

# Кибербезопасность

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 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.

# КРАЖИ ЧЕРЕЗ МОБИЛЬНЫЙ БАНКИНГ



## КАК ЗАЩИТИТЬ МОБИЛЬНОЕ УСТРОЙСТВО



использовать ПИН-код, а также дополнительные способы блокирования устройства (графический ключ, пароль, отпечаток пальца и др.);



своевременно обновлять операционную систему устройства, антивирус;



устанавливать приложения из PlayMarket, AppStore или только из проверенных источников;



обращать внимание, к каким функциям гаджета запрашивает доступ приложение;



включить встроенные функции устройства для определения его местонахождения;



в случае утери (кражи) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам, а также обратиться в правоохранительные органы;



при смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру;



при продаже устройства произвести его сброс до заводских настроек.



Источник: МВД Беларуси.



## РАЗНОВИДНОСТЬ КИБЕРПРЕСТУПЛЕНИЙ - КРАЖА ДЕНЕГ АБОНЕНТОВ СОТОВОЙ СВЯЗИ ЧЕРЕЗ МОБИЛЬНЫЙ БАНКИНГ.

- Злоумышленники ищут жертв в общественных местах или обращаются к знакомым и просят телефон, чтобы сделать звонок.
- Делая вид, что набирает номер, при помощи USSD-запроса или выхода в интернет преступник активирует услугу мобильного банкинга. С ее помощью можно совершить платежные операции с лицевого счета абонента и получить у оператора сотовой связи лимитированный микрозайм.
- Сумма, поступившая хозяину гаджета, и средства с баланса телефона переводятся на абонентские номера или банковские счета злоумышленника.

## ЧЕГО ДЕЛАТЬ НЕЛЬЗЯ

- передавать незнакомым мобильный телефон или сим-карту, а в случае передачи - контролировать все действия, которые производятся с устройством;
- устанавливать приложения с низким рейтингом и отрицательными отзывами;
- перезванивать на незнакомые иностранные номера;
- хранить важную информацию на мобильном устройстве;
- делать полное снятие ограничений на устройстве.

# 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



# 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

# 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 знаком 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**

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 закрыть дело

5 

затем звонит  
имитационеру/  
исследователю  
и подтверждает  
легенду

6 

за деньгами  
призывает  
курьера

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

**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.

**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.