие вредоносного файла ведет к заражению вашего смартфона и получению мошенником контроля над ним.

Затем схема мошенничества повторяется, теперь уже вашим контактам рассылается фишинговое письмо.



Мошенники действуют под «маской» Telegram с целью кражи аккаунтов.

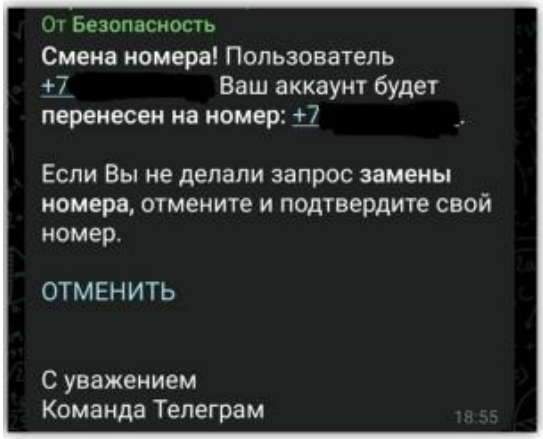
Жертвы мошенников получают сообщения якобы от Команды Телеграм, в которых предлагается перейти по ссылкам.

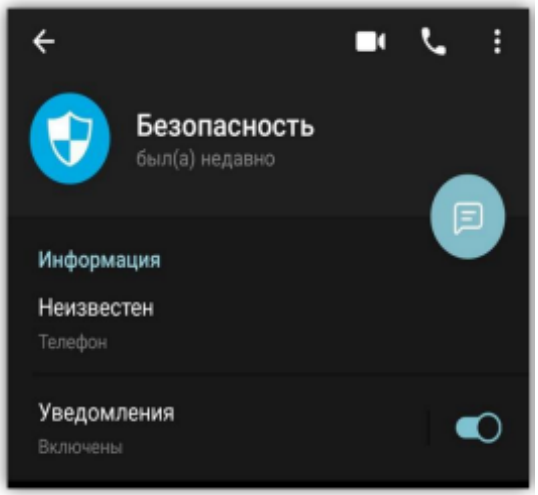
Сами ссылки спрятаны под текст: «Отменить», «Нажмите на сообщение» (под таким текстом скрываются подобные фишинговые ссылки: hxxps://telegramn[.]ru/MTgzNzU= или hxxps://telegramn[.]ru/MTg0MTI).

В сообщении побуждают:

- обновить систему безопасности;
- отменить привязку другого номера к аккаунту;
- обновить аккаунт и т.д.

Во всех таких сообщениях мошенники скрыто манипулируют человеком, побуждая к необдуманным действиям.





Используя современные технологии, мошенники генерируют фейковые ГОЛОСОВЫЕ СООБЩЕНИЯ, которые отправляют через мессенджеры

Будьте бдительны если:

• сообщение выходит за рамки привычного обсуждения – например, связано с денежным переводом, запросом пароля, необходимостью взаимодействия с правоохранительными органами и т.п.;

• вы не ждали личного сообщения от руководителя;

• в сообщении присутствует давление через свой авторитет;

• в сообщении присутствует момент срочности.

6. Инструкция: Как не попасться на мошенничество в социальных сетях.

ВАЖНО:

1	**Не вступайте в переписку, если:** • **вы не ждали данное сообщение;** • **если собеседник манипулирует своим авторитетом;** • **использует ваши слабости *(страх, любопытство, желание помочь, срочность и т.д.)*, чтобы достичь своих целей.**
2	**Никому не сообщайте ваши пароли, коды подтверждения операций, приходящие на устройство.**
3	**Прежде чем переходить по ссылке или открывать файл:** • **решите, а есть ли в этом необходимость;** • **проанализируйте входящее сообщение на скрытую манипуляцию вашими эмоциями или желаниями.**
4	**Настройте двухфакторную аутентификацию аккаунта в мессенджере**

Для заметок

ВНИМАНИЕ!

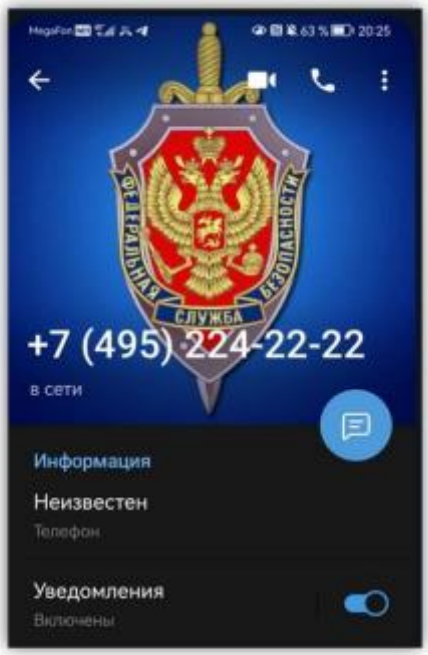
Злоумышленники пытаются максимально расположить к себе собеседника, для этого:

- **подменяют номер телефона на официальный** *(например, при входящем звонке отображается телефон ФСБ России и т.д.)*;
- **направляют фото якобы своего служебного удостоверения;**
- **используют официальную символику органов государственных власти** *(например, при входящем звонке отображается геральдический знак – эмблема ФСБ России и т.д.)*.
- **направляют от имени органа государственной власти якобы официальные обращения, заверенные подписью и печатью руководителя, в которых сообщают:**
  - о голосовом согласии в сотрудничестве с органами государственной власти;
  - о том, что вы являетесь подозреваемым (обвиняемым);
  - об установлении в отношении вас факта мошеннических действий;
  - о необходимости выполнения процедуры обновления единого лицевого счета;
  - о необходимости получения кредита и перевода денег на «безопасный счет» или передачи их курьеру и т.д.

ВАЖНО ПОМНИТЬ!

- ✓ **Уведомление гражданина органы государственной власти осуществляют лично ИСКЛЮЧИТЕЛЬНО В ПИСЬМЕННОМ ВИДЕ И ВРУЧАЮТ ЛИЧНО.**
- ✓ **Сотрудники органов государственной власти НИКОГДА НЕ ПРИСЫЛАЮТ гражданам копии своих служебных удостоверений.**
- ✓ **Органы государственной власти НЕ ИСПОЛЬЗУЮТ личные сбережения или кредитные средства граждан для оказания помощи оперативным подразделениям в предупреждении и раскрытии преступлений.**
- ✓ **Официальные телефоны органов государственной власти используются ИСКЛЮЧИТЕЛЬНО ДЛЯ ПРИЕМА ИНФОРМАЦИИ от граждан и организаций.**

7. Примеры конатктной информации и дейтсвий мошенников в социальных сетях.



ФСБ РОССИИ
Управление
Федеральной службы безопасности
Российской Федерации
по Московской области
(УФСБ России по Московской области)
ул.Большая Лубянка, д.2, г.Москва, 107031

Согласие на сотрудничество

_____ дав голосовое согласие на сотрудничество с Федеральной Службой Безопасности Российской Федерации обязуется не разглашать сведений, составляющих государственную и служебные тайны, точно выполнять относящиеся к ней (нем) требования приказов, положений, инструкций по обеспечению режима секретности проводимых работ.

Об ответственности по закону разглашений сведений, составляющих государственную тайну, утрату документов, содержащие такие сведения, а также об ответственности за нарушения установленного режима секретности проводимых работ предупрежден (а).

Инструктаж провел _____

ст. следователь следственного отдела УФСБ

«26» сентября 2023 г. _____


УФСБ
был(а) недавно
Информация
@ufcb12
Имя пользователя
Уведомления
Включены
Добавить в контакты


Вы
СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ
РУКОВОДИТЕЛЬ ОТДЕЛА
СЛУЖБЫ БЕЗОПАСНОСТИ
ЦЕНТРАЛЬНОГО БАНКА
РОССИЙСКОЙ ФЕДЕРАЦИИ


МВД РОССИИ
ВВК № 958841
Действительно до 20 марта 2024
Личный № А-14491
ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ
ПО МОСКОВСКОЙ ОБЛАСТИ
СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ
№ 958841
Старший Лейтенант внутренней службы
Савин
Андрей Владимирович
должность Старший Следователь
ГУ МВД РФ
20 марта 2021