

# 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 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

## 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.

# 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

## 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 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 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 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

# 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](#)



КИБЕРКРЕПОСТЬ

## ✗ 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

# Как не превратить iPhone в «кирпич»

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

## Основные схемы обмана

- ❌ **«Помощь с файлами»**  
Ссылаясь на «неисправное устройство», просят помощи в доступе к файлам (фотографиям, документам и т.д.) из облачного хранилища iCloud путем авторизации в мошеннической учётной записи
- ❌ **«Бесплатные игры и приложения»**  
Рекламируют доступ к играм («PUBG Mobile», «Standoff 2») и приложениям («AioGram») в TikTok или Telegram, предлагая установить их через предоставленный аккаунт Apple
- ❌ **«Работа/подработка»**  
Обещают вакансию (часто связанную с тестированием приложений), но требуют входа в «корпоративный» аккаунт Apple

## Как защитить себя

- ✓ не сообщайте никому свои учётные данные (логин и пароль) от аккаунта Apple (iCloud)
- ✓ не входите на своём мобильном устройстве в аккаунт Apple (iCloud), предоставленный незнакомцами из Интернета
- ✓ не переходите по неизвестным ссылкам и не вводите данные Apple ID на посторонних сайтах

## ВАЖНО!

Если ваш аккаунт заблокирован мошенником, сервисные центры не помогут. Разблокировка возможна только через официальную техподдержку Apple при наличии документов, подтверждающих покупку устройства.

БОЛЬШЕ ИНФОРМАЦИИ

В Telegram-канале  
КИБЕРКРЕПОСТЬ  
CYBER\_FORTRESS\_BREST



Главное управление  
по противодействию  
киберпреступности  
КМ МВД Республики Беларусь

# БЕЗОПАСНЫЙ WI-FI

## Рекомендуется:



отключить общий доступ к своей точке Wi-Fi, даже если у вас безлимитный интернет;



использовать надежный пароль для доступа к своей точке Wi-Fi;



выключить автоматическое подключение своих устройств к точкам Wi-Fi.

## ВАЖНО ПОНИМАТЬ,

что многие уязвимости в защите возникают из-за устаревшего ПО, поэтому обязательно установите все последние обновления для своего ноутбука или телефона.

## Не рекомендуется:

доверять открытым точкам Wi-Fi: именно такие сети используют злоумышленники для воровства личных данных пользователей;



вводить свой логин и пароль доступа к учетной записи или системе банковского обслуживания при подключении к бесплатным точкам Wi-Fi.



# ВНИМАНИЕ!

## БЕРЕГИТЕ СВОИ ДЕНЬГИ

УЧАСТИЛИСЬ СЛУЧАИ ХИЩЕНИЯ ДЕНЕГ С БАНКОВСКИХ КАРТ-СЧЕТОВ!



Если вам пришло сообщение в мессенджере, социальных сетях или по электронной почте...



... в котором говорится, что банковская карта заблокирована и предлагается разблокировать ее, пройдя по ссылке...



... ни в коем случае не переходите по ссылке!  
Незамедлительно обращайтесь в службу безопасности банка!

### Если вы получили сообщение о блокировке банковской карты:

- не переходите по прикрепленной ссылке;
- никуда не пересылайте свои данные;
- проверьте баланс своей карты в банкомате, инфокиоске, мобильном или интернет-банкинге;
- обратитесь в службу безопасности банка.



Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь



# Безопасный интернет для детей

**СОХРАНИ  
ИНФОРМАЦИЮ**

**не сообщай незнакомцам  
свой логин и пароль**

**не открывай файлы из  
непроверенных источников**

**не заходи на сайты, которые  
защита компьютера считает  
подозрительными**



**НЕ отправляй незнакомцам  
свои фото и видео**

Злоумышленники могут узнать что-то  
нужное им о твоей жизни



**НЕ встречайся с людьми,  
с которыми знакомишься только  
в интернете**

За маской онлайн-собеседника  
может скрываться злоумышленник



**НЕ сообщай в интернете  
свой реальный  
адрес и телефон**

Злоумышленник может встретить  
тебя с недобрыми намерениями



**НЕ отправляй личные данные  
для участия в конкурсах  
на малоизвестных сайтах**

Информацией могут завладеть и  
воспользоваться недоброжелатели

**РОДИТЕЛИ!  
научите детей  
пользоваться  
интернетом  
правильно!**

**ГЛАВНЫЕ  
ПРАВИЛА  
ЦИФРОВОЙ  
ГИГИЕНЫ**



**Всегда важно помнить: неправильное поведение  
в интернете может принести большой вред.**



**не дай себя обмануть!**



**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РЕСПУБЛИКИ БЕЛАРУСЬ**

**круглосуточный  
единый  
номер**

**102**

# Как не стать жертвой киберпреступника.

## ЗАЩИТА БАНКОВСКОЙ КАРТЫ

### Наиболее распространенные методы работы злоумышленников



выманивание реквизитов  
банковских платежных  
карт с  
использованием  
взломанных аккаунтов  
знакомых в  
социальных сетях



#### ЛЖЕПОКУПАТЕЛЬ -

под видом покупателя  
злоумышленник связывается с продавцом,  
предлагает внести залог перед покупкой товара, а для  
получения денежного перевода предоставляет ему  
ссылку на мошеннический сайт, визуально похожий на  
официальный сайт банка



**ВИШИНГ** - представляясь по телефону  
сотрудником банка, злоумышленник пытается  
узнать у держателя карты конфиденциальную  
информацию (ее реквизиты, а также номер паспорта,  
личный идентификационный номер, логины, пароли,  
СМС-коды)



### НЕ СООБЩАЙТЕ НИКОМУ

- информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код
- цифровые или буквенные коды
- паспортные данные



### ЕСЛИ ВАМ ПОСТУПИЛ СОМНИТЕЛЬНЫЙ ЗВОНОК

- немедленно завершите разговор
- обратитесь в контакт-центр банка, выпустившего карту
- следуйте рекомендациям сотрудника банка



Для защиты денежных  
средств клиентов у банка  
есть вся необходимая  
информация



Работники банка по телефону  
не должны спрашивать ни  
реквизиты карты, ни  
паспортные данные



Не давайте никому свой  
мобильный телефон и  
предупредите об этом ваших  
близких, особенно детей и  
лиц пожилого возраста

научись пользоваться интернетом правильно!

# БЕЗОПАСНЫЙ ИНТЕРНЕТ ДЛЯ ДЕТЕЙ

## ПРАВИЛА

ЦИФРОВОЙ  
ГИГИЕНЫ

**не сообщай незнакомцам  
свой логин и пароль**

**не открывай файлы из  
непроверенных источников**

**не заходи на сайты, которые  
защита компьютера считает  
подозрительными**

**СОХРАНИ  
ИНФОРМАЦИЮ**



**не дай себя обмануть!**



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный  
единый  
номер

**102**

# ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 

поступает звонок  
с неизвестного  
номера

2 

звонящий  
представляется  
вашим  
родственником

3 

он говорит,  
что сбил человека  
или из-за него  
человек  
попал в ДТП

4 

он просит денег  
как компенсацию  
вреда или  
чтобы «замять» дело

5 

затем звонит  
«милиционер»/  
«следователь»  
и подтверждает  
легенду

6 

за деньгами  
приезжает  
курьер

Мама, папа, я  
в беде!

Нужны деньги!  
Срочно!

Что делать?

1. немедленно положить трубку
2. самому перезвонить родственнику
3. не передавать курьерам никаких денег
4. сообщить в милицию

не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный  
единый  
номер

102