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 03

+ Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

× Переходить по непроверенным ссылкам
× Вводить информацию на сайтах, если соединение не защищено (нет https и 🔒)

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ 04

НЕОБХОДИМО:

+ Подключить двухфакторную аутентификацию
+ Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)
+ Использовать СПАМ-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

× Реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники
× Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ 05

+ Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
+ Обращать внимание, к каким функциям

× Размещать персональную и контактную информацию о себе в открытом доступе
× Использовать указание геолокации на фото в постах

гаджета приложение запрашивает доступ

+ Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

× 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

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ 06

+ 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.

Инфографика

Если Вы стали жертвой киберпреступников, обращайтесь в главное управление по противодействию киберпреступности криминальной милиции МВД Республики Беларусь

Законные сделки с криптовалютой

В соответствии с Указом Президента "Об обращении цифровых знаков (токенов)" разрешено покупать и продавать токены исключительно через резидентов Парка высоких технологий.

Действие установленного порядка распространяется на всех лиц, находящихся на территории Республики Беларусь или использующих платежные карты, эмитированные банками нашей страны.

При необходимости продажи купленных ранее токенов сделать это можно также посредством резидентов ПВТ.

Чтобы не нарушить закон при покупке цифровых знаков, следуйте следующим правилам:

- зарегистрируйтесь на белорусской криптобирже, пройдя процедуру верификации. Площадка гарантирует надежность, возможность легко подтвердить свои доходы от криптовалюты, отсутствие мошеннических схем;

- после создания аккаунта пополните счет с помощью банковской карты или перевода;

- выберите доступные к покупке криптовалюты, которые зарекомендовали себя и не характеризуются как высокорисковые. Это гарантия не потерять сбережения.

Таким образом, вы сможете быть уверены, что соблюдаете нормы законодательства, а ваш актив не имеет криминального прошлого.


ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:
МОШЕННИКИ УБЕЖДАЮТ, представляясь сотрудниками правоохранительных органов, банковских организаций или руководителем вашей организации.
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 смс, такие сведения предоставляют мошенникам доступ к счету или сервису
ОСТОРОЖНО! МОШЕННИЧЕСТВО!
В СОЦИАЛЬНЫХ СЕТЯХ И НА ТОРГОВЫХ ПЛОЩАДКАХ:
Перевести предоплату за несуществующий товар в лжемагазине 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 СМС, 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

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»;

«Кибердетектив» – УПК КМ УВД Брестского облисполкома.

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