

ДЕСТРУКТИВНОЕ ПОВЕДЕНИЕ!

Под давлением или принуждением мошенников Вы можете стать участником преступления (совершить поджог и т.д.), за что предусмотрена уголовная ответственность: ст. 167 УК РФ «Умышленное уничтожение или повреждение имущества» предусматривает наказание до 5 лет лишения свободы; ст. 205 УК РФ «Тerrorистический акт» предусматривает наказание вплоть до пожизненного лишения свободы; ст. 275 УК РФ «Государственная измена» предусматривает наказание вплоть до пожизненного лишения свободы;

Что такое «Самозапрет»?

Это значит, что с 01 марта 2025 г. гражданин может посредством сервиса «Госуслуги» или путем обращения в МФЦ установить в своей кредитной истории самозапрет на заключение с ним кредитными организациями и (или) микрофинансовыми организациями договоров потребительского кредита (займа).

Что такое период «Охлаждения»?

Это значит, что денежные средства с 01 сентября 2025 г. по кредиту или займу от 50 тыс. до 200 тыс. рублей можно будет получить только через 4 часа после заключения договора.

Если сумма превышает этот порог, то средства перечислят не раньше, чем через 48 часов.

Кто такие и чем занимаются ДРОППЕРЫ?

Получают на свои банковские карты деньги от незнакомцев и передают их другим лицам наличными или переводом;

Предоставляют злоумышленникам банковские карты или доступ к онлайн банку;

Принимают (забирают) наличные денежные средства от неизвестных людей, вносят их на свои счета для последующего перевода.

За проделанную работу дропперы получают денежное вознаграждение.

Что грозит ДРОППЕРАМ:

- уголовная ответственность за соучастие в преступлении (ст. 159 УК РФ «Мошенничество», предусматривает наказание до 10 лет лишения свободы)

Уважаемые жители Воронежской области! Будьте осторожны!

В 2024 году жертвами «телефонных мошенников» стали более 5 тысяч жителей Воронежской области.

Причиненный материальный ущерб составил порядка 2.5 млрд. рублей, из которых половина являлась заемными (кредитными) денежными средствами.

Лишились недвижимого имущества более 20 граждан.

В 5 случаях потерпевшие по указанию мошенников впоследствии стали участниками преступлений, а именно совершили поджоги чужого имущества.

Переходи по ссылке, повысь свой уровень кибербезопасности



Полиция
Воронежской
области

t.me/mvd36

Вестник
Киберполиции
России
t.me/cyberpolice_rus



Правительство
Воронежской области

БУДЬТЕ БДИТЕЛЬНЫ!



НЕ СТАНЬТЕ ЖЕРТВОЙ МОШЕННИКОВ!



Управление МВД России
по г. Воронежу

Не станте жертвой мошенников!

Основными предлогами являются:

Продление договора с оператором связи:

Уведомление об истечении срока действия договора связи и необходимости его продления. Требования операторов сотовой связи предоставить код из СМС-сообщения;

Звонок от представителя банковских учреждений и правоохранительных органов:

Звонящий сообщает, что Вам необходимо участвовать в «спецоперации» по поимке мошенников, которые получили доступ к Вашим счетам;

Двухэтапное давление на пользователя:

При первом звонке явно дают понять, что разговаривает мошенник. Затем звонят во второй раз – якобы представитель банка (либо сотрудник ФСБ, МВД, Росфинмониторинга и т.д.), который предлагает обезопасить счета после звонка мошенника.

Предложение разблокировать якобы заблокированный из-за подозрительной активности аккаунт:

например в Госуслугах или банке.

Доставка архивного письма из отделения почты или службы доставки:

Просят назвать код из СМС, либо перейти по ссылке

Предложение о бесплатной замене счетчиков:

Просят назвать код из СМС, либо перейти по ссылке

Мошенничество в онлайн - игре «Roblox»:

Получают доступ к банковской карте путем продажи игровой валюты по заниженной стоимости, минуя игровую площадку;



МИНИСТЕРСТВО ФИНАНСОВ
ВОРОНЕЖСКОЙ ОБЛАСТИ

Распространение файлов в мессенджерах с расширением .APK (Android Package Kit) под видом голосования, фото и видеофайлов:

Данный файл может являться вредоносным;

Письма-штрафы с QR-кодом:

При переходе по которым злоумышленник получает доступ к банковским реквизитам. Необходимо использовать только официальные сервисы проверки штрафов;

Бронирование поездки «BlaBlaCar»:

Якобы для бронирования поездки нужно подтвердить свои намерения по ссылке, которая является фишинговой;

Авто-доставка:

Просят перейти по внешней ссылке, которую указывают в переписке на «Авито». Безопасную сделку можно оформить исключительно в самом сервисе;

Звонок от руководителя (бывшего руководителя, коллеги по работе, близкого знакомого):

Как правило в мессенджере, с его похищенного аккаунта, с просьбой занять денежные средства

Предложение подработки:

От оформления и передачи sim или банковской карты до получения неизвестных посылок.

Выигрыш в конкурсе, лотерее:

Просят назвать код из СМС, либо перейти по ссылке

ПОМНИТЕ:

Если Вы или Ваши близкие стали жертвами мошенников или Вы подозреваете, что в отношении Вас планируются противоправные действия - незамедлительно обратитесь в полицию!

ЗВОНИТЕ 02 или 112 !

Вам обязательно помогут!



Как защититься от мошенников

- недопустимо доверять «официальным» звонкам и сообщениям вслепую, **НЕ ОТВЕЧАТЬ НА ЗВОНИКИ В МЕССЕНДЖЕРАХ, ПОСТУПАЮЩИХ С НЕИЗВЕСТНЫХ НОМЕРОВ;**
- запомнить, что **БЕЗОПАСНЫХ СЧЕТОВ НЕ СУЩЕСТВУЕТ;**
- не делиться своими персональными данными, **НЕ НАЗЫВАТЬ КОДЫ ИЗ СМС;**
- при регистрации на различных сервисах в сети Интернет использовать **СЛОЖНЫЕ ПАРОЛИ;**
- **НЕ ПЕРЕХОДИТЬ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ**, это может привести к хищению персональной информации, в том числе данных о банковских картах и платежных реквизитах;
- **НЕ СКАЧИВАТЬ ФАЙЛЫ ИЗ НЕНАДЕЖНЫХ ИСТОЧНИКОВ**, это повышает риск заражения персонального компьютера или мобильного устройства. Устанавливать приложения и файлы с расширениями .ipk (для устройств с операционной системой iOS), .apk (для устройств с операционной системой Android) только из официальных приложений: «App Store», «Google Store», «RuStore», «GetApps»;
- **НЕДОПУСТИМО СОВЕРШАТЬ ДЕЙСТВИЯ ПОД ДИКТОВКУ НЕЗНАКОМЦЕВ, КЕМ БЫ ОНИ НЕ ПРЕДСТАВЛЯЛИСЬ;**

**НИКОГДА НЕ СООБЩАЙТЕ
НЕЗНАКОМЫМ ЛЮДЯМ
ТРЕХЗНАЧНЫЙ КОД
НА ОБОРОТЕ КАРТЫ,
PIN-КОД И ПАРОЛИ ИЗ СМС,
КЕМ БЫ ОНИ
НЕ ПРЕДСТАВЛЯЛИСЬ**