

- 01 НАДЕЖНЫЕ ПАРОЛИ
- 02 БЕЗОПАСНЫЙ WI-FI
- 03 БРАУЗЕРЫ И САЙТЫ
- 04 ЗАЩИТА ОНЛАЙН-БАНКИНГА
- 05 ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ
- 06 БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

6

правил  
информационной  
безопасности

|GROUP|IB|



# КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕР- ПРЕСТУПНИКА

|GROUP|IB|



**НЕОБХОДИМО:**

- + Создавать персональные (уникальные) пароли к разным сервисам и менять их каждые 3 месяца
- + Использовать сложные пароли: минимум 12 символов, одновременно цифры, строчные и прописные буквы, знаки пунктуации
- + 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

**НЕОБХОДИМО:**

- + Отключить общий доступ к вашей Wi-Fi сети и использовать надежный пароль к ней
- + Обновить прошивку роутера и сменить пароль к административной панели
- + Запретить автоматическое подключение своих устройств к открытым Wi-Fi точкам


**НЕ РЕКОМЕНДУЕТСЯ:**

- 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.

**НЕОБХОДИМО:**

- + Обновлять браузер и плагины
- + Использовать VPN

**НЕ РЕКОМЕНДУЕТСЯ:**

- Переходить по непроверенным ссылкам
- Вводить информацию на сайтах, если соединение не защищено (нет https и )
- Сохранять персональные данные в браузере

**НЕОБХОДИМО:**

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

**НЕ РЕКОМЕНДУЕТСЯ:**

- 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 для доступа к системе интернет-банкинга
- Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

**НЕОБХОДИМО:**

- + Устанавливать приложения только из официальных магазинов
- + Обращать внимание, к каким функциям устройства приложение запрашивает доступ
- + Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

**НЕ РЕКОМЕНДУЕТСЯ:**

- Размещать персональную и контактную информацию о себе в открытом доступе
- Указывать геолокацию 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 негативными отзывами

**НЕОБХОДИМО:**

- + Подключить двухфакторную аутентификацию
- + Использовать разную почту для переписок и для регистраций на сайтах
- + 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

# 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**

# ПРАВИЛА ВЫЖИВАНИЯ В ЦИФРОВОМ МИРЕ



**Киберпространство** — это особая цифровая среда, где полезное и интересное соседствует с опасностью и риском. Чтобы пользоваться интернетом безопасно, важно соблюдать базовые правила.

## Безопасность устройств

- Регулярно обновляй операционную систему и приложения на смартфоне, планшете и персональном компьютере.
- Устанавливай приложения только из официальных источников (App Store, Google Play и Windows Market).
- Для каждого аккаунта используй индивидуальный пароль, который рекомендуется менять раз в три месяца. Роутера это тоже касается.
- Обязательно делай резервные копии важной информации.
- Всегда блокируй свои устройства (ПК, смартфон, планшет), когда не работаешь с ними.

## Фишинг

- Помни, что злоумышленники постоянно придумывают новые правдоподобные сценарии, чтобы обмануть тебя — заставить открыть файл, перейти по ссылке или ввести персональные данные на мошеннической странице.
- Всегда внимательно проверяй адресата, от имени которого тебе пришло сообщение в электронной почте. Если возникли сомнения, лучше позвонить или другим способом связаться с человеком, от которого пришло письмо, чтобы убедиться, что это не мошенник.
- Не открывай подозрительные ссылки, файлы от незнакомцев в почте и в социальных сетях.
- Если тебе звонят из банка и просят выполнить какое-то подозрительное действие или раскрыть данные, сразу положи трубку и перезвони в банк по номеру телефона, указанному на сайте или на оборотной стороне банковской карты.

## Безопасность в соцсетях

- Никогда не размещай в соцсетях данные паспорта, банковской карты или других документов, содержащих твои персональные данные.
- Не добавляй в друзья неизвестных тебе людей и закрой свой профиль от незнакомцев.
- Не хвастайся дорогими покупками в интернете и не раскрывай незнакомцам подробности о своей семье и семейном бюджете.
- Не выкладывай в соцсети фотографии родителей, родственников, близких и знакомых без их согласия.

## Кибербуллинг и травля в интернете

- Если кто-то оскорбляет и провоцирует тебя в сети, сохраняй спокойствие и не ведись на провокацию.
- Сразу прекрати общение с этим человеком, заблокируй его и сообщи родителям или взрослому, которому доверяешь.

# ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ



**Не торопись** переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт



**НЕ пользуйся** открытыми вай-фай-сетями в кафе или на улице



**Не спеши** переходить по ссылке: введи адрес вручную



Фишинговая ссылка может прийти в мессенджере, по электронной почте, в смс-сообщении



**Сохрани эту информацию и поделись с другими**

# ВНИМАНИЕ!

## БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

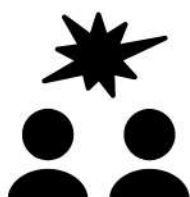


**Размещать** персональную и контактную информацию о себе в открытом доступе



**Использовать** указание геолокации на фото в постах

### НЕЛЬЗЯ



**Отвечать** на агрессию и обидные выражения



**Реагировать** на письма от неизвестного отправителя



**Открывать** подозрительное вложение к письму



**Сохрани эту информацию и поделись с другими**

# ВНИМАНИЕ!

## ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ



**Хранить** пинкод вместе с картой



**Распространять** личные данные, логин и пароль доступа к системе «Интернет-банкинг»

### НЕЛЬЗЯ



**Сообщать** CVV-код или отправлять его фото



**Сообщать** данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.



**Сохрани эту информацию и поделись с другими**

# ВНИМАНИЕ!

## ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ



**НЕ переходите** по ссылкам и письмам от незнакомцев, не нажимайте на картинки и кнопки



**НЕ верьте** обещаниям внезапных выигрышей

**УСТАНОВИТЕ АНТИВИРУС НА ВСЕ  
ВАШИ УСТРОЙСТВА**



**НЕ сообщайте** свои персональные данные и данные банковской карты



**НЕ указывайте** личную информацию в открытых источниках



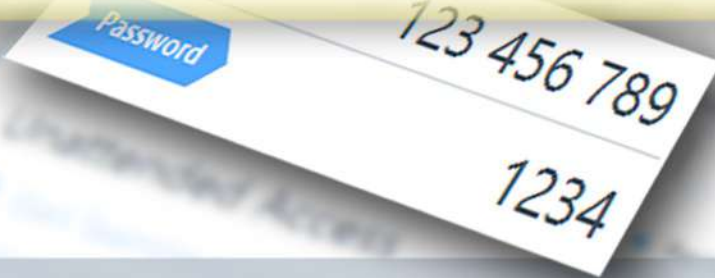
**НЕ используйте** одинаковые пароли для всех аккаунтов



**Сохрани эту информацию и поделись с другими**

# **ВНИМАНИЕ!**

## **ПОЯВИЛСЯ НОВЫЙ ВИД ВИШИНГА!**



**НЕ СОВЕРШАЙТЕ НИКАКИХ ДЕЙСТВИЙ НА СМАРТФОНЕ ПО ПРОСЬБЕ ПОСТОРОННИХ ЛЮДЕЙ! ТЕМ БОЛЕЕ, НЕ СООБЩАЙТЕ ИМ КОДЫ, ПАРОЛИ, И ДР.ИНФОРМАЦИЮ**

**НЕ СОХРАНЯЙТЕ В ПРИЛОЖЕНИЯХ И БРАУЗЕРАХ ПАРОЛИ, КОДЫ, ЛОГИНЫ. ПРЕСТУПНИК МОЖЕТ УЗНАТЬ КОД ИЗ ПРИСЛАННОГО SMS-СООБЩЕНИЯ**



128 293 154

**ПРЕСТУПНИК ПО ТЕЛЕФОНУ ПРОСИТ ВАС УСТАНОВИТЬ ПРОГРАММУ НА ТЕЛЕФОН ДЛЯ ДИСТАНЦИОННОГО ДОСТУПА И СООБЩИТЬ ЕМУ ПАРОЛЬ И КОД**



**УПРАВЛЕНИЕ «К» МВД БЕЛАРУСИ**



# 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

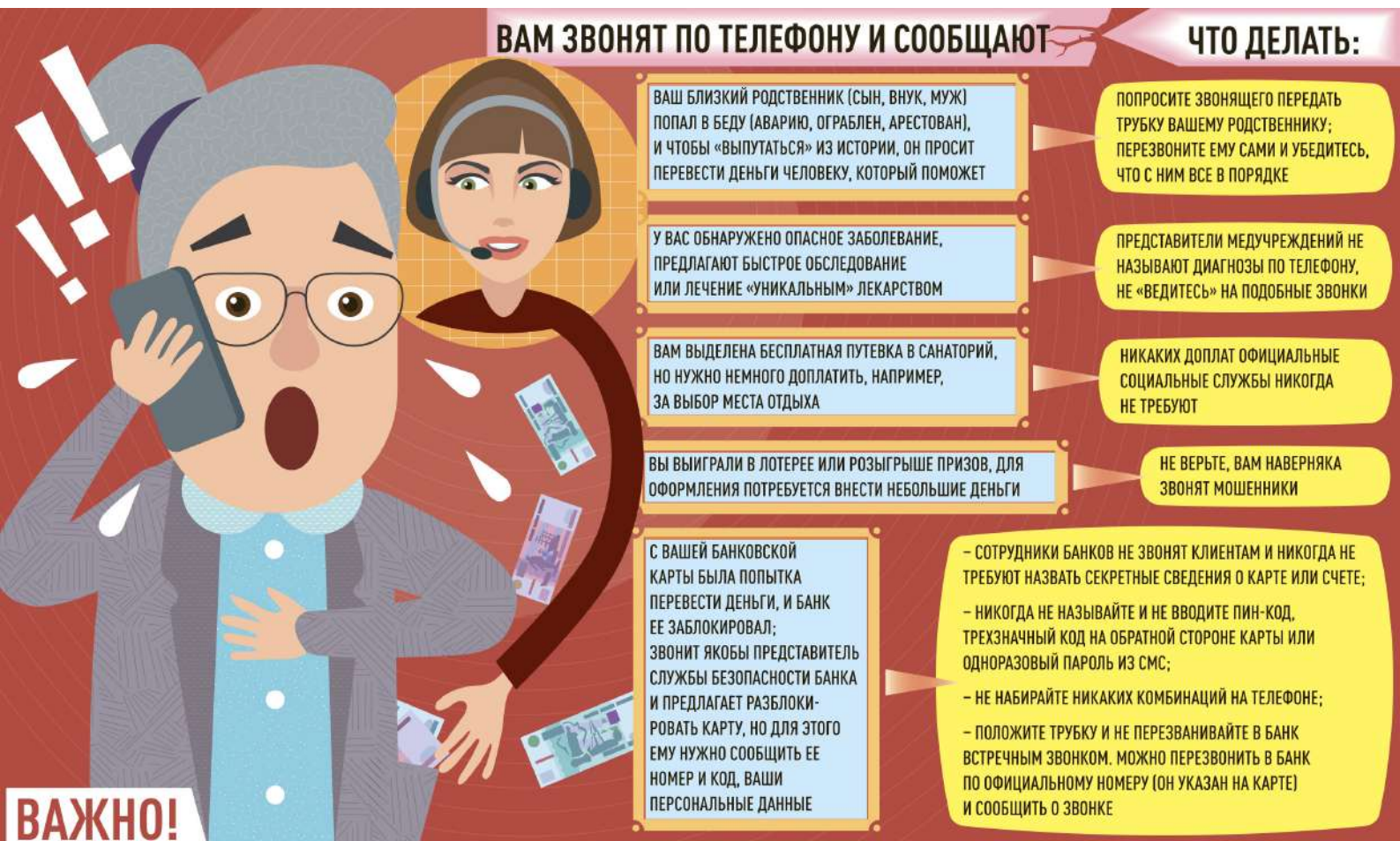
- × Размещать персональную и контактную информацию о себе в открытом доступе
- × Использовать указание геолокации на фото в постах
- × Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса
- × Употреблять ненормативную лексику при общении
- × Устанавливать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



## ВАМ ЗВОНЯТ ПО ТЕЛЕФОНУ И СООБЩАЮТ

## ЧТО ДЕЛАТЬ:

ВАШ БЛИЗКИЙ РОДСТВЕННИК (СЫН, ВНУК, МУЖ) ПОПАЛ В БЕДУ (АВАРИЮ, ОГРАБЛЕН, АРЕСТОВАН), И ЧТОБЫ «ВЫПУТАТЬСЯ» ИЗ ИСТОРИИ, ОН ПРОСИТ ПЕРЕВЕСТИ ДЕНЬГИ ЧЕЛОВЕКУ, КОТОРЫЙ ПОМОЖЕТ

ПОПРОСИТЕ ЗВОНЯЩЕГО ПЕРЕДАТЬ ТРУБКУ ВАШЕМУ РОДСТВЕННИКУ; ПЕРЕЗВОНИТЕ ЕМУ САМИ И УБЕДИТЕСЬ, ЧТО С НИМ ВСЕ В ПОРЯДКЕ

У ВАС ОБНАРУЖЕНО ОПАСНОЕ ЗАБОЛЕВАНИЕ, ПРЕДЛАГАЮТ БЫСТРОЕ ОБСЛЕДОВАНИЕ ИЛИ ЛЕЧЕНИЕ «УНИКАЛЬНЫМ» ЛЕКАРСТВОМ

ПРЕДСТАВИТЕЛИ МЕДУЧРЕЖДЕНИЙ НЕ НАЗЫВАЮТ ДИАГНОЗЫ ПО ТЕЛЕФОНУ, НЕ «ВЕДИТЕСЬ» НА ПОДОБНЫЕ ЗВОНКИ

ВАМ ВЫДЕЛЕНА БЕСПЛАТНАЯ ПУТЕВКА В САНАТОРИЙ, НО НУЖНО НЕМНОГО ДОПЛАТИТЬ, НАПРИМЕР, ЗА ВЫБОР МЕСТА ОТДЫХА

НИКАКИХ ДОПЛАТ ОФИЦИАЛЬНЫЕ СОЦИАЛЬНЫЕ СЛУЖБЫ НИКОГДА НЕ ТРЕБУЮТ

ВЫ ВЫИГРАЛИ В ЛОТЕРЕЕ ИЛИ РОЗЫГРЫШЕ ПРИЗОВ, ДЛЯ ОФОРМЛЕНИЯ ПОТРЕБУЕТСЯ ВНЕСТИ НЕБОЛЬШИЕ ДЕНЬГИ

НЕ ВЕРЬТЕ, ВАМ НАВЕРНЯКА ЗВОНЯТ МОШЕННИКИ

С ВАШЕЙ БАНКОВСКОЙ КАРТЫ БЫЛА ПОПЫТКА ПЕРЕВЕСТИ ДЕНЬГИ, И БАНК ЕЕ ЗАБЛОКИРОВАЛ; ЗВОНИТ ЯКОБЫ ПРЕДСТАВИТЕЛЬ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА И ПРЕДЛАГАЕТ РАЗБЛОКИРОВАТЬ КАРТУ, НО ДЛЯ ЭТОГО ЕМУ НУЖНО СООБЩИТЬ ЕЕ НОМЕР И КОД, ВАШИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

– СОТРУДНИКИ БАНКОВ НЕ ЗВОНЯТ КЛИЕНТАМ И НИКОГДА НЕ ТРЕБУЮТ НАЗВАТЬ СЕКРЕТНЫЕ СВЕДЕНИЯ О КАРТЕ ИЛИ СЧЕТЕ;  
– НИКОГДА НЕ НАЗЫВАЙТЕ И НЕ ВВОДИТЕ ПИН-КОД, ТРЕХЗНАЧНЫЙ КОД НА ОБРАТНОЙ СТОРОНЕ КАРТЫ ИЛИ ОДНОРАЗОВЫЙ ПАРОЛЬ ИЗ СМС;  
– НЕ НАБИРАЙТЕ НИКАКИХ КОМБИНАЦИЙ НА ТЕЛЕФОНЕ;  
– ПОЛОЖИТЕ ТРУБКУ И НЕ ПЕРЕЗВАНИВАЙТЕ В БАНК ВСТРЕЧНЫМ ЗВОНКОМ. МОЖНО ПЕРЕЗВОНИТЬ В БАНК ПО ОФИЦИАЛЬНОМУ НОМЕРУ (ОН УКАЗАН НА КАРТЕ) И СООБЩИТЬ О ЗВОНКЕ

**ВАЖНО!**

МОШЕННИКИ ВОРУЮТ БАЗЫ ДАННЫХ И НАЗЫВАЮТ ВАС ПО ИМЕНИ-ОТЧЕСТВУ, А В ТЕЛЕФОНЕ ВИДЕН НОМЕР ВАШЕГО БАНКА

**БУДЬТЕ ГОТОВЫ И ПРОЯВИТЕ БДИТЕЛЬНОСТЬ**

научись пользоваться интернетом правильно!

СОХРАНИ  
ИНФОРМАЦИЮ

БЕЗОПАСНЫЙ  
INTERNET  
ДЕТЯМ

1

**не сообщай незнакомцам  
свой логин и пароль**

2

**не открывай файлы из  
непроверенных источников**

3

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



**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**

научись пользоваться интернетом правильно!

# Безопасный интернет для детей



## ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ



**НЕ отправляй незнакомцам свои фото и видео**

Злоумышленники могут узнать что-то важное 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

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

# 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**



# **ВНИМАНИЕ!** **АТАКА НА ГОСОРГАНИЗАЦИИ!**

**СПЕЦИАЛИСТЫ ОТМЕЧАЮТ УВЕЛИЧЕНИЕ  
ЧИСЛА ФИШИНГОВЫХ АТАК НА ЭЛЕКТРОННЫЕ  
ПОЧТОВЫЕ ЯЩИКИ ГОСОРГАНИЗАЦИЙ!**

**ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ**

## **НЕ НАДО:**

... ОТКРЫВАТЬ ВЛОЖЕНИЯ  
ПОЧТОВЫХ СООБЩЕНИЙ  
ОТ НЕИЗВЕСТНЫХ  
ОТПРАВИТЕЛЕЙ

... ПЕРЕХОДИТЬ ПО  
ССЫЛКАМ, ПОЛУЧЕННЫМ  
ОТ НЕИЗВЕСТНЫХ

... ХРАНИТЬ И  
ПЕРЕДАВАТЬ В ОТКРЫТОМ  
ВИДЕ ВАЖНЫЕ ДАННЫЕ  
(ЗААРХИВИРУЙТЕ ИХ И  
УСТАНОВИТЕ ПАРОЛЬ)

... ПРИ РЕГИСТРАЦИИ  
ЯЩИКА УКАЗЫВАТЬ  
БИОГРАФИЧЕСКИЕ  
ДАННЫЕ. ИСПОЛЬЗОВАТЬ  
ПРОСТЫЕ ПАРОЛИ И  
ПОВТОРЯЮЩИЕСЯ  
СИМВОЛЫ

## **НАДО:**

... ПОДКЛЮЧИТЬ  
2-ФАКТОРНУЮ  
АУТЕНТИФИКАЦИЮ

... РЕГУЛЯРНО МЕНЯТЬ  
ПАРОЛЬ ОТ ЭЛ.ПОЧТЫ

... ИСПОЛЬЗОВАТЬ  
НЕСКОЛЬКО ПОЧТОВЫХ  
ЯЩИКОВ ДЛЯ РАЗНЫХ  
РЕСУРСОВ (ПЕРЕПИСКА,  
РЕГИСТРАЦИЯ, ДЕЛОВАЯ  
ПОЧТА)

... ИСПОЛЬЗОВАТЬ  
УНИКАЛЬНЫЕ ПАРОЛИ  
ДЛЯ РАЗНЫХ  
ИНТЕРНЕТ-РЕСУРСОВ

... ВВОДИТЬ  
ИНФОРМАЦИЮ ТОЛЬКО НА  
ЗАЩИЩЕННЫХ САЙТАХ  
(HTTPS)

**ВНИМАНИЕ!**  
**ЕДИНСТВЕННЫЙ НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ**  
**- ЭТО ВАША БДИТЕЛЬНОСТЬ!**

# Как не стать жертвой киберпреступника.

## ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

### Основные правила информационной безопасности по защите банковской карточки:

-  хранить в тайне пин-код карты
-  прикрывать ладонью клавиатуру при вводе пин-кода
-  оформлять отдельную карту для онлайн-покупок
-  деньги зачислять только в размере предполагаемой покупки
-  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
-  подключить услугу "SMS-оповещение"



### Не рекомендуется

-  хранить пин-код вместе с карточкой/на карточке
-  сообщать CVV-код или отправлять его фото
-  распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
-  сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли\*\*\*, код авторизации, пароли 3-D Secure

\* Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).

\*\* Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.

\*\*\* Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.



Источник: МВД Беларуси.

© Инфографика 

# 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**

**МОШЕННИЧЕСКАЯ СХЕМА “ЧЕЛОВЕК ПОСЕРЕДИНЕ”:  
ЗАЩИТИТЕ СВОЮ ЭЛЕКТРОННУЮ ПОЧТУ!**

**НИКОМУ НЕ  
СООБЩАЙТЕ ПАРОЛИ,  
НЕ ИСПОЛЬЗУЙТЕ  
АВТОСОХРАНЕНИЕ В  
БРАУЗЕРЕ**

**ПРОВЕРЯЙТЕ  
ПРАВИЛЬНОСТЬ  
АДРЕСА  
КОНТРАГЕНТА**



**НЕ ИСПОЛЬЗУЙТЕ В  
ЛИЧНЫХ ЦЕЛЯХ  
СЛУЖЕБНЫЕ  
ЭЛ.ЯЩИКИ**

**ПРЕЖДЕ, ЧЕМ  
ОТПРАВИТЬ ПЕРЕВОД,  
СОЗВОНИТЕСЬ С  
ПОЛУЧАТЕЛЕМ**



# КАК ЗАЩИТИТЬ ПРЕДПРИЯТИЕ ОТ КИБЕРУГРОЗ

**В 2018-2020 ГГ ПРЕДПРИЯТИЯМ ПРИЧИНЕН УЩЕРБ НА СУММУ БОЛЕЕ 2 МЛН. РУБЛЕЙ**

## ОСНОВНЫЕ СХЕМЫ КИБЕРПРЕСТУПНИКОВ



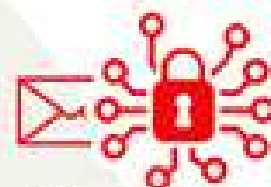
### Шифрование коммерческой информации

Хакеры получают доступ к данным организации, превращают их в бессмысленный набор символов и оставляют письмо с предложением расшифровать данные за деньги.



### Подмена реквизитов для перевода средств

Эта криминальная схема используется в длительных и успешных деловых отношениях белорусской фирмы и зарубежного контрагента, которые активно контактируют по электронной почте. Злоумышленники получают доступ к одному из ящиков, участвующих в переписке. Когда у компаний намечается крупная сделка, со взломанного email предприятия (или же другой электронной почты с максимально похожим адресом) хакеры высылают письмо, в котором от имени юрлица уведомляют партнеров об изменении реквизитов для перевода средств.



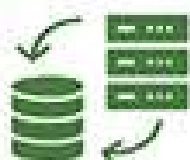
### Фишинговое письмо

На электронную почту учреждения приходит письмо с вложением-аредоном, способным превращать ценную для компании информацию в бесполезный набор символов.

## КАК ЗАЩИТИТЬСЯ ОТ КИБЕРУГРОЗ



воспользоваться услугами профессионалов по защите данных



регулярно выполнять резервное копирование данных



пользоваться актуальными антивирусами



настроить специальное программное обеспечение, блокирующее таргетированные атаки на информационные системы

# 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.

**Главное управление по противодействию киберпреступности  
криминальной милиции МВД Республики Беларусь**

# ГЛАВНЫЕ ПРАВИЛА **ЦИФРОВОЙ ГИГИЕНЫ** ДЛЯ ДЕТЕЙ

**Не сообщай личную информацию незнакомцу. И, вообще, в интернете не размещай сведения о себе и семье**

**Советуйся с родителями, как правильно поступить, если столкнулся с чем-то непонятным или пугающим**

**Помни, что в интернете надо быть очень-очень внимательным. Старайся избегать общения с незнакомыми людьми в онлайн-играх и соцсетях, не выполняй бездумно то, что они попросят тебя сделать**



ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ МВД

# НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ ФИНАНСОВОЙ ГРАМОТНОСТИ

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ

**НЕ** УСТАНАВЛИВАЙТЕ  
ПРОГРАММЫ

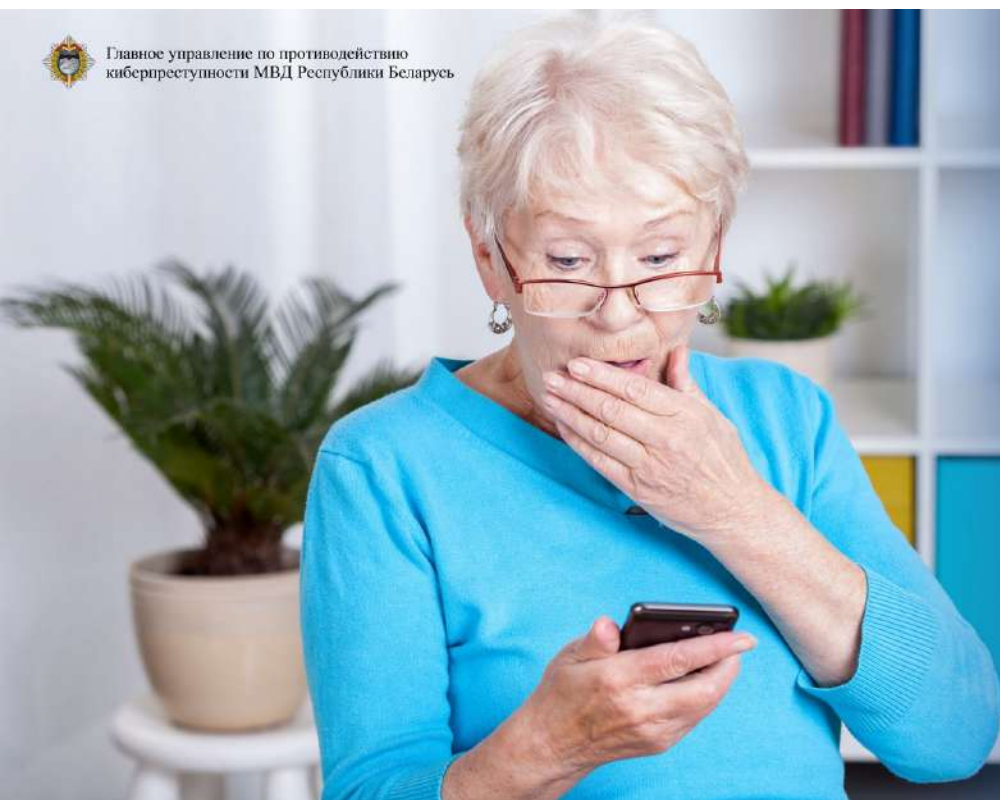
**НЕ** ПЕРЕВОДИТЕ  
ДЕНЬГИ



Главное управление по противодействию  
киберпреступности МВД Республики Беларусь



Главное управление по противодействию  
киберпреступности МВД Республики Беларусь



**НАУЧИТЕ  
РОДИТЕЛЕЙ  
ФИНАНСОВОЙ  
ГРАМОТНОСТИ**

**ПО ПРОСЬБЕ  
ТРЕТЬИХ ЛИЦ**

**НЕ ПЕРЕВОДИТЕ  
ДЕНЬГИ**

**НЕ УСТАНАВЛИВАЙТЕ  
ПРОГРАММЫ**

# ВНИМАНИЕ! ОПЕРАЦИЯ «ВИШИНГ»!

АФЕРИСТ МОЖЕТ  
ПОВЗОНИТЬ ПО ПОВОДУ  
ТОВАРА НА ТОРГОВОЙ  
ПЛОЩАДКЕ И  
ПРЕДЛОЖИТЬ СДЕЛКУ С  
ПРЕДОПЛАТОЙ



АФЕРИСТ МОЖЕТ  
ПРЕДСТАВИТЬСЯ  
БАНКОВСКИМ РАБОТНИКОМ И  
ВЫМАНИТЬ  
КОНФИДЕНЦИАЛЬНЫЕ  
ДААННЫЕ



АФЕРИСТ СООБЩАЕТ,  
ЧТО РОДСТВЕННИК  
ЖЕРТВЫ ПОПАЛ В БЕДУ  
И ЕМУ НУЖНА  
ФИНАНСОВАЯ ПОМОЩЬ



**ВИШИНГ** - СПОСОБ МОШЕННИЧЕСТВА С ПОМОЩЬЮ ТЕЛЕФОНА, КОГДА МОШЕННИК ПОД РАЗЛИЧНЫМ ПРЕДЛОГОМ ПЫТАЕТСЯ ВЫМАНИТЬ ПЕРСОНАЛЬНУЮ ИНФОРМАЦИЮ ЖЕРТВЫ ДЛЯ ПОСЛЕДУЮЩЕГО ХИЩЕНИЯ ДЕНЕГ С ЕЕ БАНКОВСКОГО СЧЕТА

- НИКОГДА НЕ СООБЩАЙТЕ  
НЕЗНАКОМОМУ СВОИ  
ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- НЕ ТОРОПИТЕСЬ ВЫПОЛНЯТЬ  
ТО, ЧТО ОТ ВАС ПРОСИТ  
СОБЕСЕДНИК. МОШЕННИКИ  
ОЧЕНЬ ИЗОБРЕТАТЕЛЬНЫ И  
УБЕДИТЕЛЬНЫ!



- НАДЕЖНО ЗАЩИЩАЙТЕ СВОИ  
ДААННЫЕ (ДВУХФАКТОРНАЯ  
АВТОРИЗАЦИЯ,  
СМС-ОПОВЕЩЕНИЕ, И Т.Д.)

- В СЛУЧАЕ УТЕРИ ИЛИ КРАЖИ  
КАРТЫ ЗАБЛОКИРУЙТЕ ЕЕ ПО  
ТЕЛЕФОНУ ИЛИ В БАНКЕ

ГУПК КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ



# БЫТЬ ХАКЕРОМ: не развлечение, а преступление!



Уголовная ответственность за киберпреступления наступает:



## Статья 212 УК Беларуси

с 14  
лет

Хищение путем использования компьютерной техники или введения в компьютерную систему ложной информации наказывается вплоть до лишения свободы на срок **до 3 лет**.



Те же действия, совершенные **повторно или группой лиц по предварительному сговору**, наказываются лишением свободы на срок **до 5 лет**.



Если хищение **крупное**, то предусмотрено наказание в виде лишения свободы на срок **до 7 лет**.



За хищение, совершенное **организованной группой или в особо крупном размере**, грозит **до 12 лет** лишения свободы.



## Статья 349 УК Беларуси

с 16  
лет

Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, наказывается вплоть до лишения свободы на срок **до 2 лет**.



За несанкционированный доступ к компьютерной информации, повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные **тяжкие последствия**, грозит наказание вплоть до лишения свободы на срок **до 7 лет**.

# ВНИМАНИЕ! ОТКРЫТЫЙ WI-FI

## УГРОЗА для владельцев WI-FI:



## УГРОЗА для пользователей:

- ЗЛОУМЫШЛЕННИК МОЖЕТ ВНЕДРИТЬ  
ВРЕДОНОСНЫЕ ПРОГРАММЫ НА ВАШЕ  
УСТРОЙСТВО ЧЕРЕЗ ОТКРЫТОЕ  
WI-FI-СОЕДИНЕНИЕ

- ВАШ ТРАФИК МОЖЕТ БЫТЬ ПЕРЕХВАЧЕН  
ЗЛОУМЫШЛЕННИКОМ, ВКЛЮЧАЯ  
ПЕРСОНАЛЬНЫЕ ДАННЫЕ, РЕКВИЗИТЫ КАРТ, И  
Т.Д.

- ВАШ КОМПЬЮТЕР МОЖЕТ БЫТЬ ПОДКЛЮЧЕН К  
БОТ-СЕТИ, ОСУЩЕСТВЛЯЮЩЕЙ DDOS-АТАКИ,  
ЧТО МОЖЕТ ПОВЛЕЧЬ УГОЛОВНУЮ  
ОТВЕТСТВЕННОСТЬ

- ВВОДИМЫЕ ВАМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ  
МОГУТ БЫТЬ ПЕРЕХВАЧЕНЫ ХАКЕРОМ  
(ПЛАТЕЖНАЯ ИНФОРМАЦИЯ, РЕВИЗИТЫ,  
КОНТАКТЫ НА ТЕЛЕФОНЕ, ПАРОЛИ)

- ЗЛОУМЫШЛЕННИК МОЖЕТ ПОЛУЧИТЬ  
ДОСТУП К ВАШИМ ПЕРСОНАЛЬНЫМ ДАННЫМ,  
ФОТО-ВИДЕО, ХРАНЯЩИМСЯ НА УСТРОЙСТВЕ,  
И Т.Д.

- ЗЛОУМЫШЛЕННИК МОЖЕТ ВЗЛОМАТЬ ВАШИ  
ПРОГРАММЫ И СОЦИАЛЬНЫЕ СЕТИ,  
СОВЕРШАЯ ЗАТЕМ РАЗЛИЧНЫЕ ДЕЙСТВИЯ ОТ  
ВАШЕГО ИМЕНИ



**ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ  
КРИМИНАЛЬНОЙ МИЛИЦИИ МВД РЕСПУБЛИКИ БЕЛАРУСЬ**



# **ВНИМАНИЕ, ОПАСНОСТЬ! ВРЕДОНОСНЫЕ РАСШИРЕНИЯ ДЛЯ БРАУЗЕРОВ!**

## **ЧТО УМЕЮТ ДЕЛАТЬ ВИРУСНЫЕ РАСШИРЕНИЯ?**

- Размещать навязчивую рекламу в вашем браузере
- Совершать действия от имени пользователя в соцсетях (лайкать нужные материалы, делать рекламные посты)
- Перенаправлять на фишинговые или зараженные сайты
- Незаметно для пользователя кликать на вредоносные или рекламные ссылки, активировать скрипты
- Подсовывать пользователю для скачивания вирусное ПО, или веб-приложения
- Самовосстанавливаться после удаления
- Подменять контент, видоизменять кнопки, интерфейс страницы, оформление
- Следить за серфингом пользователя в интернете: куда он ходит, какие сайты посещает, чем интересуется



## **КАК ОНИ ПОПАДАЮТ В ВАШ КОМПЬЮТЕР?**

- В комплекте с другими программами (“в нагрузку” с какими-то нужным файлом или программой)
- Выдает себя за полезное ПО (наряду с полезными функциями программа может иметь и несколько “неполезных”)
- Обманом и шантажом (мошенники не дают пользователю уйти с их сайта, пока тот не установит программу или приложение)

## **В КАКИХ БРАУЗЕРАХ ОНИ УСТАНАВЛИВАЮТСЯ?**

Дополнительные расширения поддерживают такие браузеры:

GOOGLE CHROME

OPERA

MOZILLA FIREFOX

EDGE

SAFARI

ЯНДЕКС.БРАУЗЕР

INTERNET EXPLORER

AMIGO, и др.



## КАК ЗАЩИТИТЬСЯ ОТ "ВРЕДНОСА"?



- Внимательно следить за ПО, которое устанавливаете
- Устанавливайте расширения ТОЛЬКО из официальных источников!
- Проверяйте права доступа, которые запрашивает приложение
- Используйте браузер со встроенной защитой
- Быть бдительным при открытии файлов \*.exe, .vbs, .scr
- Удалите все подозрительные файлы и расширения, затем просканируйте компьютер
- Если расширение появляется и после удаления - удалите приложение и создайте новый ярлык браузера
- Обновите антивирус и просканируйте компьютер. Если антивирус не помог - восстановите систему до более ранней версии
- В крайнем случае, напишите разработчику браузера

**ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ  
КИБЕРПРЕСТУПНОСТИ НМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ**



# «ОСНОВНЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ»

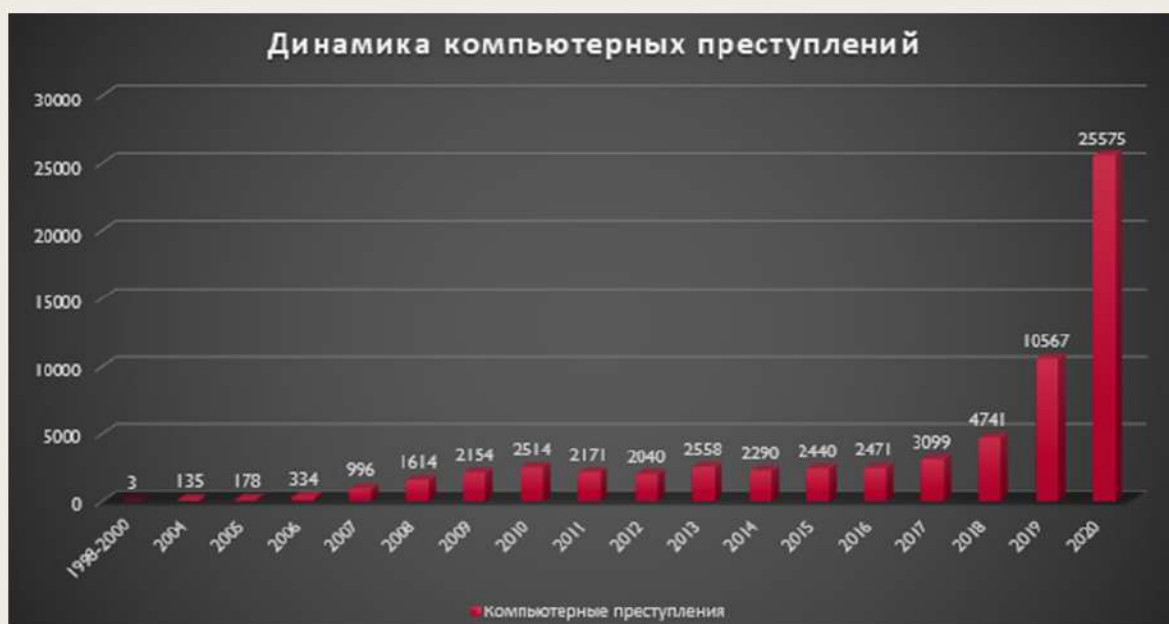
Старший оперуполномоченный по особо важным делам  
главного управления по противодействию киберпреступности  
криминальной милиции МВД Республики Беларусь  
подполковник милиции **Ластовский Александр Андреевич**

## Наш «цифровой двойник» - КТО ЭТО?



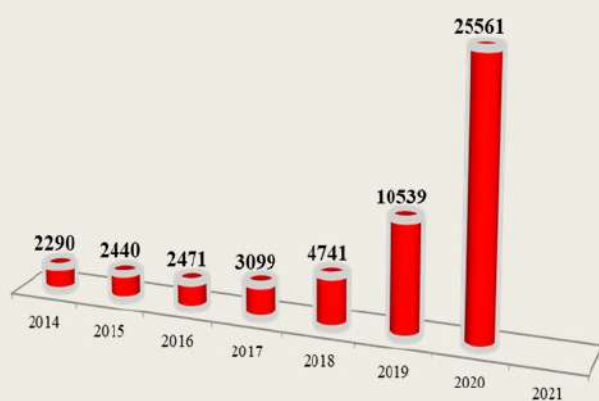
- В цифровой среде у всех нас есть двойник: аккаунты в соцсетях, платежные профили, информация о нас по роду деятельности.
- Эта информация требует самой серьезной защиты от посягательств.
- Главная защита от злоумышленника – неукоснительное соблюдение правил «цифровой гигиены» (смена паролей, двухфакторная аутентификация, обновление ПО).

## Динамика киберпреступлений (1998-2020 годы)

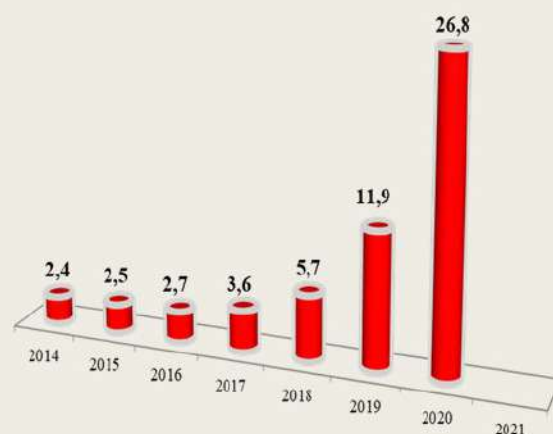


## Статистические данные о киберпреступности за 2014-2020 годы

Сведения  
о количестве зарегистрированных  
киберпреступлений  
в 2014 – 2020 гг.



Сведения  
об удельном весе киберпреступлений от общего  
количества регистрируемых  
преступлений в 2014 – 2020 гг.



## Аудитория интернета (по состоянию на 2018-2020 годы)



**3,8 млрд**  
активные пользователи Интернета  
(51% населения)



**3,5 млрд**  
пользователи мобильного Интернета  
(92% всех пользователей)

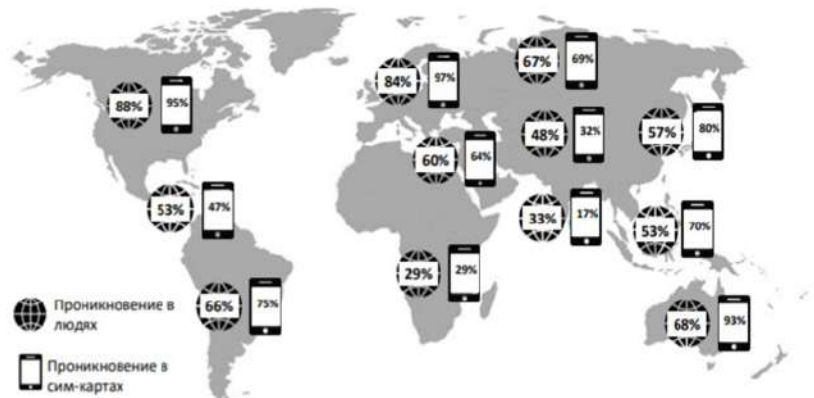


**3 млрд**  
активные пользователи соцсетей  
(40% населения)



**2,8 млрд**  
активные мобильные пользователи соцсетей (37% населения)

**92% ПОЛЬЗОВАТЕЛЕЙ В МИРЕ ИСПОЛЬЗУЮТ МОБИЛЬНЫЙ ТЕЛЕФОН ДЛЯ ВЫХОДА В ИНТЕРНЕТ**



**59%**  
доля трафика через мобильные устройства (+21% YoY)



**4,9 млрд**  
число уникальных мобильных пользователей



**1,64**  
среднее число мобильных абонентов на уникального пользователя

## Тип устройств для выхода в интернет



## Востребованность информационных источников



## Основные угрозы, которым подвергается молодежь в интернете:

### 1. Информационная:

- новостная повестка (новостные сайты, экстремистские группы, блогосфера, политическая сфера)
- реклама наркотиков, табака, алкоголя
- порнографические материалы
- агрессивный контент («вписки», «группы смерти», группы маргинальной направленности)
- троллинг и кибербуллинг

### 2. Мошенничество:

- индустрия развлекательного контента (платные подписки на игры и сервисы, обман при продаже игровой валюты или предметов, онлайн-казино, онлайн-игры)
- мошенничество в соцсетях (благотворительные сборы-распродажа, якобы бесплатный товар, схема «мама вышли денег»)

### 3. Киберпреступления:

- хищение имущества путем модификации компьютерной информации (фишинг, вишинг)
- использование подставных лиц (дропов)
- несанкционированный доступ к компьютерной информации, ее модификация
- вымогательства
- сваттинг

# 1. Информационная угроза

каналы деструктивной и экстремистской направленности



события и их оценка в информационной сфере (события в РБ и Украине)

интернет-реклама (наркотики, спиртное, алкоголь и т.д.)



агрессивный контент (группы «вписки», группы смерти «синий кит», «АУЕ»)

## 2. Мошенничество

МОШЕННИКИ В СОЦИАЛЬНЫХ СЕТЯХ



обман в онлайн-играх

интернет-казино



### 3. Киберпреступления



вишинг, фишинг, иные хищения

подставные лица («дропы»)



вымогательства

сваттинг

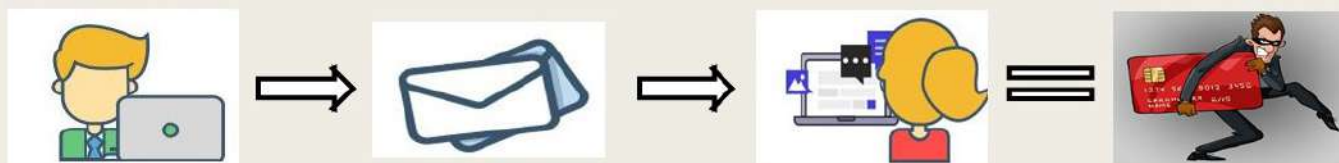
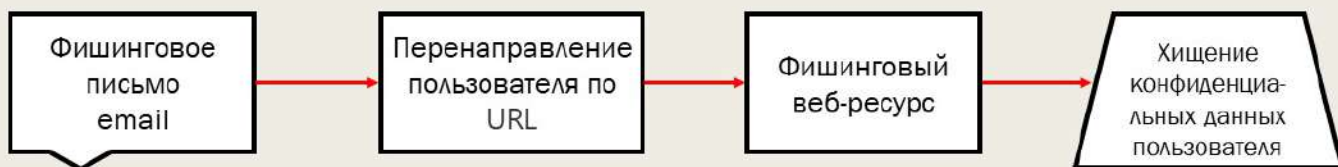


## Схема преступной деятельности, связанной с «ВИШИНГОМ»

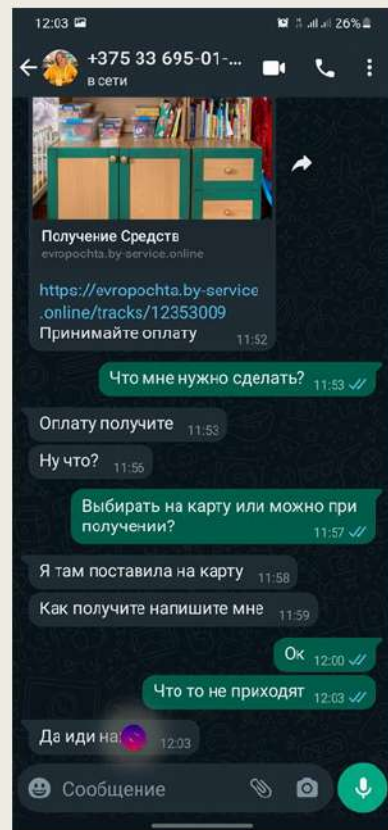
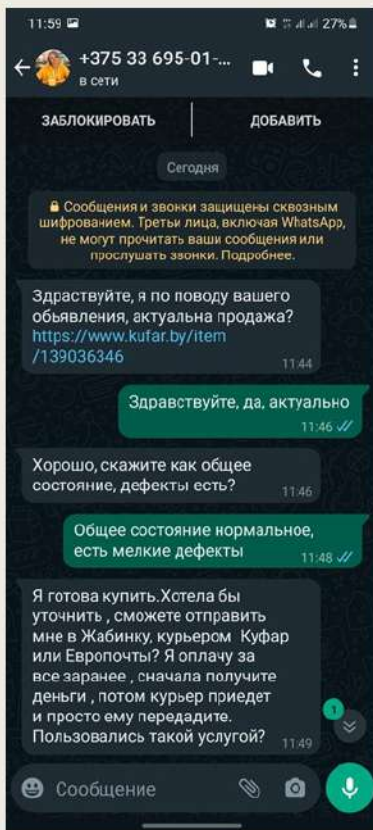


Вишинг (англ. vishing – voice + phishing) – это устная разновидность фишинга. Злоумышленники представляются сотрудниками банков и под различными предлогами просят предоставить паспортные данные, а также реквизиты банковских платежных карточек и коды, поступающие на телефонный номер клиента банка.

## Схема преступной деятельности, связанной с «фишингом»



Фишинговый сайт-обманка очень похож на оригинальный: те же шрифты, иконки, цветовая гамма. Но отличить можно по адресу ссылки ресурса: она может отличаться одним-двумя символами.



Внимание!

# БАНКОВСКИЕ ТРОЯНЫ АТАКУЮТ ПРЕДПРИЯТИЯ

## КАК ЗАЩИТИТЬСЯ



Не открывать вложения от неизвестных источников



Не оставлять в компьютере подключенным USB-ключ



Не использовать служебные e-mail в личных целях



Своевременно обновлять ПО, антивирус, браузеры и т.д.

Управление информации и общественных связей МВД Республики Беларусь

# ФИШИНГ: КАК ЗАЩИТИТЬ СВОЙ БАНКОВСКИЙ СЧЕТ

НИКОГДА НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ,  
ПРИСЛАННЫМ ВАМ В МЕССЕНДЖЕРАХ, ПО ЭЛ.ПОЧТЕ, В SMS-СООБЩЕНИИ

## Признаки явного мошенничества



Потенциальный покупатель вашего товара предлагает **перейти в мессенджер**, отказываясь общаться непосредственно на торговой площадке.

Наиболее крупные площадки для защиты своих пользователей ограничивают функцию отправки ссылок



Неизвестный в мессенджере присылает **ссылку для перехода на интернет-сайт**

под предлогом контроля карт-счета, просмотра баланса или проверки состояния оплаты.



Незнакомец предлагает передать ему полные данные вашей банковской карты, включая CVV-код либо логин и пароль от вашего интернет-банкинга.



## ПОДРОБНОСТИ - ПО QR-ССЫЛКЕ

© Совместная инфографика:



ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

# ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ



**НЕ следуй** инструкциям  
незнакомцев, позвонившим  
с неизвестного номера



**НЕ сообщай** неизвестным  
лицам свои персональные  
данные



**НЕ совершай** никаких  
действий на смартфоне по  
просьбе посторонних лиц



**НЕ переводи** деньги  
незнакомым людям в  
качестве предоплаты



**Сохрани эту информацию и поделись с другими**