



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

МВД России

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](mailto:mvd73@mvd.gov.ru)) о результатах использования Министерством направляемых материалов.

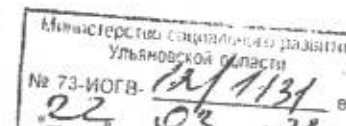
Приложение: по тексту, на 7 л. в 1 экз.

Начальник

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



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](https://t.me/mvd_73)**



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

**Интернет-сайт  
УМВД России по  
Ульяновской области  
[73.mvd.rf](https://73.mvd.rf)**



## УМВД России по Ульяновской области предупреждает

В последнее время на территории Ульяновской области участились случаи мошеннических действий. Для совершения которых преступники используют следующие способы и предлоги.



1. Сообщение по телефону, что ваш родственник совершил ДТП, попал в полицию за правонарушение, преступление;



2. SMS-сообщения, телефонные звонки с информацией о том, что ваша банковская карта заблокирована;



3. Звонки, якобы, из поликлиники с сообщением, что у вас или ваших родственников нашли неизлечимую болезнь;



4. Необходимо «снять порчу», провести ритуал;



5. Представляясь сотрудниками собеса, почты, службы газа преступники входят в доверие и сообщают о обмене денежных средств, о предоставлении от различных государственных организаций подарков, продовольственных заказов;



6. Находясь около магазинов, банков, незнакомые лица сообщают о проведении различных акций в которых необходимо предоставить имеющиеся у вас денежные сбережения;



7. Объявления в интернет ресурсах о продаже авто-, мототранспортных средств, различных вещей и предметов, где просят сделать предоплату.

# ОСТОРОЖНО, МОШЕННИКИ!

**В случаях обращения к вам  
незнакомых граждан  
при вышеуказанных обстоятельствах  
незамедлительно обращайтесь  
в отдел полиции вашего района  
или по телефону дежурной части  
УМВД России по Ульяновской области**

**42-29-60 02**

# ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!



## МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- Сотрудником Банка
- Сотрудником службы безопасности банка
- Сотрудником больницы
- Сотрудником благотворительной организации
- Родственником

ОН

## МОЖЕТ ПОПРОСИТЬ:

### Данные карты:



- номер карты
- CVV/CVC-код
- PIN-код
- срок действия карты

### Пароль:



- от интернет-банка;
- из SMS-сообщения (для входа в интернет-банк или подтверждения операции)

### Перевести деньги:



- на специальный счет или карту, где они будут в безопасности

НЕ



- сообщайте никому данные карты
- сообщайте никому пароли и коды из SMS
- выполняйте действия с банковской картой по просьбе третьих лиц



## 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



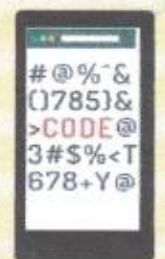
Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель - узнать личный код банковской карты.

#### 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



Банк России

# 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



Подробнее о правилах кибергигиены читайте на [fincult.info](http://fincult.info)



Финансовая  
культура



Банк России

## 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 поймают

## 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](http://fincult.info)



Финансовая  
культура



# НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

## **SMS-ПРОСЬБА О ПОМОЩИ**

ТРЕБОВАНИЕ ПЕРЕВЕСТИ ОПРЕДЕЛЁННУЮ СУММУ НА УКАЗАННЫЙ НОМЕР. ИСПОЛЬЗУЕТСЯ ОБРАЩЕНИЕ «МАМА», «СЫНОК», «ДРУГ» И Т.Д.

## **ТЕЛЕФОННЫЙ НОМЕР-«ГРАБИТЕЛЬ»**

ПЛАТНЫЙ НОМЕР, ЗА ОДИН ЗВОНОК НА КОТОРЫЙ, СО СЧЁТА СПИСЫВАЕТСЯ ДЕНЕЖНАЯ СУММА

## **ОБМАН ПО ТЕЛЕФОНУ**

ТРЕБОВАНИЕ ВЫКУПА, ВЗЯТКИ ЗА ОСВОБОЖДЕНИЕ ИЗ ОТДЕЛЕНИЯ ПОЛИЦИИ РОДСТВЕННОКА ИЛИ ЗНАКОМОГО

## **ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ**

ПРОСЯТ ВЕРНУТЬ ДЕНЬГИ, А ПОТОМ ДОПОЛНИТЕЛЬНО СНИМАЮТ СУММУ ПО ЧЕКУ

## **ПРОСТОЙ КОД ОТ ОПЕРАТОРА СВЯЗИ**

ПРЕДЛОЖЕНИЕ УСЛУГИ - ДОСТАТОЧНО ВВЕСТИ КОД, КОТОРЫЙ НА САМОМ ДЕЛЕ ЗАБЛОКИРУЕТ ВАШУ SIM-КАРТУ

## **УСЛУГА, ЯКОБЫ, ПОЗВОЛЯЮЩАЯ ПОЛУЧИТЬ ДОСТУПК SMS И ЗВОНКАМ ДРУГОГО ЧЕЛОВЕКА**

## **ШТРАФНЫЕ САНКЦИИ И УГРОЗА ОТКЛЮЧЕНИЯ НОМЕРА**

ЯКОБЫ, ЗА НАРУШЕНИЕ ДОГОВОРА С ОПЕРАТОРОМ ВАШЕЙ МОБИЛЬНОЙ СВЯЗИ

## **ВЫИГРЫШ В ЛОТЕРЕЕ, КОТОРУЮ, ЯКОБЫ, ПРОВОДИТ ОПЕРАТОР СВЯЗИ ИЛИ РАДИОСТАНЦИЯ**

ВАС ПРОСЯТ ПРИОБРЕСТИ КАРТЫ ЭКСПРЕСС-ОПЛАТЫ И СООБЩИТЬ КОДЫ, ЛИБО ПЕРЕВЕСТИ КРУПНУЮ СУММУ НА СВОЙ СЧЁТ, А ЗАТЕМ ВВЕСТИ СПЕЦИАЛЬНЫЙ КОД

# ПОМНИТЕ!

# ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ!

- ОТМЕТЬТЕ В ТЕЛЕФОННОЙ КНИЖКЕ МОБИЛЬНОГО ТЕЛЕФОНА НОМЕРА ВСЕХ РОДСТВЕННИКОВ ДРУЗЕЙ И ЗНАКОМЫХ

- НЕ РЕАГИРУЙТЕ НА SMS-СООБЩЕНИЯ БЕЗ ПОДПИСИ С НЕЗНАКОМЫ НОМЕРОВ

- ОСТОРОЖНО ОТНОСИТЕСЬ К ЗВОНКАМ С НЕЗНАКОМЫХ НОМЕРОВ

ЕСЛИ ВЫ СОМНЕВАЕТЕСЬ, ЧТО ЗВОНИВШИЙ - ДЕЙСТВИТЕЛЬНО ВАШ ДРУГ ИЛИ РОДСТВЕННИК, ПОСТАРАЙТЕСЬ ПЕРЕЗВОНИТЬ НА ЕГО МОБИЛЬНЫЙ ТЕЛЕФОН. ЕСЛИ ТЕЛЕФОН ОТКЛЮЧЁН, ПОСТАРАЙТЕСЬ СВЯЗАТЬСЯ С ЕГО КОЛЛЕГАМИ, ДРУЗЬЯМИ ИЛИ БЛИЗКИМИ ДЛЯ УТОЧНЕНИЯ ИНФОРМАЦИИ.

## БУДЬТЕ БЛИТЕЛЬНЫ И ВНИМАТЕЛЬНЫ!

# Информационный стенд в учреждении

## ИНФОРМАЦИЯ

**ОСТОРОЖНО МОШЕННИКИ!**

- 1. Вам предлагают работу, которую вы не выполняли раньше.
- 2. Вам предлагают работу, которую вы не выполняли раньше.
- 3. Вам предлагают работу, которую вы не выполняли раньше.
- 4. Вам предлагают работу, которую вы не выполняли раньше.
- 5. Вам предлагают работу, которую вы не выполняли раньше.
- 6. Вам предлагают работу, которую вы не выполняли раньше.
- 7. Вам предлагают работу, которую вы не выполняли раньше.
- 8. Вам предлагают работу, которую вы не выполняли раньше.
- 9. Вам предлагают работу, которую вы не выполняли раньше.
- 10. Вам предлагают работу, которую вы не выполняли раньше.

22-70-60 02

QR-код по ссылке на информационный ресурс

22-70-60 02

QR-код по ссылке на информационный ресурс

22-70-60 02

**УСТАНОВИТЕ СЛУЖБУ ПРОТЕКЦИИ ПОЛЬЗОВАТЕЛЕЙ**

ОН ПОПРОСИТЬ

**ОСТОРОЖНО МОШЕННИКИ**

НЕ ДАЙТЕ СЕБЕ ОБМАНУТЬ

**КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА**

**ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?**

**КАКОВАЯ РАБОТА У МОШЕННИКОВ**

**ПОМНИТЕ!**