



Министерство внутренних дел Республики Беларусь

Служим Закону, Народу, Отчизне!

Кибербезопасность

04.02.2026 Киберпреступность

Актуальные мошеннические аккаунты в социальных сетях, с помощью которых распространяется ложная информация о продаже товаров и оказании услуг

Информация об актуальных мошеннических аккаунтах в социальных сетях, с помощью которых распространяется ложная информация о продаже товаров и оказании услуг

Мошенники не дремлют и постоянно придумывают новые способы обмана. Вам звонят из банка и просят сообщить данные карты? Будьте осторожны – это может быть вишинг! Узнайте, как защитить себя от мошенников, посмотрев новый видеоролик «ВИШИНГ-Азбука цифровой безопасности».

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ

01

НЕОБХОДИМО:

- + Создавать персональные (уникальные) пароли к разным сервисам
- + Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
- + Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

- × Использовать повторения символов
- × Хранить пароли на бумажных носителях
- × Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
- × Сохранять пароль автоматически в браузере
- × Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI

02

- + Отключить общий доступ к своей Wi-Fi точке, даже если у вас «безлимитный» Интернет
- + Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
- + Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам
- × Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ

Как не превратить iPhone в кирпич.

Мошенники используют различные уловки, чтобы заблокировать ваше устройство, вынуждая войти в их учетную запись Apple (iCloud)

Основные схемы обмана

- «Получи с файлом»
- «Забудь твои игры и приложения»
- «Работа/работайка»

Как защитить себя

- Не скачивай файлы с сомнительных источников
- Не вводи данные Apple ID
- Не вводи данные Apple ID на сомнительных сайтах
- Не вводи данные Apple ID на сомнительных сайтах

ВАЖНО!

Если вы видите заблокированное устройство, обратитесь в службу поддержки. Репаратура возможна только через официальную службу поддержки Apple при наличии документов, подтверждающих покупку устройства.

Безопасный интернет для детей

Не сообщай личными свои логины и пароли

Не открывай файлы из непроверенных источников

Не заходи на сайты, которые защита компьютера считает подозрительными

СОХРАНИ ИНФОРМАЦИЮ

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Не стройся с сайтами, которые выдают задание

Не сообщай в интернете свои реальные адрес и телефон

Не сообщай о своем адресе и телефоне в интернете

Не сообщай о своем адресе и телефоне в интернете

РОДИТЕЛИ! Научите детей пользоваться интернетом правильно!

Не дай себя обмануть!

Круглосуточный единый номер 102

БЕЗОПАСНЫЙ ИНТЕРНЕТ ДЛЯ ДЕТЕЙ

Не сообщай знакомым свой логин и пароль

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Не открывай файлы из непроверенных источников

Не заходи на сайты, которые защита компьютера считает подозрительными

СОХРАНИ ИНФОРМАЦИЮ

Не дай себя обмануть!

Круглосуточный единый номер 102

ВНИМАНИЕ! МОШЕННИЧЕСТВО!

Мама, папа, я в беде! Нужны деньги Срочно!

Что делать?

- немедленно положить трубку
- самому позвонить родственнику
- не передавать курьерам никаких денег
- сообщить в полицию

Не дай себя обмануть!

Круглосуточный единый номер 102

устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)

к письму, сначала позвоните отправителю и узнайте, что это за файл

+ Использовать СПАМ-фильтры

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ 05

- + Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
- + Обращать внимание, к каким функциям гаджета приложение запрашивает доступ
- + Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

- × Размещать персональную и контактную информацию о себе в открытом доступе
- × Использовать указание геолокации на фото в постах
- × Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса
- × Употреблять ненормативную лексику при общении
- × Устанавливать приложения с низким рейтингом и отрицательными отзывами

В соответ
токены и ис

Действие
Беларусь

При необ

Чтобы не

- зарегис
надежнос

- после со

- выбери
высокори

Таким об
криминал

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ

- + Хранить в тайне пин-код карты
- + Прикрывать ладонью клавиатуру при вводе пин-кода
- + Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
- + Использовать услугу «3-D Secure» и лимиты на максимальные суммы онлайн-операций
- + Скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

- × Хранить пин-код вместе с карточкой / на карточке
- × Сообщать CVV-код или отправлять его фото
- × Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет-банкинг»
- × Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.

продавать

спублики

в ПВТ.

зантирует
схем;

ются как

не имеет

Законные сделки с криптовалютой



Убедитесь, что Ваши сделки соответствуют действующему законодательству Республики Беларусь

Порядок осуществления сделок с криптовалютой определен Декретом Президента Республики Беларусь от 21 декабря 2017 г. №8 «О развитии цифровой экономики» и Указом Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)»

В Республике Беларусь физическим лицам:

✓ РАЗРЕШЕНО

Добыча криптовалюты в результате майнинга (как на территории Республики Беларусь, так и на территории иностранного государства)

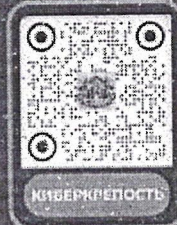
Продажа (покупка) криптовалюты за денежные средства на белорусских криптоплатформах, являющихся резидентами Парка высоких технологий

Обмен криптовалюты на иные токены (на белорусских и иностранных криптоплатформах)

Получение криптовалюты в дар или наследство

БОЛЬШЕ ИНФОРМАЦИИ

В Telegram-канале
КИБЕРКРЕПОСТЬ
CYBER_FORTRESS_BREST



✗ ЗАПРЕЩЕНО

Продажа (покупка) криптовалюты за денежные средства на иностранных криптоплатформах

Продажа (покупка) криптовалюты за денежные средства напрямую между физическими лицами



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:



Получить кредит, чтобы отменить якобы оформленный неизвестными на ваше имя другой кредит и перевести деньги на специальный счет

Установить программное обеспечение, якобы для предотвращения мошеннической атаки на ваш счет

Перевести накопления на якобы безопасный счет, чтобы не изъяли при обыске

Передать личные данные и код из SMS, такие сведения предоставляют мошенникам доступ к счету или сервису

ОСТОРОЖНО! МОШЕННИЧЕСТВО!

В СОЦИАЛЬНЫХ СЕТЯХ И НА ТОРГОВЫХ ПЛОЩАДКАХ:

Перевести предоплату за несуществующий товар в лэмагазине или по измененным реквизитам банка

Перейти по поддельной ссылке банковской системы и ввести личные данные (логин и пароль, номер и трехзначный код с оборотной стороны банковской карты, код из SMS, кодовое слово)

Перечислить деньги на карту или оплатить родственнику, другу, любящему человеку

На поддельной бирже вложить деньги в проект, якобы для получения пассивного дохода

МОШЕННИКИ УБЕЖДАЮТ, представляясь продавцами, друзьями, партнерами по бизнесу, руководителями инвестиционных проектов



Больше информации на сайте <https://mvd.gov.by>



Главное управление по противодействию киберпреступности КМ МВД Республики Беларусь

Телефонные МОШЕННИКИ

ПРЕДСТАВЛЯЮТСЯ:

- сотрудниками гос. органов и банков
- продавцами, инвесторами, брокерами
- работниками служб связи (Белпочта, Белтелеком, А1, МТС)
- работниками коммунальных служб (энергонадзора, водоканала, газовой службы)


УГРОЖАЮТ И ЗАПУГИВАЮТ:

- подозрением в преступлении и проведением обыска
- сложной ситуацией с родственником
- окончанием действия прибора учета или услуги

УБЕЖДАЮТ И ЗАСТАВЛЯЮТ:

- под предлогом декларирования перевести деньги на "безопасный" счет
- внести предоплату за товар или взнос в инвестиционный проект
- передать личные данные и коды из сообщения, установить приложение

Не дайте себя обмануть!

 Главное управление по противодействию киберпреступности
КМ МВД Республики Беларусь

В настоящее время функционируют следующие основные ресурсы.

Telegram-каналы:

«КИБЕРКРЕПОСТЬ» – УПК КМ УВД Брестского облисполкома;

«Цифровая грамотность» – УПК КМ УВД Витебского облисполкома.

Telegram-боты:

«MINOBL STOP SCAM» – УПК КМ УВД Минского облисполкома (совместно с ОПК КМ Борисовского РУВД);

«@ScamBY_bot» – УПК КМ ГУВД Мингорисполкома;

«AntiScamBot» (@k_AntiScamBot) – УПК КМ УВД Гродненского облисполкома;

«КиберЩит»;

«Киберпрофилактика»;

<https://mvd.gov.by/ru/news/7021/print>

«Кибердетектив» – УПК КМ УВД Брестского облисполкома.

Адрес страницы в интернете: <https://mvd.gov.by/ru/news/7021>

2026 © Министерство внутренних дел Республики Беларусь