

Не попадитесь на уловки мошенников! Помните:

- представители правоохранительных органов, государственных организаций **НИКОГДА НЕ ЗВОНЯТ** на **МЕССЕНДЖЕРЫ!** (исключения, если Вы сами дали свой номер для связи сотруднику и знаете его лично).

- ни под каким предлогом не сообщайте по телефону персональные (паспортные) данные, номера банковских карт или одноразовые пароли, пришедшие Вам на мобильный телефон;

- приложение мобильного оператора можно скачивать только из магазинов «Google Play», «App Store», «App Gallery», а не с направленных Вам ссылок на сайты незнакомыми лицами;

- никогда не оформляйте кредиты по просьбе или требованию третьих лиц;

- не проводите через банкоматы, а также системы банковского обслуживания сети интернет, никакие денежные операции по инструкциям, полученным по телефону или мессенджеру.

Если поступил сомнительный звонок, незамедлительно завершите разговор и обратитесь в милицию по номеру «102».

Наиболее актуальные преступные схемы:

➤ Поступает звонок в **мессенджере** (Telegram, Viber), звонивший представляется:

1. Милиционером, следователем (сотрудником других правоохранительных органов), Вас пытаются убедить:

- **родственник**, иной близкий человек, **спровоцировал ДТП**, для избежания уголовной ответственности **необходимо срочно передать** через курьера **денежные средства** пострадавшему;

- **поучаствовать в операции по разоблачению преступников**, оформивших кредит на Ваше имя, для чего **перечислить Ваши деньги на «безопасный» счет**, либо **оформить кредит (для дистанционной помощи сообщить Ваши персональные данные, код пришедший на телефон)**;

2. Сотрудником банка, представителем операторов сотовой связи, домашней телефонии, провайдера сети интернет (РУП «Белтелеком» и д.р.), Вас пытаются убедить:

- **передать (перечислить) Ваши деньги представителю банка** для их декларирования;

- **перезаключить (обновить) договоры услуг (мобильной/стационарной связи, доступа к сети интернет и д.р.)**, **перейдя по направленной мошенником ссылке для установки приложения (помните, договоры на оказания таких услуг как правило бессрочны)**;

➤ **Реклама в сети интернет, предлагающая вложить (использовать) Ваши накопления с доходом на «крайне выгодных» условиях (инновационные средства заработка, заработок на бирже, приобретение криптовалюты, вложения средств с повышенной доходностью по счетам и вкладам).**

➤ **Приобретение в сети интернет товаров по цене ниже рыночной, в т.ч. перечисление предоплаты в адрес продавца для его брони.**

➤ **Сообщения (реклама, звонок) о выигрыше в лотерее (ином розыгрыша) с условием, что для его получения необходимо предварительно перечислить деньги.**

Будьте бдительны! Эти знания помогут спасти Ваши деньги!



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 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!**

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**



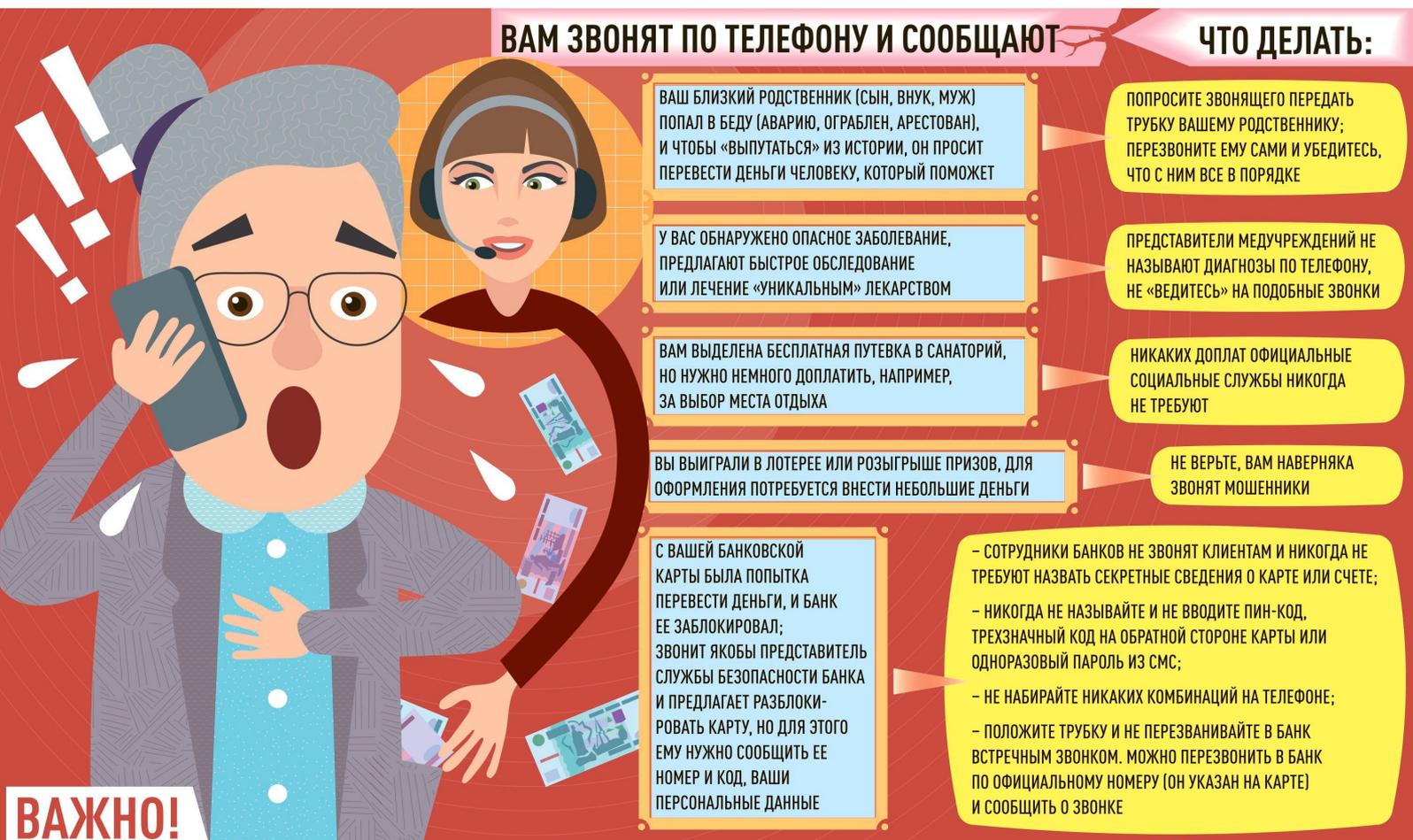
не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер

102



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

БУДЬ КИБЕРГЕРОЕМ!



Будь как ниндзя!
Не сообщай незнакомым людям в
Интернете свое настоящее имя,
адрес и номер телефона.
Будь осторожен с тем, что
пишешь о себе.

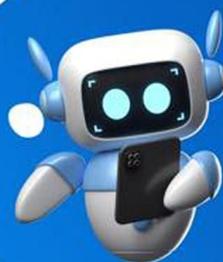


**Придумай сложный
пароль, как у супергероя!**
Никому его не говори, ведь
это твой секретный
ключ!

**Помни, что в Интернете не все
те, кем кажутся!**
Не добавляй в друзья людей,
которых не знаешь в реальной
жизни.



Будь как хакер!
Не кликай на
подозрительные
ссылки.



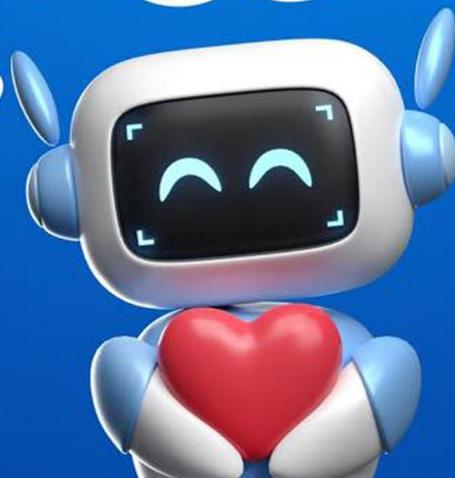
**Будь осторожен, как на
минном поле!**
Скачивай приложения только
из официальных магазинов.
Антивирус - твой верный
друг!



Не бойся просить о помощи!
Если тебя что-то тревожит в
Интернете, расскажи об этом
родителям или учителю.
Вместе вы сможете решить
любую проблему.



**Интернет - это круто, но
помни о безопасности!**
Соблюдая эти правила, ты
сможешь стать настоящим
кибергероем!



mvd.gov.by



ВНИМАНИЕ, МОШЕННИКИ!

Вам звонят посредством мессенджера
или с неизвестного номера...

ВАШИ ДЕЙСТВИЯ:

- не паникуйте и не верьте тому, что вам говорят
- не выполняйте никаких действий по просьбе третьих лиц
- прекратите разговор
- перезвоните родственникам и убедитесь, что ничего не случилось
- сообщите в милицию о звонке

ВАШ СЫН
ПОПАЛ В БЕДУ!
НУЖНЫ
ДЕНЬГИ!

?



mvd.gov.by



МТ «Общественная информационная телекомпания «Беларусь» на 1. Мая»
©2020. Мінска-Між. – Белорус. респ. Сув. права. 01
Свабоднае выданне ў Мінска-Між. на 1. Мая 2020 г.

НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ ФИНАНСОВОЙ ГРАМОТНОСТИ

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ

НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ

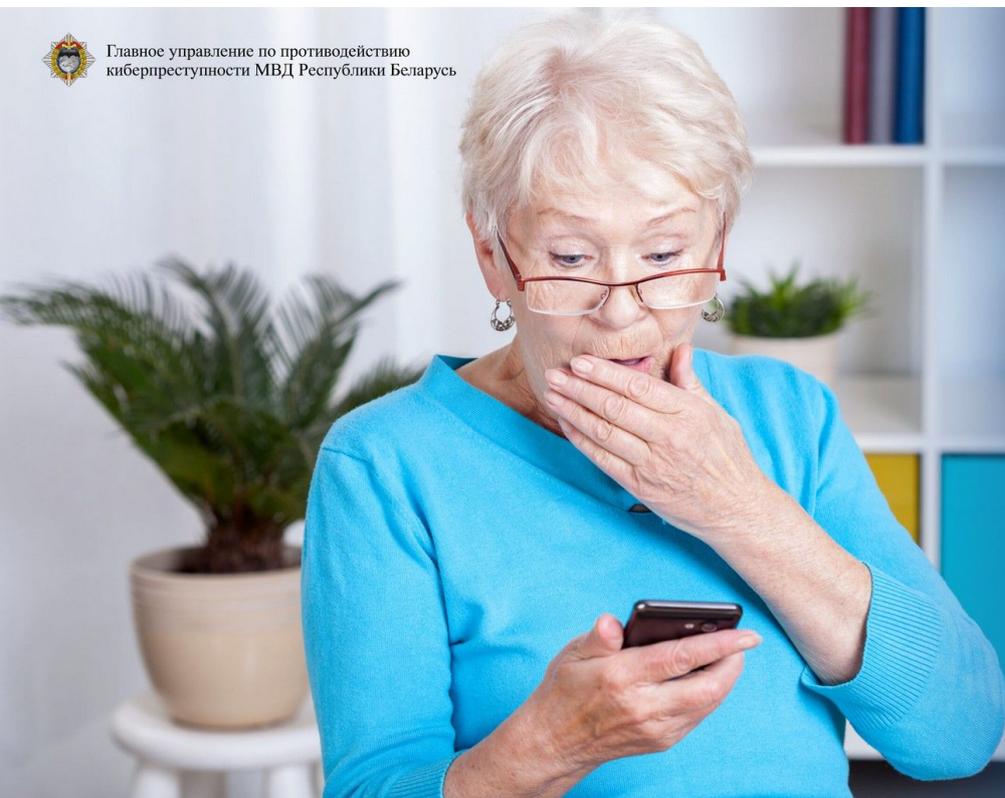
НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ



Главное управление по противодействию
киберпреступности МВД Республики Беларусь



Главное управление по противодействию
киберпреступности МВД Республики Беларусь



**НАУЧИТЕ
РОДИТЕЛЕЙ
ФИНАНСОВОЙ
ГРАМОТНОСТИ**

**ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ**

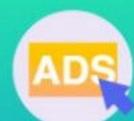
**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ**

**НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ**

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ



Всегда проверяй
ссылки на ресурсы



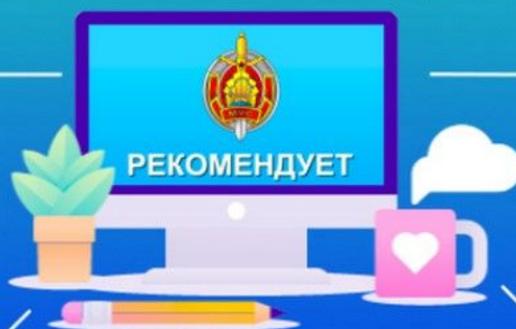
Остерегайся
назойливой рекламы



Используй
сложные пароли



Не переходи по
незнакомым ссылкам



Используй только
безопасные платежи



Подключайся к
безопасным сетям



Используй проверенные
программы

MVD.GOV.BY

MVD.GOV.BY

MVD.GOV.BY

MVD.GOV.BY

Осторожно - мошенники!

Как не стать жертвой киберпреступника



Помните! Никому нельзя сообщать: номер, срок действия, коды подтверждения на обороте карты, коды из СМС-сообщений, логины и пароли.



Designed by www.behance.net/Procyon

НЕ СТАНЬТЕ ЖЕРТВОЙ КИБЕР- ПРЕСТУПНИКА

**НЕЛЬЗЯ СООБЩАТЬ (ПЕРЕДАВАТЬ) И
КОМУ-ЛИБО ПОКАЗЫВАТЬ ДАННЫЕ:**



банковской карты, срок ее
действия и трехзначный код на
обратной стороне карты

полученные в виде SMS-сообщений,
сеансовые пароли, код авторизации



OV.BY

Управление внутренних дел
Минского областного
исполнительного комитета

MYD.GOV.BY





Советы по защите персональных данных в сети Интернет

Будьте внимательны, размещая личные данные в сети Интернет, не доверяйте важную информацию непроверенным сайтам

При регистрации на сайтах внимательно читайте политику обработки персональных данных

Не отправляйте незнакомым людям свои фотографии, копии паспорта и других документов

Не сообщайте никому данные банковских карт, даже если звонящие представляются сотрудниками банков или социальных служб

При регистрации в сети Интернет придумывайте сложные пароли



Не переходите по ссылкам с непроверенных сайтов, не открывайте незнакомые файлы

Не ставьте метки геолокации, не указывайте адрес проживания

Не отвечайте на письма о выигрыше в лотереях, в которых Вы не участвовали

Не сохраняйте личные данные на общедоступном компьютере

Будьте осторожны при общении с незнакомыми людьми в сети Интернет

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

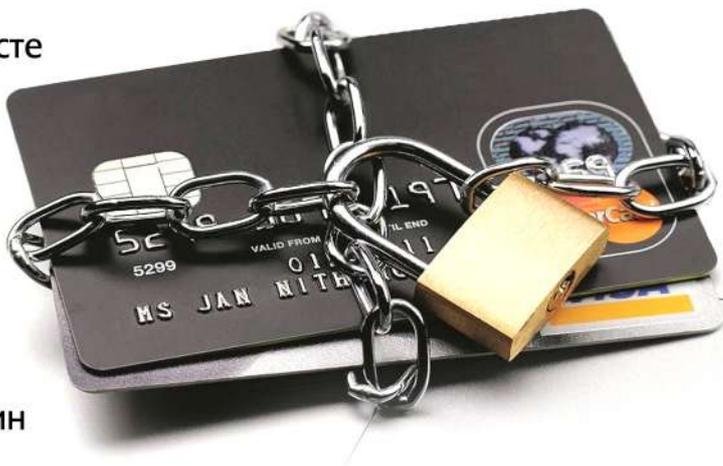


Хранить пинкод вместе с картой



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!

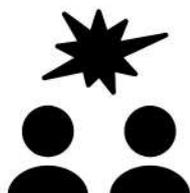


Размещать персональную и контактную информацию о себе в открытом доступе



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

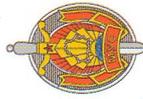
БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ**НЕОБХОДИМО:**

- + 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