

научись пользоваться интернетом правильно!

Безопасный интернет для детей

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ



НЕ отправляй незнакомцам свои фото и видео

Злоумышленники могут узнать что-то нужное 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

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 **(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**

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

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

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

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!

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!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

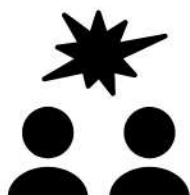


Размещать персональную и контактную информацию о себе в открытом доступе



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

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

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

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

БЕЗОПАСНЫЙ WI-FI**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

ЗАЩИТА ОНЛАЙН-БАНКИНГА**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

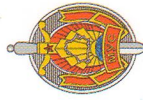
БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ**НЕОБХОДИМО:**

- + 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

- 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



|GROUP|IB|



|GROUP|IB|

6

правил
информационной
безопасности

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕР- ПРЕСТУПНИКА