ЧТО ТАКОЕ «САМОЗАПРЕТ»?

Это значит, что с 01.03 2025 г. гражданин может посредством сервиса «Госуслуги» или путём 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 01.09.2025 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.

Уважаемые жители Воронежской области! Будьте осторожны!

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

Причинённый материальный **ущерб** составил порядка, **2.5 млрд. рублей** из которых половина являлась заёмными (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.

Переходите по ссылке, повысьте свой уровень кибербезопасности

Полиция Воронежской области

t.me/mvd36

Партия «Новые люди»

t.me/newpeople_voronezh

ПАРТИЯ НОВЫЕ ЛЮДИ

БУДЬТЕ БДИТЕЛЬНЫ!

НЕ СТАНЬТЕ ЖЕРТВОЙ МОШЕННИКОВ!

УПРАВЛЕНИЕ МВД РОССИИ ПО Г. ВОРОНЕЖУ

Не станьте 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

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

Авито-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

КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ?

- недопустимо доверять «официальным» звонкам и сообщениям вслепую, **не отвечать на звонки 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 ненадёжных 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