
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!
КОНКУРС!

ПРЕДУПРЕЖДЁН – ЗНАЧИТ ВООРУЖЁН!

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

ВПОЛНЕ ВЕРОЯТНО, ЧТО ЭТО МОШЕННИКИ !

ПРЕДУПРЕЖДЁН – ЗНАЧИТ ВООРУЖЁН!

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 Мета, деятельность которой признана экстремистской и запрещена в России)

ПРЕДУПРЕЖДЁН – ЗНАЧИТ ВООРУЖЁН!

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

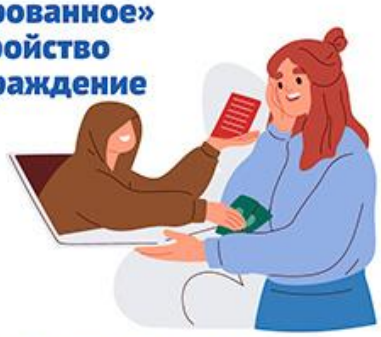
ПРЕДУПРЕЖДЁН – ЗНАЧИТ ВООРУЖЁН!

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

Заодно узнаете, как у него дела!

МОШЕННИЧЕСТВО ПРИ ПОИСКЕ РАБОТЫ

«Гарантированное» трудоустройство за вознаграждение



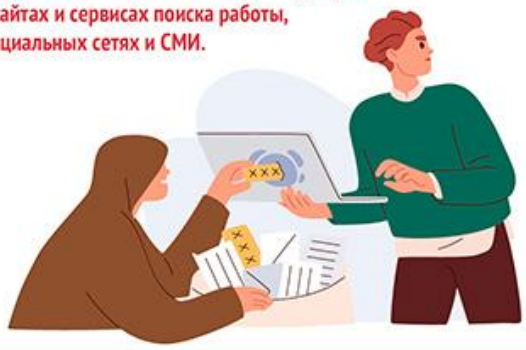
Если вам предлагают пройти обучение по специальной программе, заплатить за подготовку «крутого резюме» или за медосмотр, после чего гарантируют 100% трудоустройства, то, как правило, вы вложитесь, и «работодатель» пропадает.

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 ПРЕДУПРЕЖДАЕТ!

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

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!

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.

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

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!

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 магазин 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.

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.

5. Косвенные индикаторы фейка:

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

Правила цифровой гигиены

ЛОВУШКИ ВИРТУАЛЬНОГО МИРА

ЛЁГКИЙ ЗАРАБОТОК

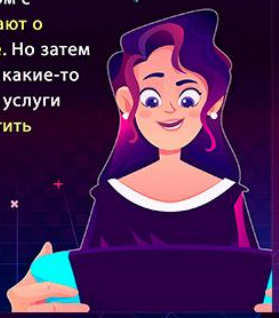
Незнакомец связывается с ребёнком в любом из мессенджеров и предлагает заработать путем просмотра видеороликов известных блогеров. Далее злоумышленник отправляет ссылку и просит ввести банковские данные одного из родителей, а также код из смс-уведомления, пояснив, что в дальнейшем по этим реквизитам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

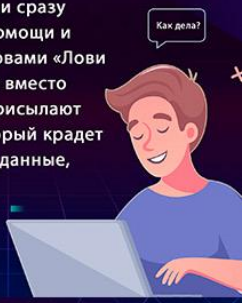
ВЫИГРЫШ В КОНКУРСЕ

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



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



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 «приятель» 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)

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