КУДА ОБРАЩАТЬСЯ ПРИ МОШЕННИЧЕСКИХ ДЕЙСТВИЯХ

01 | В банк.
02 | В отделение полиции по месту жительства.
03 | На Горячую линию МВД по телефону: **8-800-222-74-47.**
04 | На сайт **мвд.рф.**

В МИФИ при поступлении звонков или сообщений, похожих на мошеннические, обращайтесь к проректору Роману Сергеевичу Черниговцеву:

Телефон:
+7 (903) 127 76 78;
+7 (495) 788 56 99, доб. 9906.

E-mail:
rschernigovtsev@mephi.ru

Получить поддержку
в Психологическом центре МИФИ
Тел.: +7 (800) 222 55 71

Иллюстрация: ru.freepik.com

ЧТО ДЕЛАТЬ, ЕСЛИ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ

НАЗВАЛИ МОШЕННИКАМ ДАННЫЕ СВОЕЙ БАНКОВСКОЙ КАРТЫ ИЛИ КОД ИЗ СМС

Заблокируйте банковскую карту и сообщите в банк любым удобным способом:

- через приложение;
- по горячей линии банка;
- обратитесь в офис.

ЕСЛИ У ВАС С БАНКОВСКОЙ КАРТЫ УКРАЛИ ДЕНЬГИ

- Заблокируйте карту.
- Сообщите в банк по горячей линии о краже денежных средств.
- Подайте заявление в полицию.

ЕСЛИ ВЗЛОМАЛИ МЕССЕНДЖЕРЫ

- Проинформируйте о взломе близких, коллег и друзей. По возможности – всех, с кем переписывались в последние дни.
- Завершите работу приложения на всех устройствах – нужно выйти из мессенджера на всех привязанных устройствах (ПК, планшет, смартфон).
- Сообщите о взломе в службу технической поддержки мессенджера.

Иллюстрация: ru.freepik.com

МОШЕННИЧЕСКАЯ АКТИВНОСТЬ:
КАК ОБЕЗОПАСИТЬ СЕБЯ

В основе лифлета – материалы Кибрария, Сбер.

НИЯУ МИФИ

КАК ОБЕЗОПАСИТЬ СЕБЯ

01 | Не отвечайте на видеозвонки с незнакомых номеров в мессенджерах.
02 | Не переходите по подозрительным ссылкам в письмах и сообщениях.
03 | Не сообщайте никому свои пароли, ПИН- и CVV-коды и коды из СМС, даже сотрудникам банка.
04 | Используйте только официальные приложения банков и госсервисов.
05 | Используйте антивирусы.
06 | Сообщайте банку о смене номера мобильного.
07 | Устанавливайте двухфакторную аутентификацию в мессенджерах, приложениях банков и госсервисах (Госуслуги, Мой налог и др.).
08 | Не оставляйте без присмотра банковскую карту.
09 | Не покупайте ничего в сомнительных интернет-магазинах, с общедоступных компьютеров или с использованием бесплатного вайфая.
10 | Если вы потеряли карту или подозреваете, что ваш счёт атакуют мошенники – заблокируйте её.
11 | Нигде не записывайте ПИН-код, никому его не говорите.
12 | Проверяйте выписки с банковских счетов, отслеживайте оповещения об операциях, сообщайте банку о любых несоответствиях.

СХЕМЫ ОБМАНА

1 /// ЗВОНКИ ФЕЙКОВЫХ СОТРУДНИКОВ

• Звонки из медицинских учреждений.
• Звонки от сотового оператора.
• Рабочие звонки: от руководства организации или бывшего начальника.
• Звонок представителя банка или Центробанка.
• Звонки сотрудников Госслужб.
• Звонок из службы финансовой безопасности Центробанка РФ.

! Помните – сотрудники банков и правоохранительных органов никогда не попросят отправить деньги на «защищённый счёт», продиктовать полный номер карты, код из СМС или трёхзначный код на обороте карты (CVV/CVC/CVP).

Из медицинских учреждений не звонят с мобильного телефона и не просят подтвердить свои данные по телефону, а также не сообщают результаты анализов.

Полиция, прокуратура и следователи никогда не вербуют людей по телефону для розыска преступников.

2 /// ПОДДЕЛЬНЫЕ ГОССЕРВИСЫ И БАНКИ. РАСПРОСТРАНЁННЫЕ ФРАЗЫ И УВЕДОМЛЕНИЯ ОТ МОШЕННИКОВ

Если во время звонка или в сообщении вы слышите/видите представленные ниже фразы – скорее всего, это злоумышленники. **Будьте внимательны!**

• Вы откреплены от поликлиники.
• Заплатите новый налог.
• Доверенность от вашего имени разместят на Госуслугах.
• Подпишите документ с помощью Госключа.
• Поддельные электронные письма.
• Вам придёт цифровой код в СМС.
• Скачайте новое приложение.
• Опросы и обещания социальных выплат.

! Не скачивайте файлы, в надёжности которых не уверены. Не переходите по ссылкам и не загружайте файлы из писем, которые получаете от незнакомых людей.

Помните: передавая свои персональные данные незнакомцам, вы становитесь мишенью для мошеннических атак.

3 /// ОБМАН ЧЕРЕЗ ЦИФРОВЫЕ СЕРВИСЫ, МЕССЕНДЖЕРЫ И ПРИЛОЖЕНИЯ

ЧАСТЫЕ СПОСОБЫ ОБМАНА:

• Фиктивные платёжки
Злоумышленники рассылают по электронной почте или в мессенджеры фиктивные платёжки за жилищно-коммунальные услуги.

• Подделка голосовых сообщений и видеозвонков
Преступники с помощью искусственного интеллекта генерируют голосовые обращения, создают высокодетализированные динамические видеоизображения и ложные изображения реальных людей, вымогают деньги.

• Билет на балет
Злоумышленники направляют ссылку на поддельный сайт, который копирует стилистику официального сайта организации.

• Народное голосование
Преступники предлагают проголосовать за участников того или иного конкурса, но при голосовании необходимо ввести данные карты/персональные данные.

• Выплаты через Telegram
В подъездах жилых домов мошенники расклеивают листовки с обещанием разовой выплаты. Требуется перейти на Telegram-канал, где вам предоставляют якобы ссылку банка, через которую проведут выплату.

• Праздничные акции
Преступники отправляют в мессенджер сообщение с предложением принять участие в праздничной акции от имени одного из магазинов и выиграть подарок.

• Большой приз
Злоумышленники от имени крупных маркетплейсов приглашают принять участие в масштабном проекте. Обещают розыгрыш сертификатов и щедрый денежный приз.

! Не переходите по сомнительным ссылкам и не сканируйте QR-коды, которые вызывают подозрение. Не скачивайте файлы из писем незнакомых людей.

В основе лифлета – материалы Кибрария, Сбер.