



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) заблокированы»
- ▶ «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 ПЕРЕЗВНИВАЙТЕ

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**



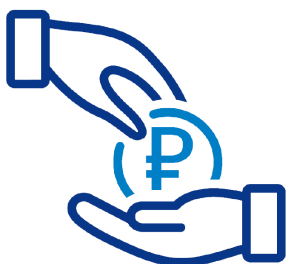
ЗВОНОК ИЛИ
СООБЩЕНИЕ ИЗ БАНКА –
ваша карта заблокирована,
её надо перевыпустить,
защитить от мошенников...



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!



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



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**

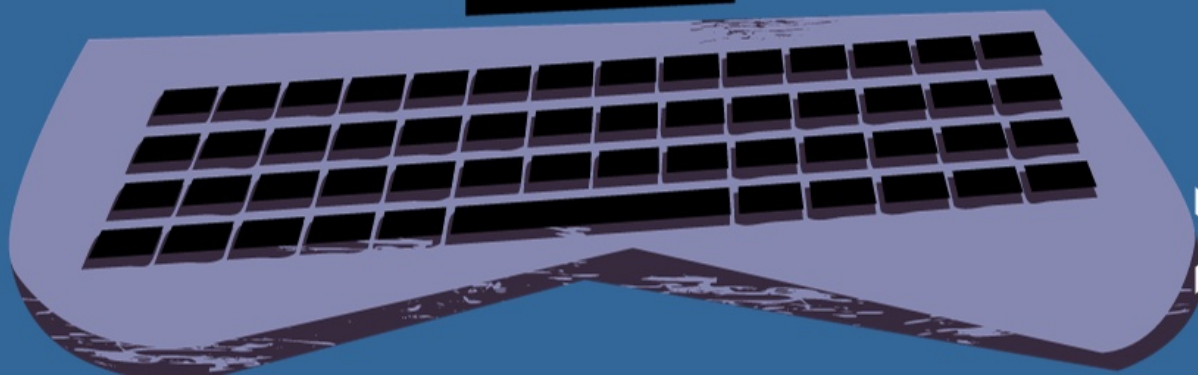
Если покупатель предложил **ПРОЙТИ К БАНКОМАТУ** для получения перевода, **ЗНАЙТЕ: ВАС ПЫТАЮТСЯ ОБМАНУТЬ!**

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





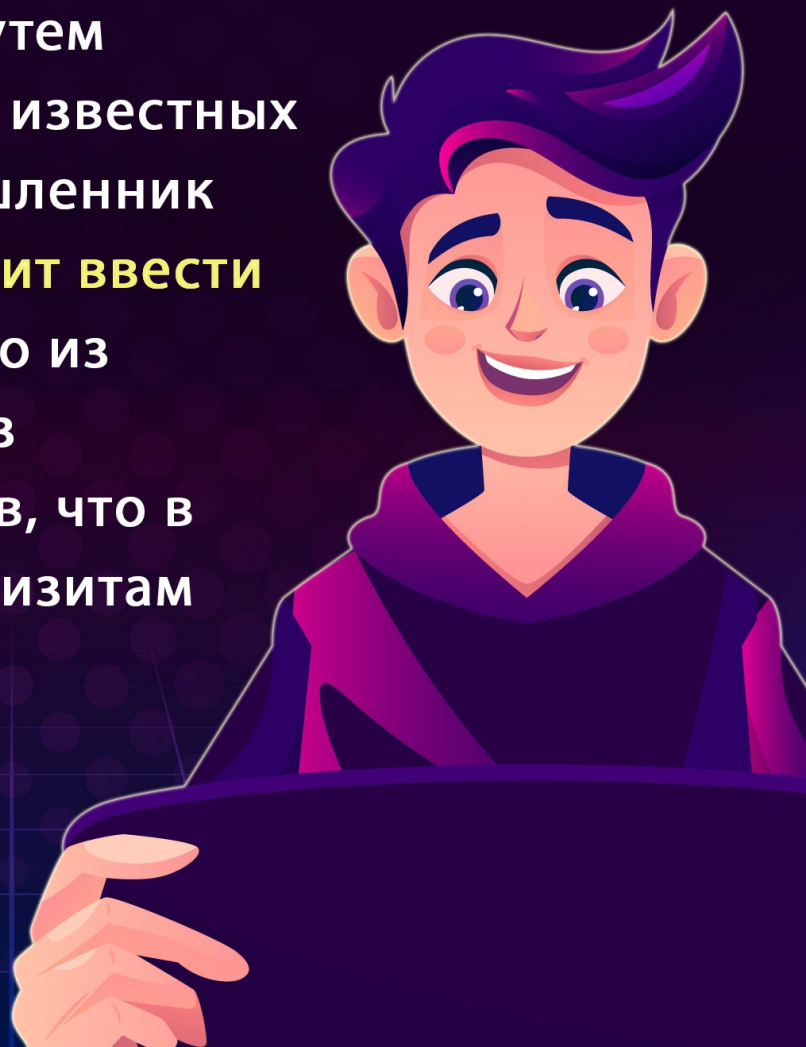
ЛОВУШКИ ВИРТУАЛЬНОГО МИРА





ЛЁГКИЙ ЗАРАБОТОК

Незнакомец связывается с ребёнком в любом из мессенджеров и предлагает заработать путем **просмотра видеороликов** известных блогеров. Далее злоумышленник **отправляет ссылку и просит ввести банковские данные** одного из родителей, а также код из **смс-уведомления**, пояснив, что в дальнейшем по этим реквизитам будет переводить деньги



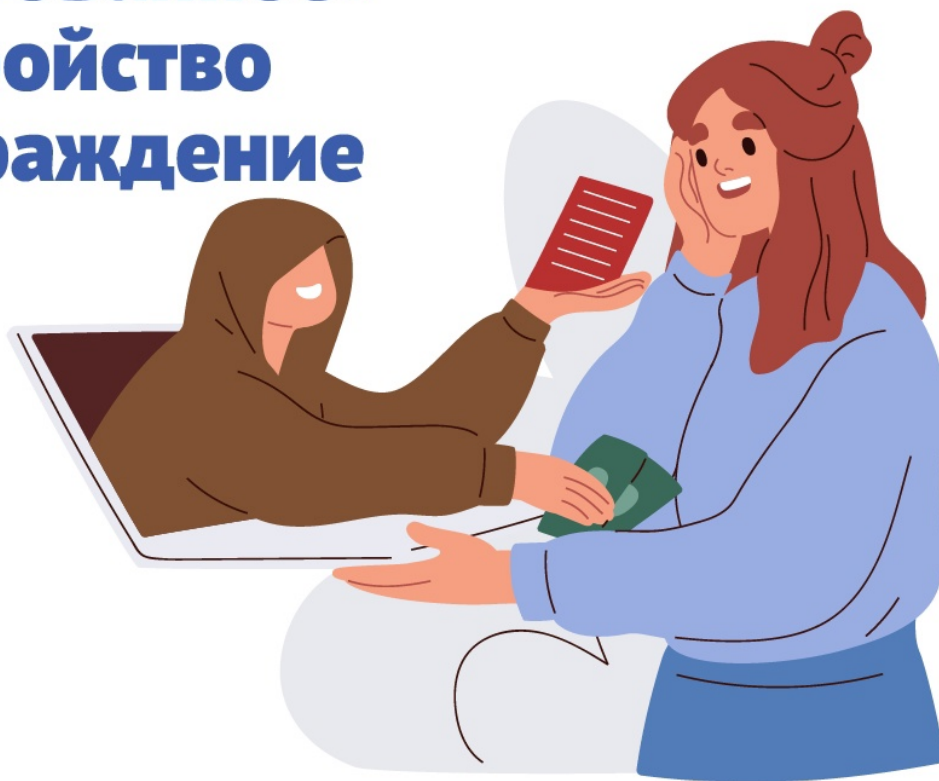


ДОПОЛНЕНИЯ ДЛЯ ОНЛАЙН-ИГР

Мошенники заманивают несовершеннолетних пользователей онлайн-игр **низкими ценами и «уникальными акциями»** на различные девайсы для своего виртуального мира, чтобы быть наравне с лидирующими игроками. Для покупки усовершенствующих дополнений отправляют ссылку, перейдя по которой просят ввести данные банковской карты



«Гарантированное» трудоустройство за вознаграждение



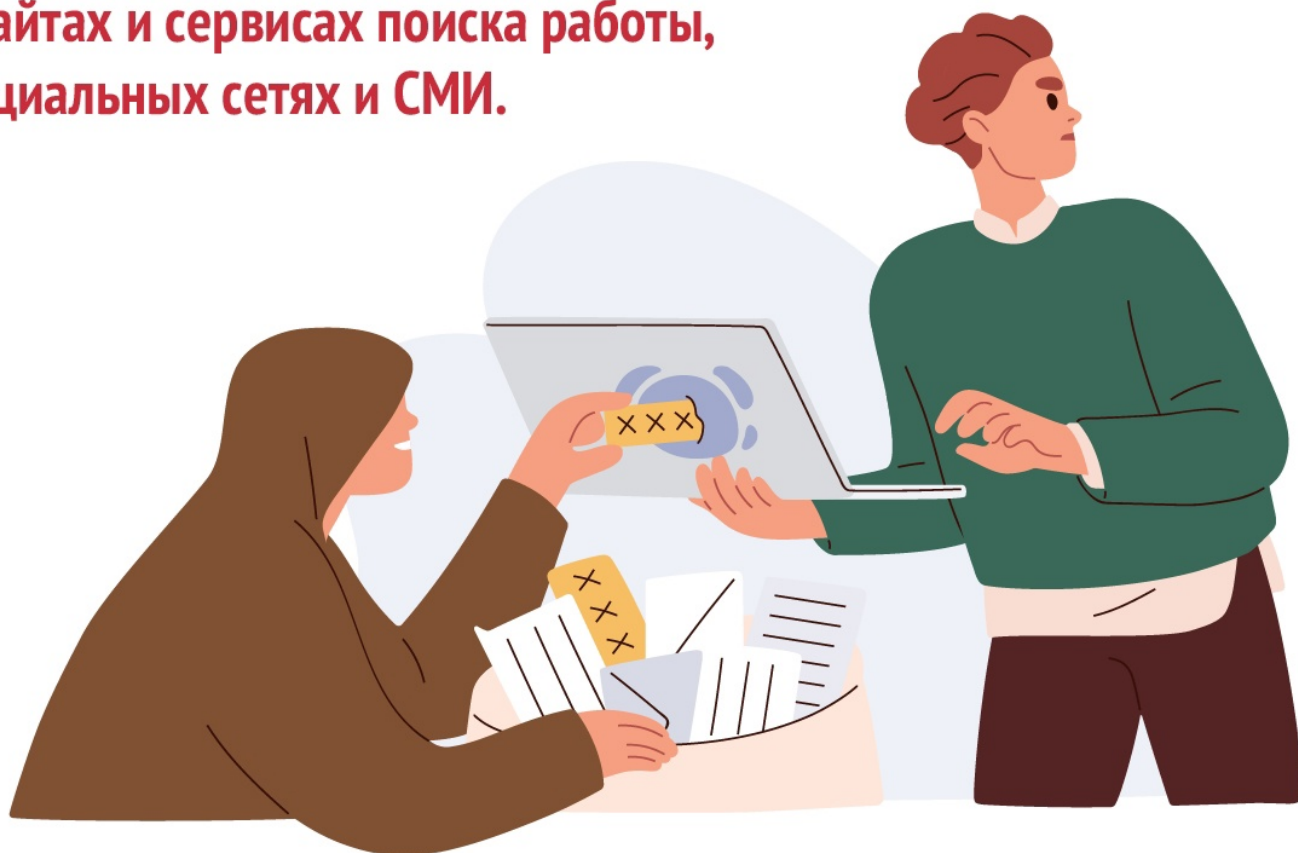
Если вам предлагают пройти обучение по специальной программе, заплатить за подготовку «крутого резюме» или за медосмотр, после чего гарантируют 100% трудоустройства, то, как правило, вы вложите, и «работодатель» пропадает.

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.



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

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





**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!



ПРЕДУПРЕЖДЁН – ЗНАЧИТ ВООРУЖЁН!

Оформление «через смс»

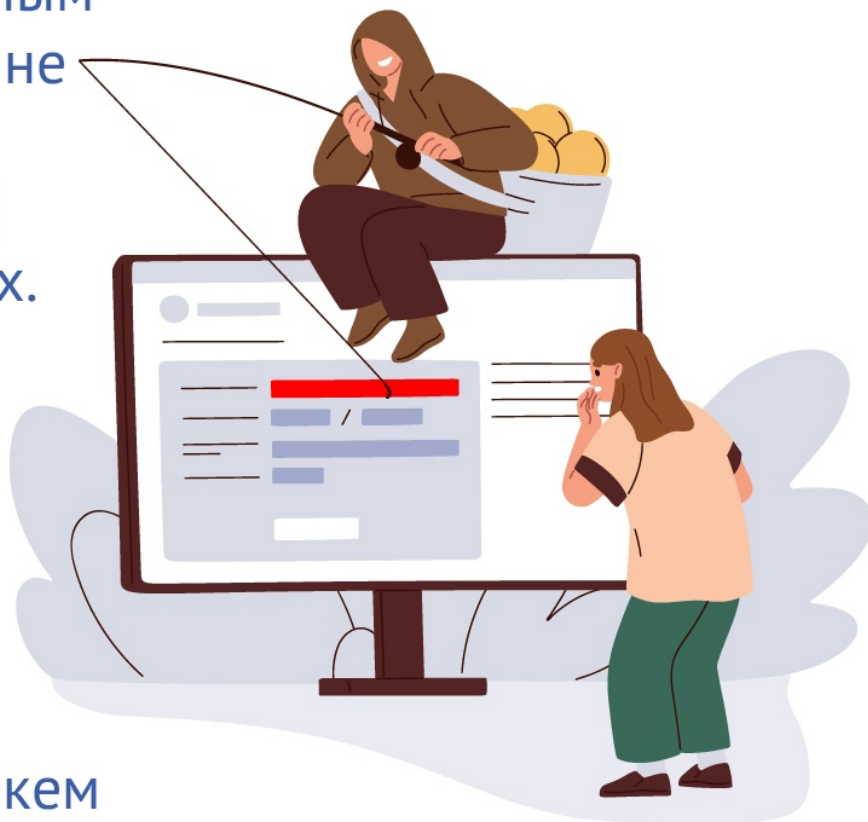
В процессе заключения онлайн-договора с вами работодатель сначала берет резюме, данные вашего паспорта, банковской карты, а затем просит назвать код из смс?

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





МВД РОССИИ ПРЕДУПРЕЖДАЕТ!

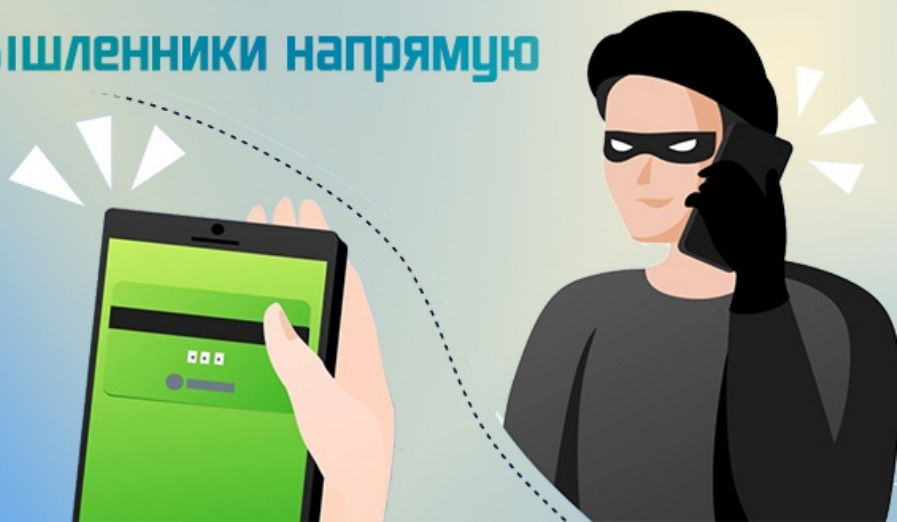
**Телефонные мошенники
не только похищают деньги
своих жертв, но и втягивают
их в совершение преступлений**





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.**



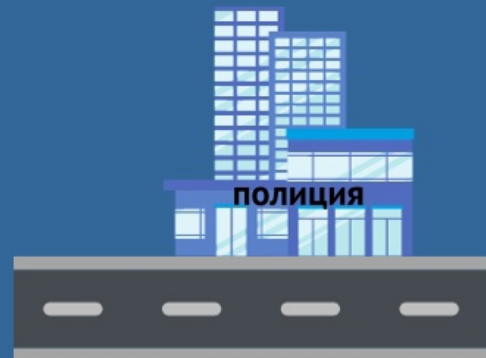
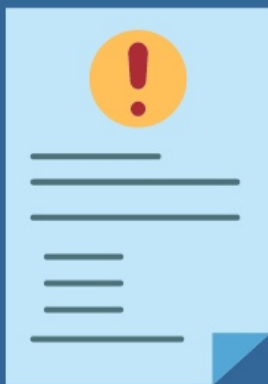


**МВД России призывает граждан очень
внимательно относиться ко всем звонкам
и сообщениям, содержанием которых
является просьбы об оказании финансовой
помощи или поддержке конкурсного
голосования**





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

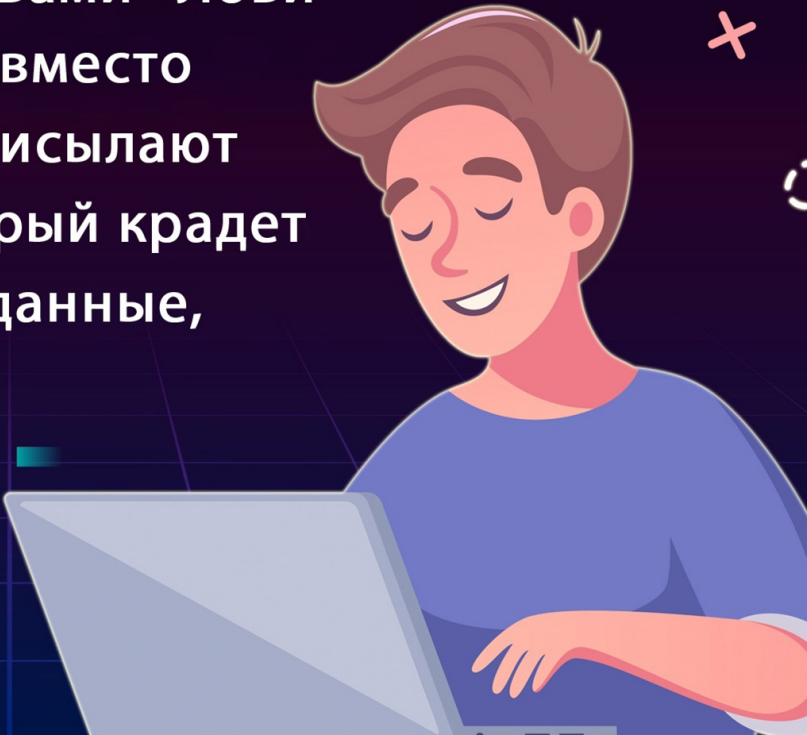
Правила цифровой гигиены

#ПредупрежденЗначитВооружен



SMS ОТ ДРУГА

Киберпреступники **взламывают** аккаунт друга в соцсетях, а затем от его имени присылают сообщение. Начинают разговор с банального «как дела?» и практически сразу переходят к просьбе о помощи и **просят в долг**. Или со словами «Лови фотки со дня рождения!» вместо ссылки на фотографии присылают **вредоносный вирус**, который крадет с гаджета персональные данные, логины и пароли

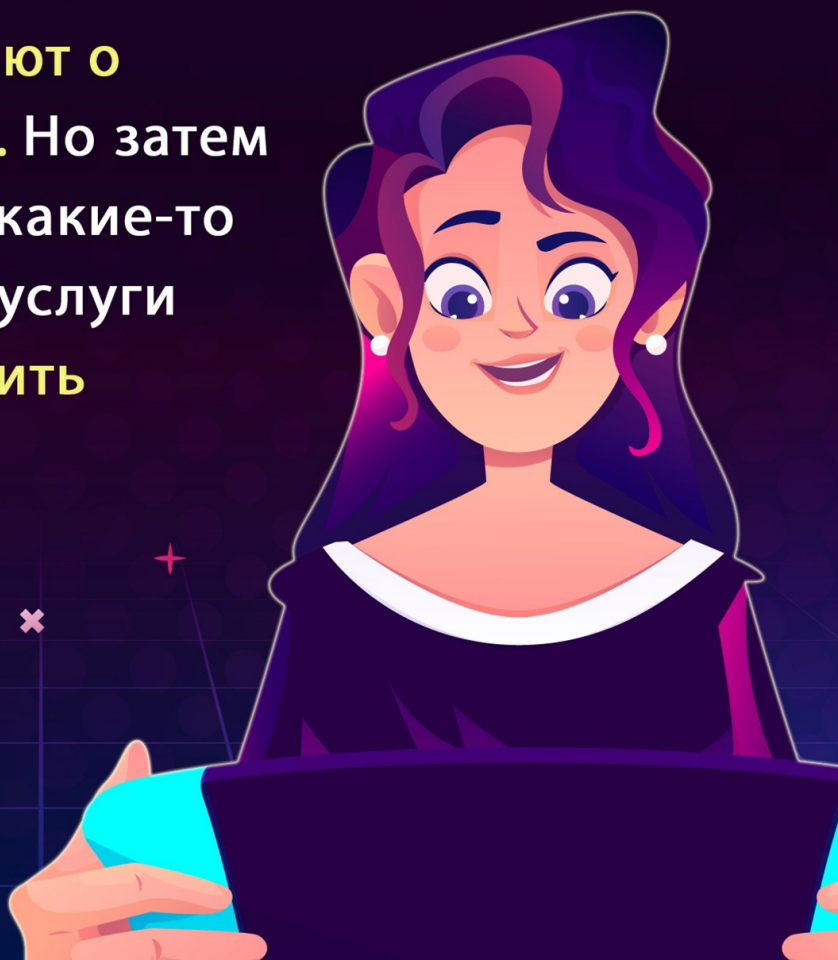


Как дела?



ВЫИГРЫШ В КОНКУРСЕ

Аферисты рассылают сообщения в социальных сетях или отмечают в комментариях под постом с розыгрышем, где **сообщают о неожиданном выигрыше**. Но затем за доставку «приза» или какие-то другие дополнительные услуги школьника **просят оплатить небольшую комиссию**





ВАЖНО!

- ✕ Не переходите по неизвестным ссылкам и не сообщайте незнакомцам данные банковских карт и коды-подтверждения из смс-сообщений
- Прежде чем выполнить всё, о чем просит «друг» в соцсетях, перезвоните ему и уточните, действительно ли нужна помощь
- Когда для получения приза организаторы конкурса просят что-либо оплатить, это повод насторожиться. Убедитесь, что это не мошенники: почитайте отзывы в Интернете, новости (вдруг они уже были замечены в обманах)





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



○ Если у ребёнка имеется собственная банковская карта, то не стоит переводить на неё огромные деньги. Кроме того, можно ограничить суммы списаний или количество операций по карте в день, чтобы мошенникам не удалось украсть с нее все сбережения разом

□ Подключите СМС или push-оповещения ко всем банковским картам, так вы сразу заметите подозрительные покупки





МОШЕННИЧЕСТВО ПРИ ПОИСКЕ РАБОТЫ





 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.**





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!**

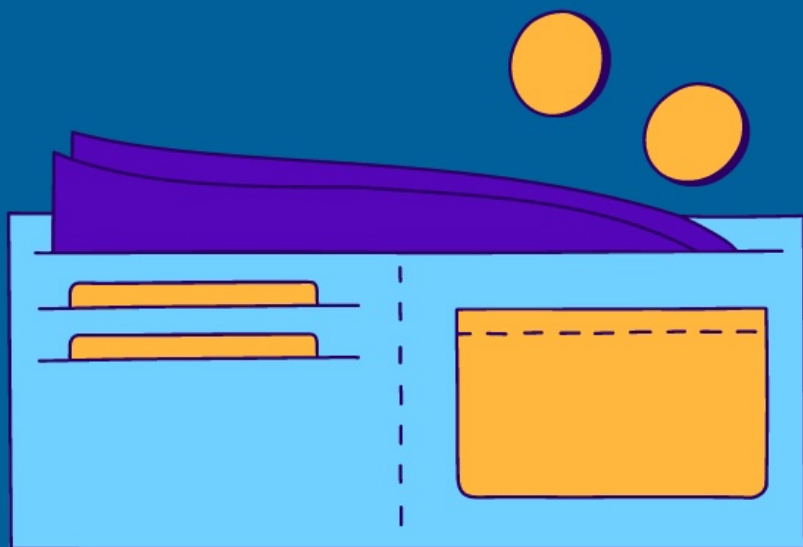


102





**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 !**