



Рег. номер: 1/3496.
Рег. дата: 18.03.2023

М В Д Р о с с и и

УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО УЛЬЯНОВСКОЙ ОБЛАСТИ
(УМВД России по Ульяновской области)

ул. К. Маркса, 31/10, Ульяновск, 432071

18.03.2023 № 1/3496

на № _____ от _____

Министру социального развития
Ульяновской области

А.А. Тверской

Об оказании содействия

Уважаемая Анна Александровна!

В качестве дополнительных мер профилактики преступлений в сфере компьютерной информации, телефонных и банковских мошенничеств эффективными мерами профилактического воздействия являются демонстрация тематических видеороликов, размещение памяток в местах массового скопления людей, проведение разъяснительной работы с населением с целью повышения уровня правовой грамотности.

УМВД России по Ульяновской области активно использует ведомственные информационные ресурсы для доведения до общественности информации о наиболее актуальных мошеннических схемах и размещения рекомендаций как не стать жертвой противоправных действий.

С целью предупреждения сотрудников структурных подразделений Министерства социального развития Ульяновской области о мошеннических действиях направляю образцы профилактических памяток, QR-код с ссылкой на файлообменник с мультимедийным контентом по профилактике мошеннических действий, QR-коды для получения мгновенного доступа к официальным аккаунтам УМВД в социальных сетях, на страницах которых ежедневно размещаются материалы об актуальных для нашего региона мошеннических схемах. Также мультимедийный контент доступен по ссылке: <https://cloud.mail.ru/public/B44H/m26uxSxC>.

В соответствии со статьей 10 Федерального закона от 07.02.2011 N 3-ФЗ "О полиции" в части оказания государственными и муниципальными органами содействия полиции при выполнении возложенных на нее обязанностей прошу до 5 апреля 2023 года проинформировать УМВД России по Ульяновской области (mvd73@mvd.gov.ru) о результатах использования Министерством направляемых материалов.

Приложение: по тексту, на 7 л. в 1 экз.

Начальник

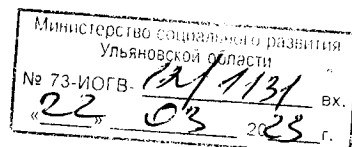
исп. И.Ю. Селюкова
тел.8(8422) 67 85 92



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

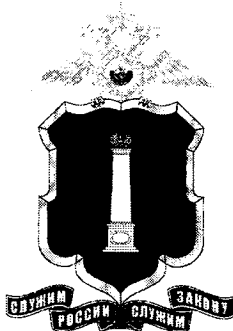
Сертификат 4050ЕС1ВА1Е590С9СЗВВВ28С1057С919
Владелец Петрушин Максим Юрьевич
Действителен с 03.02.2022 по 29.04.2023

М.Ю. Петрушин

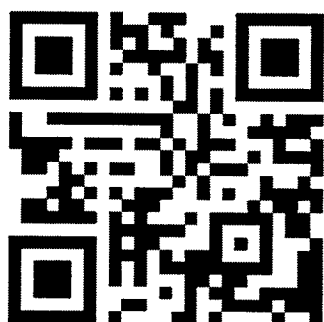


**QR-код со ссылкой на файлообменник
с мультимедийным контентом
по профилактике мошеннических
действий**

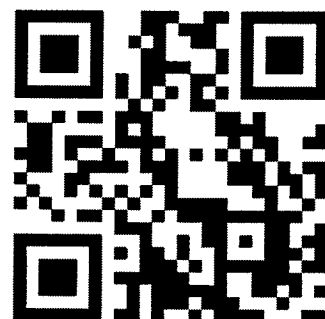




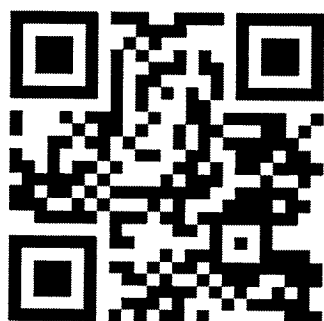
**На этих ресурсах
УМВД России по Ульяновской области
вы можете узнать о том как
не стать жертвой мошенников:**



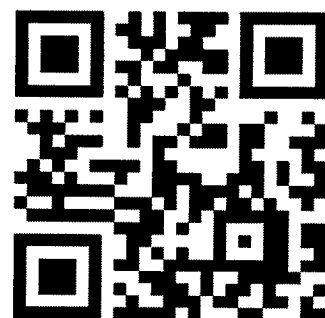
**Аккаунт в «ВКонтакте»
<https://vk.com/umvd73>**



**Аккаунт в «Телеграм»
https://t.me/mvd_73**



**Аккаунт в
«Одноклассниках»
<https://ok.ru/umvd73>**



**Интернет-сайт
УМВД России по
Ульяновской области
73.mvd.rf**

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо – повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность



3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

! ВАЖНО!

Сотрудники банков и полиции **НИКОГДА** не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

! НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные



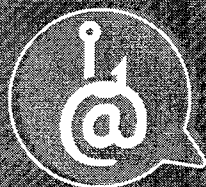
Как защитить свои финансы,
читайте на fincult.info



Финансовая
культура

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

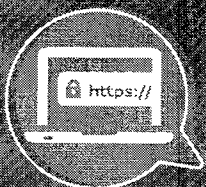
Фишинг — вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций



КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

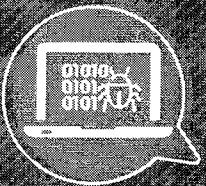
По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

- ! Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых



КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- Адрес отличается от настоящего лишь парой символов
- В адресной строке нет `https` и значка закрытого замка
- Дизайн скопирован некачественно, в текстах есть ошибки
- У сайта мало страниц или даже одна — для ввода данных карты



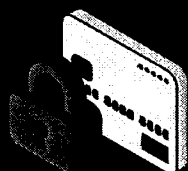
КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- Установите антивирус и регулярно обновляйте его
- Сохраняйте в закладках адреса нужных сайтов
- Не переходите по подозрительным ссылкам
- Используйте отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой



ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ



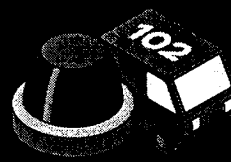
- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ



- Заявление должно быть написано:
- в течение суток после сообщения о списании денег
 - на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ



Чем больше людей подадут заявления, тем выше вероятность, что преступников поймут

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты



Подробнее о правилах безопасности
читайте на fincult.info



Финансовая
культура

020 ! МОШЕННИКИ !

НЕ СООБЩАЙТЕ ДАННЫЕ
БАНКОВСКОЙ КАРТЫ
НЕИЗВЕСТНЫМ ЛИЦАМ

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ
НА НЕИЗВЕСТНЫЕ РАСЧЕТНЫЕ
СЧЕТА И ТЕЛЕФОННЫЕ НОМЕРА

НЕ ПОСЕЩАЙТЕ НЕИЗВЕСТНЫЕ САЙТЫ



НЕ ОТКРЫВАЙТЕ ДВЕРЬ
ПОДОЗРИТЕЛЬНЫМ ЛИЦАМ

БУДЬТЕ БАДТЕЛЬНЫ
ПРИ ПОКУПКЕ
НЕИЗВЕСТНЫХ ТОВАРОВ

ВЕРНУТЬ АВТОМОБИЛЬ
ЗА ВОЗНАГРАЖДЕНИЕ

РОДСТВЕННИК В БЕДЕ

АНОНИМНОЕ СООБЩЕНИЕ
С ПРОСЬБОЙ ПОПОЛНИТЬ БАЛАНС

ВАША КАРТА ЗАБЛОКИРОВАНА

ЧУДОДЕЙСТВЕННЫЕ ТАБЛЕТКИ

**БУДЬТЕ БДИТЕЛЬНО
И НЕ ПОДАВАЙТЕСЬ
НА УЛОВКИ МОШЕННИКОВ!**



Полиция предупреждает!



Правительство
Ульяновской
области

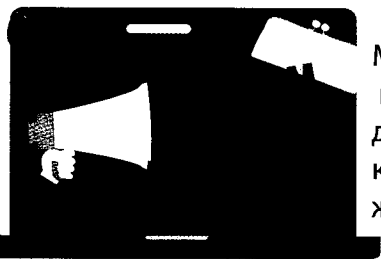
ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ



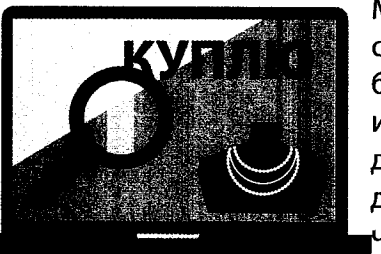
ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ



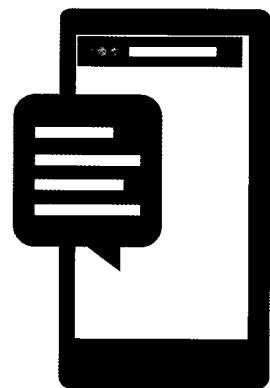
Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ



Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

СООБЩЕНИЯ ОТ ДРУЗЕЙ



Мошенник пользуется чужой страничкой в социальной сети в Интернете и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предложениями.

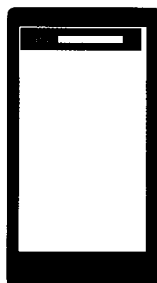
ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ



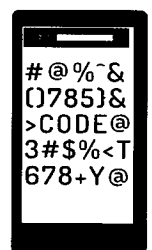
Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель - узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША



(компенсации за потерянный вклад) Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату «за сохранение денег».

ВИРУС В ТЕЛЕФОНЕ



Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не переходите по сомнительным ссылкам.