



РАСПРОСТРАНЕННЫЕ СХЕМЫ МОШЕННИЧЕСТВА



«ЛЖЕСОТРУДНИК БАНКА»
(БАНК РОССИИ, ЦЕНТРОБАНК)

- ▶ «ВАШИ ДАННЫЕ ПОПАЛИ В ТРЕТЬИ РУКИ
И НА ВАС ПЫТАЮТСЯ ОФОРМИТЬ КРЕДИТ»
- ▶ «С ВАШЕЙ КАРТЫ ПЫТАЮТСЯ ПЕРЕВЕСТИ ДЕНЬГИ»
- ▶ «ВАША КАРТА (СЧЁТ) ЗАБЛОКИРОВАН»
- ▶ «ПО КАРТЕ ЗАФИКСИРОВАНА ПОДОЗРИТЕЛЬНАЯ ОПЕРАЦИЯ»

- ▶ «ЭТО СЛЕДОВАТЕЛЬ.
Вы являетесь свидетелем по уголовному делу»
- ▶ «КАПИТАН ПОЛИЦИИ **Иванов**. По Вашему паспорту оформлен
КРЕДИТ и указана ВАША банковская карта. Нам необходимо уточнить
ЕЁ РЕКВИЗИТЫ»



«ЛЖЕПРЕДСТАВИТЕЛЬ
ПРАВООХРАНИТЕЛЬНЫХ
ОРГАНОВ»



«ДРУГ, РОДСТВЕННИК»

- ▶ «Я СТАЛ ВИНОВНИКОМ ДТП.
Чтобы избежать наказания, срочно нужны деньги.
Передаю трубку следователю»

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ



**ВОЗЬМИТЕ ПАУЗУ
И СПРОСИТЕ СОВЕТА
У РОДНЫХ И ДРУЗЕЙ!**

✓ НЕ ОТВЕЧАЙТЕ

на звонки с незнакомых номеров

✓ ПРЕРВИТЕ РАЗГОВОР,

ЕСЛИ ОН КАСАЕТСЯ ФИНАНСОВЫХ ВОПРОСОВ

✓ НЕ ТОРОПИТЕСЬ,

принимая решение

✓ ПРОВЕРЬТЕ ИНФОРМАЦИЮ В ИНТЕРНЕТЕ

или обратитесь за помощью к близким родственникам

✓ САМОСТОЯТЕЛЬНО ПОЗВОНИТЕ

близкому человеку / в банк / организацию

✓ НЕ ПЕРЕЗВАНИВАЙТЕ

по незнакомым номерам

✓ НЕ СООБЩАЙТЕ CVV/CVC И ИНЫЕ

данные банковских карт



БУДЬТЕ БДИТЕЛЬНЫ И ОСТОРОЖНЫ !

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону **102**
(с мобильных средств связи) или в дежурную часть территориального органа внутренних дел



ОСТОРОЖНО!!! ОРУДУЮТ ТЕЛЕФОННЫЕ И ИНТЕРНЕТ-МОШЕННИКИ!

ПОКУПКА, ПРОДАЖА
товаров через **ИНТЕРНЕТ**
или с сайтов **ОБЪЯВЛЕНИЙ**



ЗВОНОК ИЛИ
СООБЩЕНИЕ ИЗ БАНКА –
ваша карта заблокирована,
её надо перевыпустить,
защитить от мошенников...



ПОЛУЧИТЕ
КОМПЕНСАЦИЮ
за приобретённые ранее
товары, заплатите
ПРОЦЕНТЫ



ВАШ РОДСТВЕННИК
ПОПАЛ В БЕДУ.
Срочно нужны деньги



Под предлогом
получения
ВЫГОДНОГО КРЕДИТА



Вас просят **ВЕРНУТЬ**
ошибочный
ДЕНЕЖНЫЙ ПЕРЕВОД



**ТРИЖДЫ ПОДУМАЙ И ПРОВЕРЬ ИНФОРМАЦИЮ,
ПРЕЖДЕ ЧЕМ РАССТАТЬСЯ С ДЕНЬГАМИ**

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ



ОСТОРОЖНО!



МОШЕННИКИ!

**ЗВОНОК
от мошенника**



ПРИЗНАКИ

1

Вам предлагают перевести свои денежные средства на **БЕЗОПАСНЫЙ СЧЕТ**;

Вас просят **ПРОДИКТОВАТЬ**

РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ или **ВВЕСТИ** их на сайте;

2

3

Вам предлагают **ОТМЕНИТЬ** (взять) заявку на **КРЕДИТ** или **ЗАБЛОКИРОВАТЬ** банковскую карту;

Вам предлагают получить **БОНУСЫ** и **ПОДАРКИ** от банка, а также различные **КОМПЕНСАЦИИ**;

4

5

Вам предлагают оформить **БЕЗОПАСНУЮ СДЕЛКУ** или **ДОСТАВКУ**, при **ПОКУПКЕ/ПРОДАЖЕ ТОВАРОВ** в сети **ИНТЕРНЕТ**, при этом скидывают Вам ссылку.

ЗАПОМНИТЕ!



НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ, поступившие с неизвестных номеров, особенно зарегистрированных в другом регионе;



НЕ ВЕРЬТЕ любой информации от незнакомца, **ДАЖЕ ЕСЛИ** звонок поступил с официального телефона горячей линии банка;



ПРЕРВИТЕ РАЗГОВОР и самостоятельно позвоните на телефон горячей линии банка, набрав номер **ВРУЧНУЮ**;



ПОМНИТЕ: код от вашей карты и пароли подтверждения операций **НЕ ИМЕЕТ ПРАВА** спрашивать даже сотрудник банка!



ОСТОРОЖНО! МОШЕННИКИ!

Запомните основные схемы и признаки популярных мошенничеств!
Эта информация поможет вовремя распознать злоумышленников.

ПРИЗНАКИ

ЗВОНОК ОТ «СОТРУДНИКА БАНКА»

(СПЕЦИАЛИСТА, РАБОТНИКА СЛУЖБЫ БЕЗОПАСНОСТИ)

- 1 СООБЩАЮТ О ПОПЫТКЕ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ ЛИБО О НЕЗАКОННО ОФОРМЛЕННОМ КРЕДИТЕ
- 2 ПРЕДЛАГАЮТ ПЕРЕВЕСТИ ДЕНЬГИ НА «БЕЗОПАСНЫЙ СЧЕТ», ОФОРМИТЬ «ЗЕРКАЛЬНЫЙ КРЕДИТ»
- 3 ПРОСЯТ НАЗВАТЬ РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ, ЗАЩИТНЫЙ КОД С ЕЁ ОБРАТНОЙ СТОРОНЫ И ПОСТУПАЮЩИЕ НА ТЕЛЕФОН ПАРОЛИ

ЗАПОМНИТЕ!

НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ, ПОСТУПИВШИЕ С НЕИЗВЕСТНЫХ НОМЕРОВ, ОСОБЕННО ЗАРЕГИСТРИРОВАННЫХ В ДРУГОМ РЕГИОНЕ;

НЕ ВЕРЬТЕ ЛЮБОЙ ИНФОРМАЦИИ ОТ НЕЗНАКОМЦА, **ДАЖЕ ЕСЛИ** ЗВОНОК ПОСТУПИЛ С ОФИЦИАЛЬНОГО ТЕЛЕФОНА ГОРЯЧЕЙ ЛИНИИ БАНКА;

ПРЕРВИТЕ РАЗГОВОР И САМОСТОЯТЕЛЬНО ПОЗВОНИТЕ НА ТЕЛЕФОН ГОРЯЧЕЙ ЛИНИИ БАНКА, НАБРАВ НОМЕР **ВРУЧНУЮ**;

ПОМНИТЕ: КОД ОТ ВАШЕЙ КАРТЫ И ПАРОЛИ ПОДТВЕРЖДЕНИЯ ОПЕРАЦИЙ **НЕ ИМЕЕТ ПРАВА** СПРАШИВАТЬ ДАЖЕ СОТРУДНИК БАНКА!



ПРИЗНАКИ

ПОКУПКА/ПРОДАЖА ТОВАРОВ

НА САЙТАХ ОБЪЯВЛЕНИЙ В СЕТИ ИНТЕРНЕТ

- 1 НИЗКАЯ СТОИМОСТЬ ТОВАРА
- 2 ТРЕБОВАНИЕ БЕЗНАЛИЧНОГО РАСЧЁТА
- 3 ПРЕДЛОЖЕНИЕ ПОДКЛЮЧИТЬ «МОБИЛЬНЫЙ БАНК»
- 4 ПОКУПАТЕЛЬ ГОТОВ СДЕЛАТЬ ПОКУПКУ, НЕ ВЗГЛЯНУВ НА НЕЁ
- 5 ПОКУПАТЕЛЬ ПРОСИТ НАЗВАТЬ РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ И ПАРОЛИ ИЗ СМС-СООБЩЕНИЙ
- 6 ПРОДАВЕЦ ПОД РАЗНЫМИ ПРЕДЛОГАМИ ПРОСИТ ВАС ВНЕСТИ ПРЕДОПЛАТУ
- 7 ПОКУПАТЕЛЬ ПРЕДЛАГАЕТ ОБМЕН И ВЫСЫЛАЕТ ПО СМС ВРЕДОНОСНУЮ ССЫЛКУ НА «ТОВАР»

ЗАПОМНИТЕ!

Главная цель злоумышленников – подключиться к **ВАШЕМУ «МОБИЛЬНОМУ БАНКУ»!**

Для совершения денежного перевода необходимо **ЗНАТЬ ТОЛЬКО НОМЕР БАНКОВСКОЙ КАРТЫ**

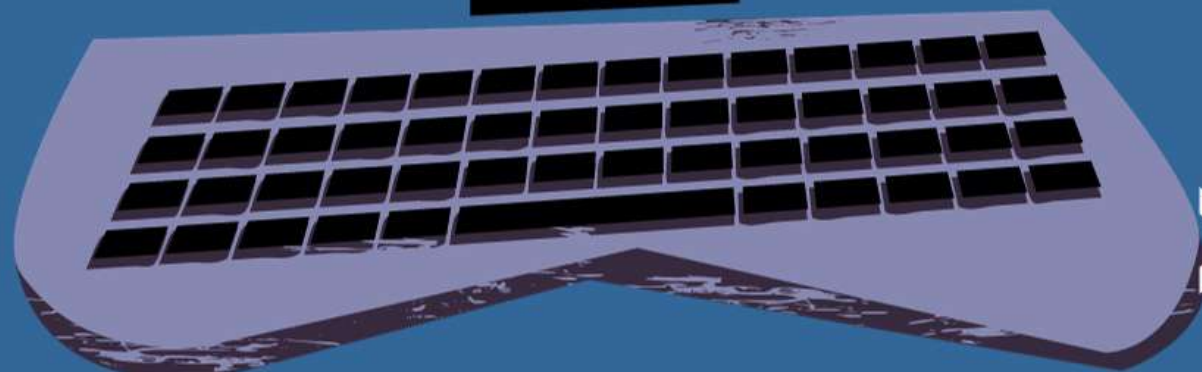
Если покупатель предложил **ПРОЙТИ К БАНКОМАТУ** для получения перевода, **ЗНАЙТЕ: ВАС ПЫТАЮТСЯ ОБМАНУТЬ!**

НЕ ОТКРЫВАЙТЕ ИНТЕРНЕТ-ССЫЛКИ ОТ ПОКУПАТЕЛЯ, ОНИ МОГУТ БЫТЬ ВРЕДОНОСНЫ!



МВД РОССИИ ПРЕДУПРЕЖДАЕТ:

Мошенники для совершения дистанционных хищений используют мессенджеры: присылают сообщения якобы от родственников, коллег и руководителей с работы





Злоумышленники осуществляют рассылку и просят проголосовать за участника какого-либо конкурса, ссылаясь на недостаточность голосов для прохождения в финал, но фактически, пройдя по ссылке, на сайте вы вводите код для предоставления удаленного доступа к своему устройству





**МВД России призывает граждан очень
внимательно относиться ко всем звонкам
и сообщениям, содержанием которых
является просьбы об оказании финансовой
помощи или поддержке конкурсного
голосования**





Если в отношении вас или ваших близких совершены противоправные деяния, как можно быстрее сообщите о случившемся в полицию!





Какие правила стоит соблюдать, чтобы не стать жертвой сетевых аферистов?

Советы от Управления по противодействию
киберпреступности МВД России

Правила цифровой гигиены

#ПредупрежденЗначитВооружен



1. Не переходите по ссылкам из рекламных писем на сайты магазинов, а вводите адрес магазина в строке браузера самостоятельно.

Не ведитесь на манипуляции: всплывающие заманивающие баннеры, акции с таймерами оставшегося времени, надпись «этот товар вместе с вами смотрят N человек» и многое другое.

Правила цифровой гигиены

#ПредупрежденЗначитВооружен



2. Проверьте дату создания сайта с помощью Whois-сервисов.

Если странице пара недель или месяц, то она скорее всего создана к праздничной дате в целях наживы.

Правила цифровой гигиены

#ПредупрежденЗначитВооружен



3. Осуществляйте онлайн-оплату только, если сайт использует протокол HTTPS и имеет действующий сертификат безопасности (изображение замочка в адресной строке).

Правила цифровой гигиены

#ПредупрежденЗначитВооружен



4. Проверьте отзывы о товарах и магазине.

Если их нет, или они исключительно положительные, то перед вами, скорее всего, ФЕЙК.

Правила цифровой гигиены

#ПредупрежденЗначитВооружен



5. Косвенные индикаторы фейка:

- цена сильно ниже рыночной
- обязательна предоплата
- недоступность самовывоза
- отсутствие возможности оплатить покупку при получении

Правила цифровой гигиены

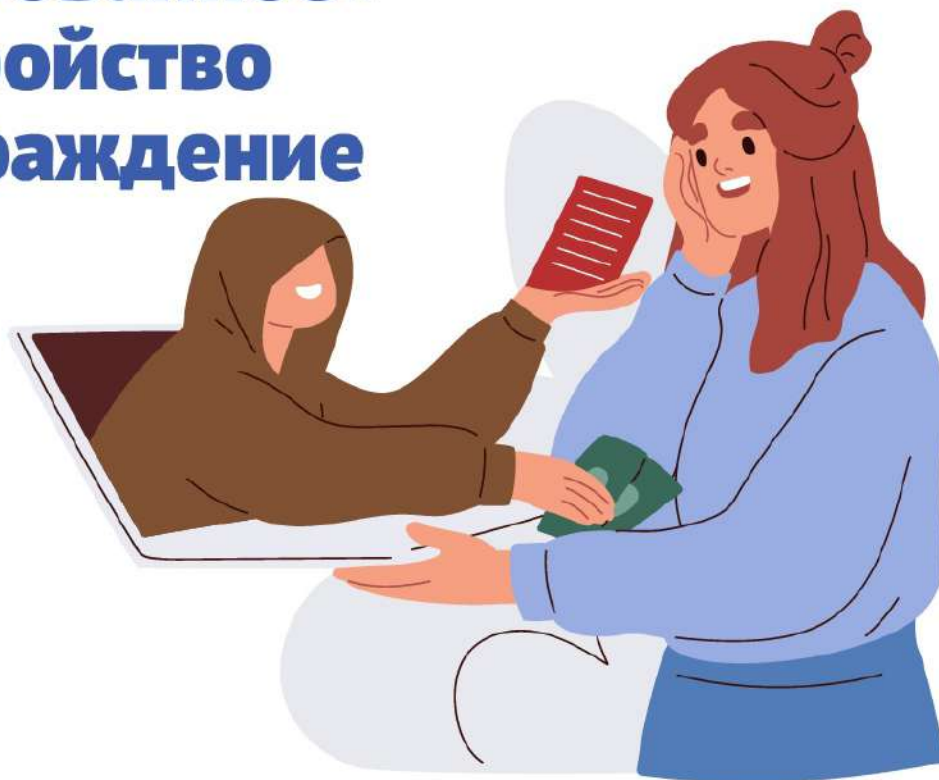
#ПредупрежденЗначитВооружен



МОШЕННИЧЕСТВО ПРИ ПОИСКЕ РАБОТЫ



«Гарантированное» трудоустройство за вознаграждение



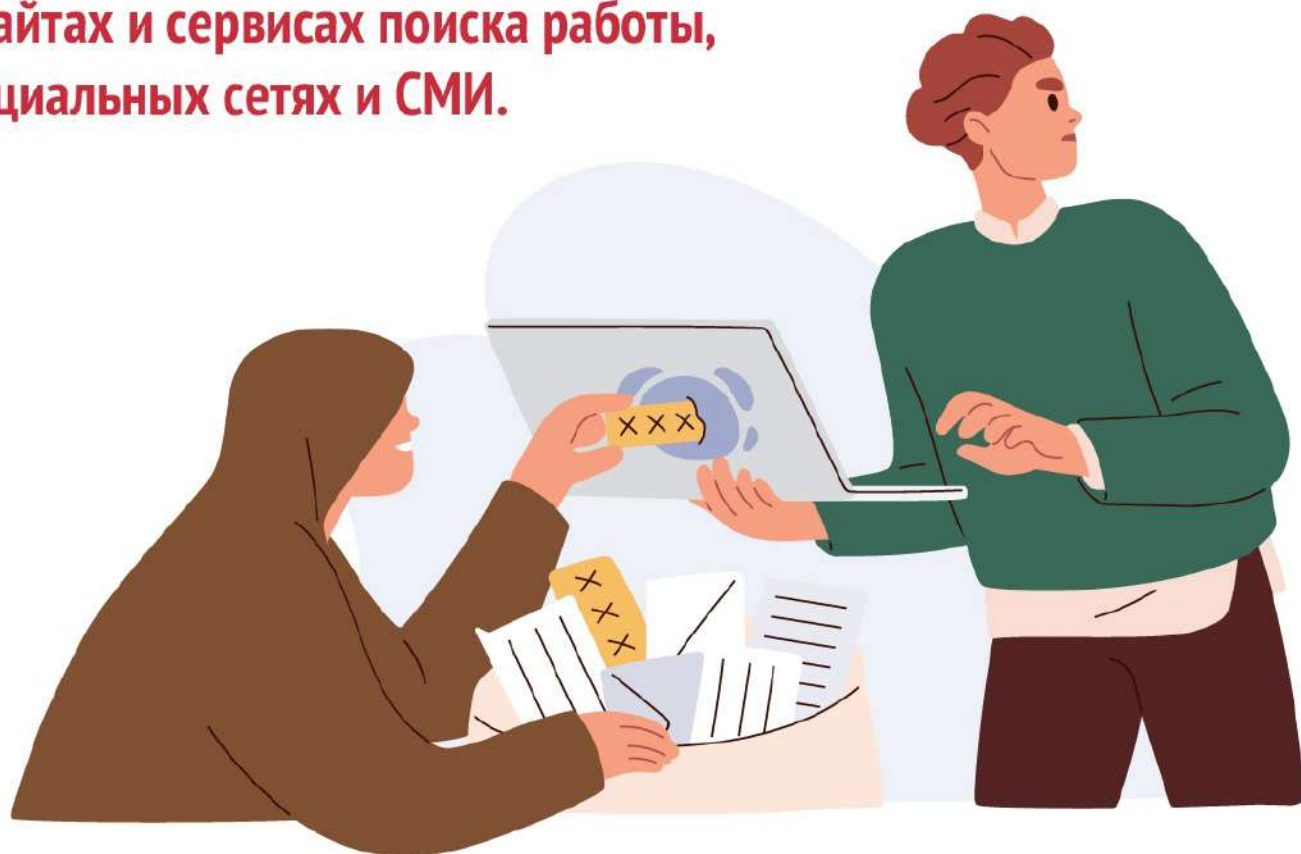
Если вам предлагают пройти обучение по специальной программе, заплатить за подготовку «крутого резюме» или за медосмотр, после чего гарантируют 100% трудоустройства, то, как правило, вы вложите, и «работодатель» пропадает.

В итоге у вас нет ни денег, ни работы.

Плата за доступ к «базам вакансий»

Если с вас требуют оплату за доступ к «базе вакансий», это мошенники. Соискатели не оплачивают услуги кадровых агентств, это делают работодатели.

**Все вакансии находятся в свободном доступе:
на сайтах и сервисах поиска работы,
в социальных сетях и СМИ.**



Работа с «быстрой прибылью»



Только мошенники, обещая сказочные и быстрые прибыли, предлагают вам начать работу со взноса своих средств в их «бизнес».

Лжеработодатель обещает вернуть вам средства (даже с процентами) с первой же зарплаты. Однако момент зарплаты, как и получение сверхприбыли, вряд ли наступит.

Оформление «через смс»

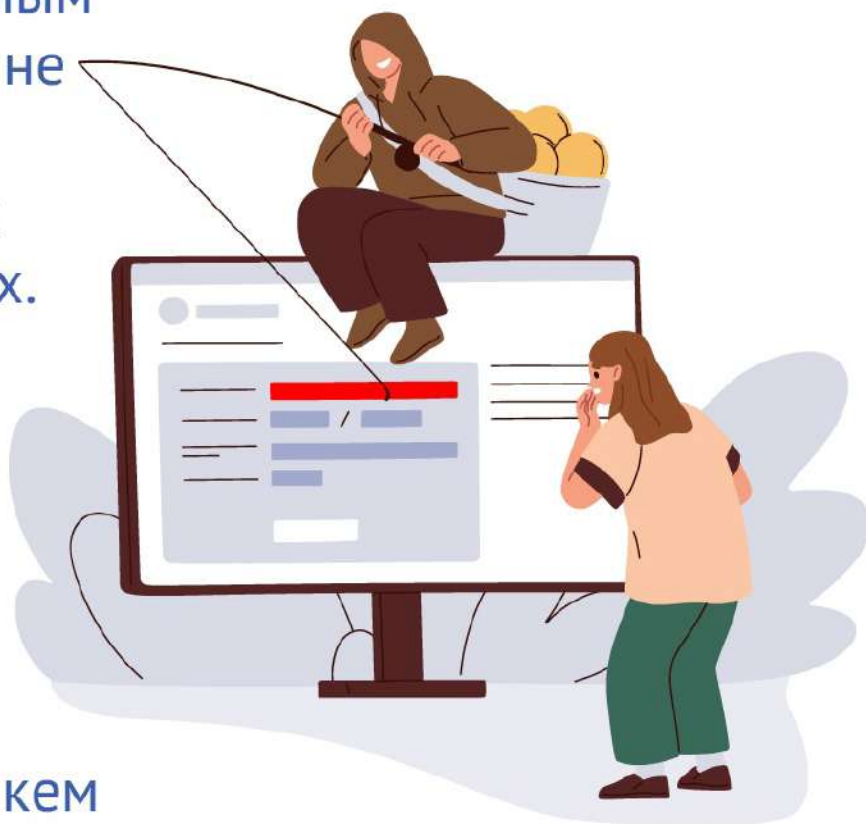
В процессе заключения онлайн-договора с вами работодатель сначала берет резюме, данные вашего паспорта, банковской карты, а затем просит назвать код из смс?

Не сообщайте код, не осуществляйте платных звонков и иных действий с вашими банковскими картами. Вместо трудоустройства вы можете просто потерять деньги.



Трудоустройство или кража персональных данных?

Работа с дистанционным «оформлением» вполне может быть уловкой для получения ваших персональных данных. Не предоставляйте документы и персональную информацию потенциальному работодателю, пока не будете уверены, с кем вы общаетесь.



Предпочтите личную встречу в офисе компании, не передавайте третьим лицам копии своих документов.



МВД России информирует!

**Соблюдая правила
предосторожности при покупках
в интернете, можно оградить себя
от возможных неприятностей**





**прежде чем что-либо приобрести на
неизвестном вам сайте, проверяйте полную
информацию о нем**



**поищите отзывы, почитайте форумы,
изучите отзывы о его работе**



**поисковые системы публикуют рейтинги
Интернет-магазинов, которые тоже являются
показателем надежности торговой площадки**





**Что делать, если при совершении сделок
купли-продажи товаров через Интернет
после их оплаты ни товаров, ни денег
обратно получить не удастся?**





**необходимо обращаться
в правоохранительные органы по месту
жительства для проведения необходимых
проверок и возбуждения уголовного дела**

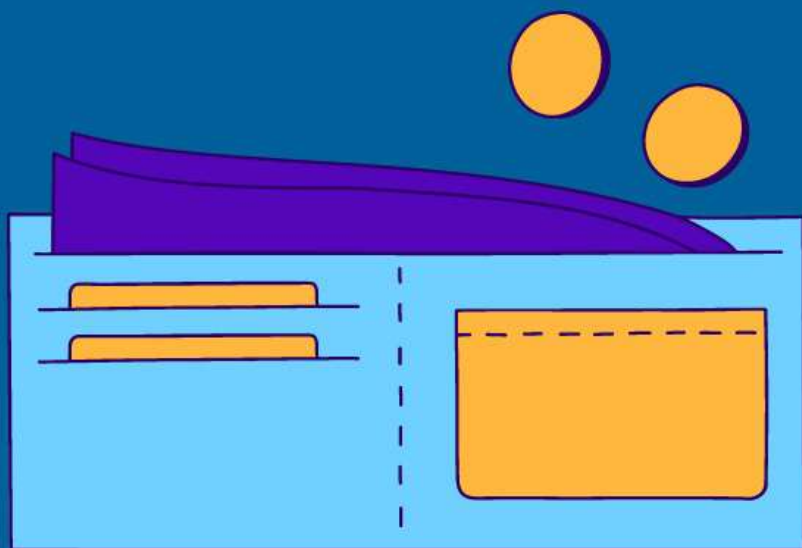


**в заявлении необходимо сообщать как
можно более полную информацию
о злоумышленниках, в частности адрес
сайта, расчетный счет, адрес электронной
почты, номера телефонов и т.д.**





**Берегите свои денежные средства
и совершайте покупки с умом**





**К ВАМ ОБРАТИЛСЯ ЧЕРЕЗ СОЦСЕТИ
СТАРЫЙ ПРИЯТЕЛЬ С ПРОСЬБОЙ
ОДОЛЖИТЬ ПАРУ ТЫСЯЧ?**



**ВПОЛНЕ ВЕРОЯТНО,
ЧТО ЭТО МОШЕННИКИ !**



Злоумышленник может получить доступ к странице вашего друга и от его имени попросить:

- одолжить денег
- предоставить реквизиты банковских карт
- перейти по сомнительной ссылке



*WhatsApp (принадлежит Meta, деятельность которой признана экстремистской и запрещена в России)



**Некоторые граждане
осуществляют необдуманные
финансовые операции и переводят
деньги на указанные им номера
и счета, в результате чего
становятся жертвами мошенников**





Не поленитесь!
Перепроверьте информацию,
позвонив дорогому вам человеку,
чтобы убедиться
в необходимости осуществления
финансовой операции

Заодно узнаете,
как у него дела!





МВД РОССИИ ПРЕДУПРЕЖДАЕТ!

**Телефонные мошенники
не только похищают деньги
своих жертв, но и втягивают
их в совершение преступлений**





КАК РАСПОЗНАТЬ АФЕРИСТОВ?

- При разговоре злоумышленники сообщают, что неизвестные оформили от Вашего имени кредит и пытаются похитить денежные средства, однако есть возможность вернуть Ваши сбережения;
- Мошенники представляются сотрудниками правоохранительных органов и предлагают гражданам оказать содействие в поимке преступников;
- Предлагают хороший заработок в короткий срок абсолютно “легальным” способом.
- Иногда и вовсе злоумышленники напрямую угрожают своим собеседникам неприятностями или даже убийством их родных и близких.





СТОИТ ПОМНИТЬ!

**Каков бы ни был предлог звонивших,
их цель - подтолкнуть
вас к совершению преступления.**

**Как правило, это - ПОДЖОГ
объектов военной,
транспортной
или банковской
инфраструктуры.**





БУДЬТЕ БДИТЕЛЬНЫ!

Внимательно относитесь ко всем звонкам и сообщениям, содержанием которых является требование совершить по инструкции собеседника какие-либо противозаконные действия.

Помните, что атаки на военные и стратегически важные объекты действующим законодательством квалифицируются как диверсия или террористический акт.

Это - особо тяжкие преступления!





ЧТО ДЕЛАТЬ?

Если Вам поступил звонок от неизвестного лица, пытающегося сомнительными предложениями или запугиванием заставить вас совершить противоправное деяние...

**Незамедлительно
кладите трубку
и звоните в полицию!**



102