

С 27 мая по 5 июня 2024 г. проводится профилактическая акция «Декада кибербезопасности».



# 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**

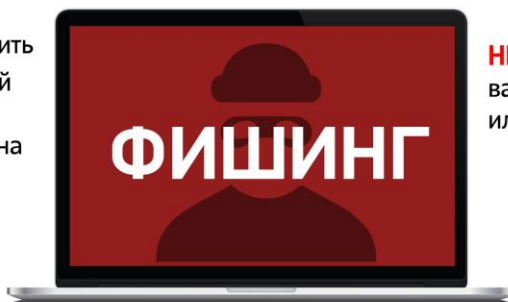
# ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ



**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 SMS-сообщении



**Сохрани эту информацию и поделись с другими**

**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
- У ВАС ОБНАРУЖЕНО ОПАСНОЕ ЗАБОЛЕВАНИЕ, ПРЕДЛАГАЮТ БЫСТРОЕ ОБСЛЕДОВАНИЕ ИЛИ ЛЕЧЕНИЕ «УНИКАЛЬНЫМ» ЛЕКАРСТВОМ
- ВАМ ВЫДЕЛЕНА БЕСПЛАТНАЯ ПУТЕВКА В САНАТОРИЙ, НО НУЖНО НЕМНОГО ДОПЛАТИТЬ, НАПРИМЕР, ЗА ВЫБОР МЕСТА ОТДЫХА
- ВЫ ВЫИГРАЛИ В ЛОТЕРЕЕ ИЛИ РОЗЫГРЫШЕ ПРИЗОВ, ДЛЯ ОФОРМЛЕНИЯ ПОТРЕБУЕТСЯ ВНЕСТИ НЕБОЛЬШИЕ ДЕНЬГИ
- 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

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

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

**НИКАКИХ ДОПЛАТ ОФИЦИАЛЬНЫЕ СОЦИАЛЬНЫЕ СЛУЖБЫ НИКОГДА НЕ ТРЕБУЮТ**

**НЕ ВЕРЬТЕ, ВАМ НАВЕРЯКА ЗВОНЯТ МОШЕННИКИ**

**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**

СОХРАНИ ИНФОРМАЦИЮ

НАУЧИТЬСЯ ПОЛЬЗОВАТЬСЯ ИНТЕРНЕТОМ ПРАВИЛЬНО!

**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**

**НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ  
ФИНАНСОВОЙ ГРАМОТНОСТИ**

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ  
**НЕ** УСТАНОВЛИВАЙТЕ  
ПРОГРАММЫ  
**НЕ** ПЕРЕВОДИТЕ  
ДЕНЬГИ



Главное управление по противодействию  
киберпреступности МВД Республики Беларусь

# 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 

# 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



# 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

**ГЛАВНЫЕ  
ПРАВИЛА  
ЦИФРОВОЙ  
ГИГИЕНЫ**



**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!**



**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!

## ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ

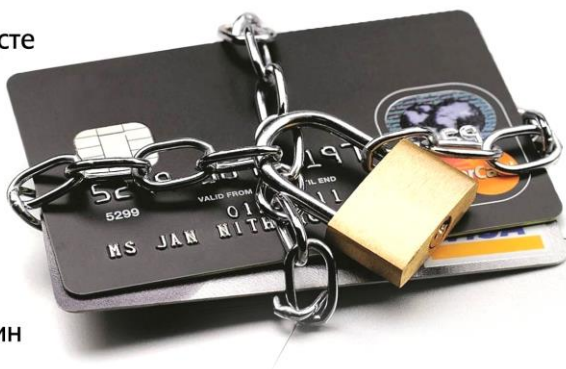


**Хранить** пинкод вместе с картой



**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**

**Безопасный Интернет для детей**

**ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ**

**НЕ отправляй незнакомящим свои фото и видео**  
Злоумышленники могут узнать что-то нужное о твоей жизни

**НЕ встречайся с людьми, с которыми знакомишь только в интернете**  
За маской онлайн-собеседника может скрываться злоумышленник

**НЕ сообщай в интернете свой реальный адрес и телефон**  
Злоумышленник может встретить тебя с неожиданными намерениями

**НЕ отправляй личные данные для участия в конкурсах на малоизвестных сайтах**  
Информацией могут завладеть и воспользоваться злоумышленники

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

**не дай себя обмануть!**

научись пользоваться интернетом правильно!

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, ОПАСНОСТЬ !

## ЗАЩИТИТЕ СЕБЯ ОТ МОШЕННИКОВ:

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

**НЕ ВЕРЬТЕ** обещаниям внезапных выигрышей

**НЕ ИСПОЛЬЗУЙТЕ** одинаковые пароли для всех  
аккаунтов

**НЕ УКАЗЫВАЙТЕ** личную информацию в открытых  
источниках

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



## НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

Если вы или ваши близкие стали  
жертвами мошенников, или вы  
подозреваете, что в отношении вас  
планируются противоправные действия  
**НЕЗАМЕДЛИТЕЛЬНО СООБЩАЙТЕ В МИЛИЦИЮ!**

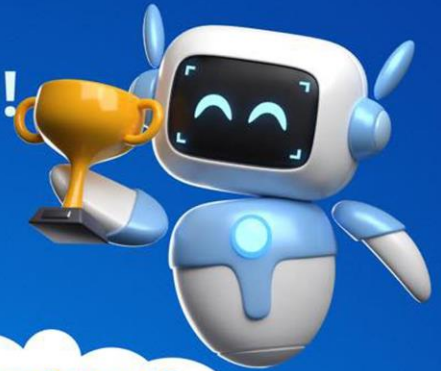
# 102



[mvd.gov.by](http://mvd.gov.by)



# 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.



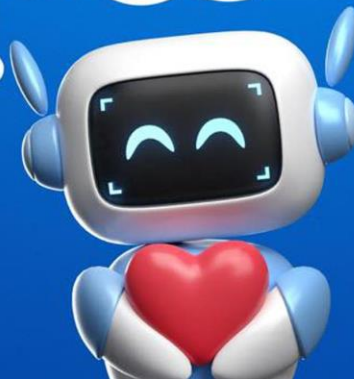
Будь осторожен, как на  
минном поле!  
Скачивай приложения только  
из официальных магазинов.  
Антивирус - твой верный  
друг!



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](http://mvd.gov.by)



# 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

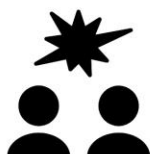
### НЕЛЬЗЯ



**Реагировать** на письма от неизвестного отправителя



**Открывать** подозрительное вложение к письму



**Отвечать** на агрессию и обидные выражения



**Сохрани эту информацию и поделись с другими**