

«ДЕКАДА КИБЕРБЕЗОПАСНОСТИ»: КАК ЗАЩИТИТЬСЯ ОТ КИБЕРПРЕСТУПЛЕНИЙ

С 27 мая по 5 июня 2024 года в Республике Беларусь проходит акция «Декада кибербезопасности». Декада направлена на противодействие киберпреступности, повышение цифровой грамотности детей и взрослых, а так же пожилых граждан. В ходе ее проведения МВД планирует осуществить комплекс информационно-профилактических мероприятий и выступлений в средствах массовой информации.

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!

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 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 используйте одинаковые пароли для всех аккаунтов



НЕ сообщайте свои персональные данные и данные банковской карты



НЕ указывайте личную информацию в открытых источниках



Сохрани эту информацию и поделись с другими



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 sms-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! **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!

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

научись пользоваться интернетом правильно!

СОХРАНИ
ИНФОРМАЦИЮ



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 отправляй незнакомцам
свои фото и видео**

Злоумышленники могут узнать
что-то важное 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, 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



! 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



НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ ФИНАНСОВОЙ ГРАМОТНОСТИ

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ

НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ

НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ



Главное управление по противодействию
киберпреступности МВД Республики Беларусь

112 BY

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 РАЗБЛОКИ-
РОВАТЬ 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

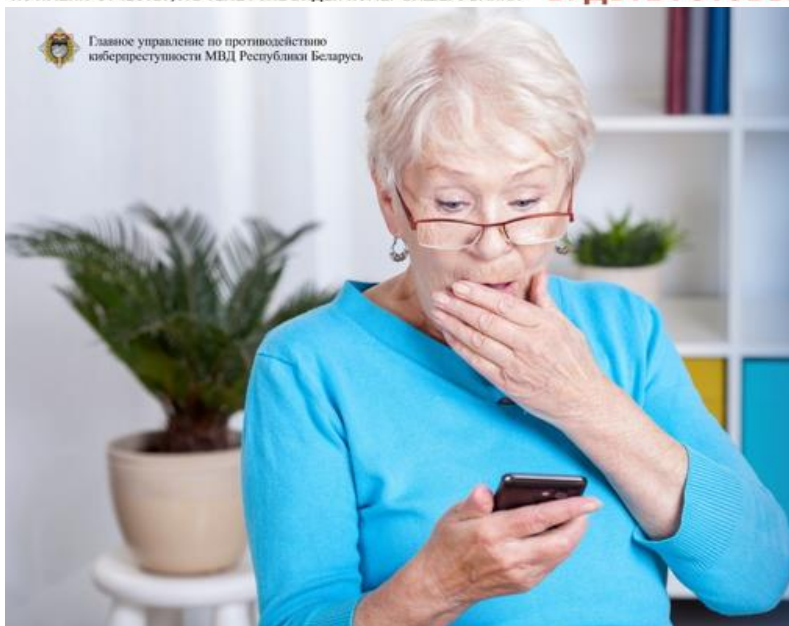
ВАЖНО!

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

БУДЬТЕ ГОТОВЫ И ПРОЯВИТЕ БДИТЕЛЬНОСТЬ



Главное управление по противодействию
киберпреступности МВД Республики Беларусь



**НАУЧИТЕ
РОДИТЕЛЕЙ
ФИНАНСОВОЙ
ГРАМОТНОСТИ**

**ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ**

НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ

НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ

112 BY

ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 

поступает звонок
с **неизвестного**
номера

2 

звонящий
представляется
вашим
родственником

3 

он говорит,
что **сбита человека**
или из-за него
человек
попал в ДТП

4 

он просит денег
как **компенсацию**
вроде или
чтобы **закончить дело**

5 

затем звонит
близким и
ославдовывает
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

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

