Министерство внутренних дел Республики Беларусь

Служим Закону, Народу, Отчизне!

Покупки через Интернет - не стань жертвой обмана!

Покупки через Интернет – это без сомнения очень удобно. Сфера Интернет-услуг расширяется, доходы сетевых ритейлеров растут, а люди все чаще предпочитают заказ товаров в сети походам по магазинам. Однако удобство Интернет-технологий распространяется не только на продавцов и покупателей. Мошенники также по достоинству оценили новые формы торговли и активно используют их своих целях.

Для того, чтобы радость онлайн-покупок не была омрачена получением некачественного товара или потерей денег мы рекомендуем вам обратить внимание на некоторые признаки потенциально опасных Интернет-магазинов.

1. Низкая цена. Если вы нашли объявление или магазин, предлагающий товары по ценам существенно ниже рыночных, имейте в виду, что мошенники часто используют данный прием для привлечения жертв.

> На что следует обратить внимание? Посмотрите стоимость аналогичных товаров в других Интернет-магазинах, она не должна отличаться слишком сильно. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион».

2. Требование предоплаты. Если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица, нужно понимать, что данная сделка является опасной.

> На что следует обратить внимание? Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинги продавца в платежных системах.

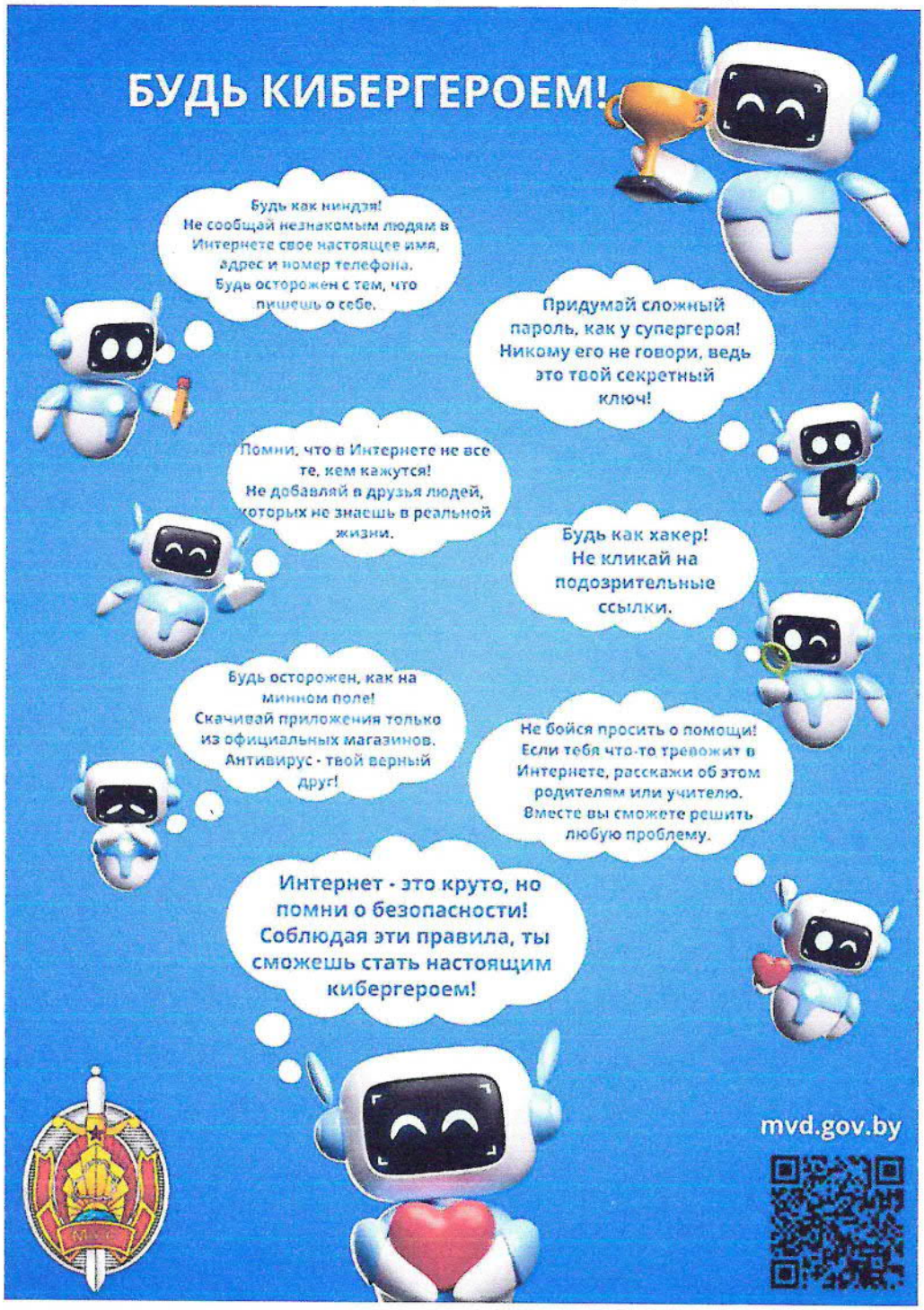
3. Отсутствие возможности курьерской доставки и самовывоза товара. Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату.

> На что следует обратить внимание? Выбирая из нескольких магазинов, следует отдать предпочтение тому, в котором есть возможность забрать товар самостоятельно. Злоумышленники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. Отсутствие контактной информации и сведений о продавце. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном, такой магазин может представлять опасность.

> На что следует обратить внимание? Внимательно изучите сведения о продавце. Помните о том, что вы собираетесь доверить деньги лицу или компании, о которой вы ничего не знаете. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Проверьте отзывы о магазине в открытых Интернет-рейтингах, пролистайте отзывы как можно дальше, злоумышленники могут прятать негативные отзывы за десятками фальшивых положительных оценок. В случае совершения покупок посредством электронных досок объявлений посмотрите историю сделок продавца и ознакомьтесь с его рейтингом, многие торговые площадки предлагают подобную услугу.

5. Отсутствие у продавца или магазина «истории». Если Интернет-магазин или учетная запись продавца зарегистрированы несколько дней назад, сделка с ними может быть опасной.


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

банк для их возврата по принципу «нулевой ответственности»	
Безопасность электронной почты	
Подключить двухфакторную аутентификацию	Реагировать на письма от неизвестного отправителя: скорее всего, это спам или «фишинговая» рассылка
Использовать минимум 2 типа e-mail адресов: закрытые (только для привязки устройств и средств защиты, интернет-банкинга и др.), открытые (отдельные для переписки, регистрации на форумах, оформления различных подписок и т.д.)	Открывать подозрительные вложения к письму: сначала позвоните отправителю и узнайте, что это за файл
Использовать спам-фильтры и соответствующее антивирусное программное обеспечение	Отправлять в открытом виде важные данные (фотоизображения документов, пароли и т.д.). В случае необходимости – заархивировать, установив сложный пароль
В случае подозрительных ситуаций проверить статистику подключений и изменить пароль	
Надежные пароли	
Создавать персональные (уникальные) пароли к разным сервисам	Хранить пароли на бумажных носителях, рабочем столе компьютера и в других легкодоступных местах, а также передавать их кому-либо
Использовать сложные пароли: минимум 12 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и т.д.	Сохранять пароль автоматически в браузере
Доверять только проверенным менеджерам паролей	Использовать в качестве пароля свой логин (имя пользователя, учетной записи, никнейм, дату рождения и т.д.)
Регулярно производить смену паролей	Использовать повторение символов, биографическую информацию и сведения, обнародованные в социальных сетях
Использование браузеров и сайтов	
Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать неблагоприятных последствий после посещения зараженных сайтов	Переходить по непроверенным ссылкам и посещать сайты сомнительного содержания
Производить регулярное обновление ПО, антивирусов и файерволов	Вводить информацию на сайтах, если соединение не защищено (нет https)
Обращать внимание при авторизации на доменное имя интернет-ресурса (может произойти подмена имени сайта с целью «фишинга»)	Открывать всплывающие окна, рекламные баннеры и устанавливать

	предлагаемое неизвестными сайтами ПО
Использование приложений, соцсетей и мессенджеров	
По возможности скрывать номер телефона, адрес электронной почты и другие сведения	Размещать персональную и контактную информацию о себе в открытом доступе
Обмениваться сообщениями в соцсетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения	Использовать указание геолокации на фото и постах
Устанавливать программное обеспечение только из достоверных источников	Отвечать на обидные выражения и агрессию в соцсетях – лучше написать об этом администратору ресурса
Безопасность мобильных устройств	
Использовать пин-код, а также дополнительные способы блокирования устройства (графический ключ, пароль, отпечаток пальца и др.)	Передавать незнакомым мобильный телефон или сим-карту. В случае передачи – контролировать все действия, которые производятся с устройством
Своевременно обновлять операционную систему устройства, антивирус и др. ПО	Устанавливать приложения с низким рейтингом и отрицательными отзывами
Устанавливать приложения из PlayMarket, AppStore или только из проверенных источников	Перезванивать на незнакомые иностранные номера
Обращать внимание, к каким функциям гаджета приложение запрашивает доступ	Хранить важную информацию на мобильном устройстве
Включить встроенные функции устройства для определения его местонахождения	Делать полное снятие ограничения на устройстве («джейлбрейк», режим «суперюзера»)
В случае утери (кражи) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам, а также обратиться в правоохранительные органы	
При смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру (лучше сделать это заблаговременно)	
При продаже устройства произвести его сброс до заводских настроек	
Безопасный Wi-Fi	
После установки устройства для доступа к Wi-Fi сразу же поменять пароль и логин, установленные по умолчанию	Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым)


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 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

БЕЗОПАСНЫЙ ИНТЕРНЕТ

- Привет, как тебя зовут?

- Алина!

- А меня Борис, мне 14 лет. А тебе?

- А мне 12.

- А у тебя есть твои личные фотографии? Может ты сфотографируешься для меня? Давай обменяемся фотографиями!

- Алина, а давай встретимся?

- Давай, а где?

- А ты знаешь, около школы № 3 есть заброшенный дом. Может там?

- Не знаю, а там не страшно?

✓ *Подумай, прежде чем выслать виртуальному другу информацию о себе или личные фото! Ты не можешь знать, как они будут использованы.*

✓ *Фотографии, попав в виртуальный мир, остаются там надолго. Их нельзя уничтожить, даже если ты уберешь их со своего сайта. Размещая интимные фотографии, подумай о том, что их могут увидеть друзья, родители, знакомые.*

✓ *Ты не знаешь, кем твой виртуальный друг может оказаться в реальной жизни. Если ты решишь встретиться с человеком, которого знаешь только по общению в Интернете, сообщи об этом кому-то из взрослых и пригласи с собой на встречу друга из реального мира. Выбирай для встреч людные места и светлое время суток.*

✓ *Помни, то, о чем ты читаешь или что видишь в Интернете, не всегда является правдой.*

✓ *Если тебя что-то смущает или пугает в виртуальном мире, либо ты получаешь письмо или сообщения с угрозами, оскорблениями, скажи об этом родителям или человеку, которому ты доверяешь.*

Милиция общественной безопасности МВД Республики Беларусь

НАУЧИСЬ ПОЛЬЗОВАТЬСЯ ИНТЕРНЕТОМ ПРАВИЛЬНО!

БЕЗОПАСНЫЙ ИНТЕРНЕТ ДЛЯ ДЕТЕЙ

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

СОХРАНИ ИНФОРМАЦИЮ

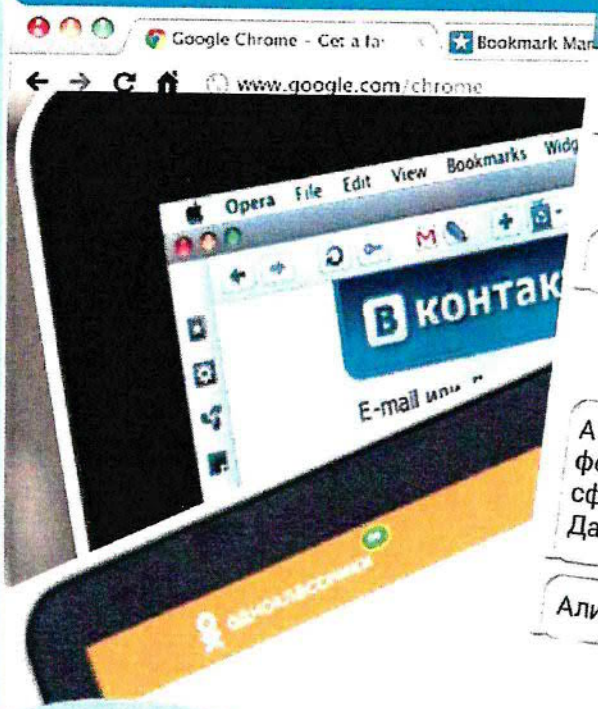
- не сообщай незнакомцам свой логин и пароль
- не открывай файлы из непроверенных источников
- не заходи на сайты, которые защита компьютера считает подозрительными

не дай себя обмануть!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный единый номер 102

БЕЗОПАСНЫЙ ИНТЕРНЕТ



Привет, как тебя зовут?

Алина!

А меня Борис, мне 14 лет. А тебе?

А мне 12.

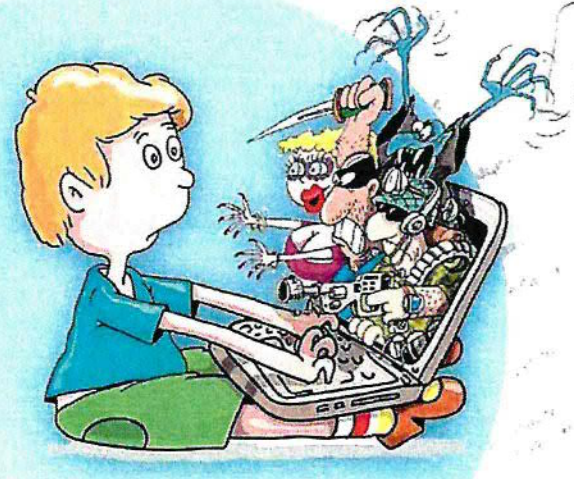
А у тебя есть твои личные фотографии? Может, сфотографируешься для меня? Давай обменяемся фотографиями!

Алина, а давай встретимся?

Давай, а где?

А ты знаешь, около школы № 3 есть заброшенный дом. Может, там?

Не знаю, а там не страшно?



Подумай, прежде чем выслать виртуальному другу информацию о себе или личные фото! Ты не можешь знать, как они будут использованы.

Фотографии, попав в виртуальный мир, остаются там надолго. Их **нельзя уничтожить**, даже если ты уберешь их со своего сайта. Размещая интимные фотографии, подумай о том, что **их могут увидеть друзья, родители, знакомые**.

Ты не знаешь, кем твой виртуальный друг может оказаться в реальной жизни. Если ты решишь встретиться с человеком, которого знаешь только по общению в Интернете, **сообщи об этом** кому-то из взрослых и пригласи с собой на встречу друга из реального мира. **Выбирай** для встреч людные места и светлое время суток.

Помни, то, о чем ты читаешь или что видишь в Интернете, **не всегда является правдой**.

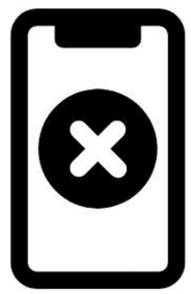
Если тебя что-то смущает или пугает в виртуальном мире, либо ты получаешь письмо или сообщения с угрозами, оскорблениями, **скажи об этом** родителям или человеку, которому ты доверяешь.

МИЛИЦИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ

НЕ следуй инструкциям незнакомцев, позвонившим с неизвестного номера

НЕ сообщай неизвестным лицам свои персональные данные



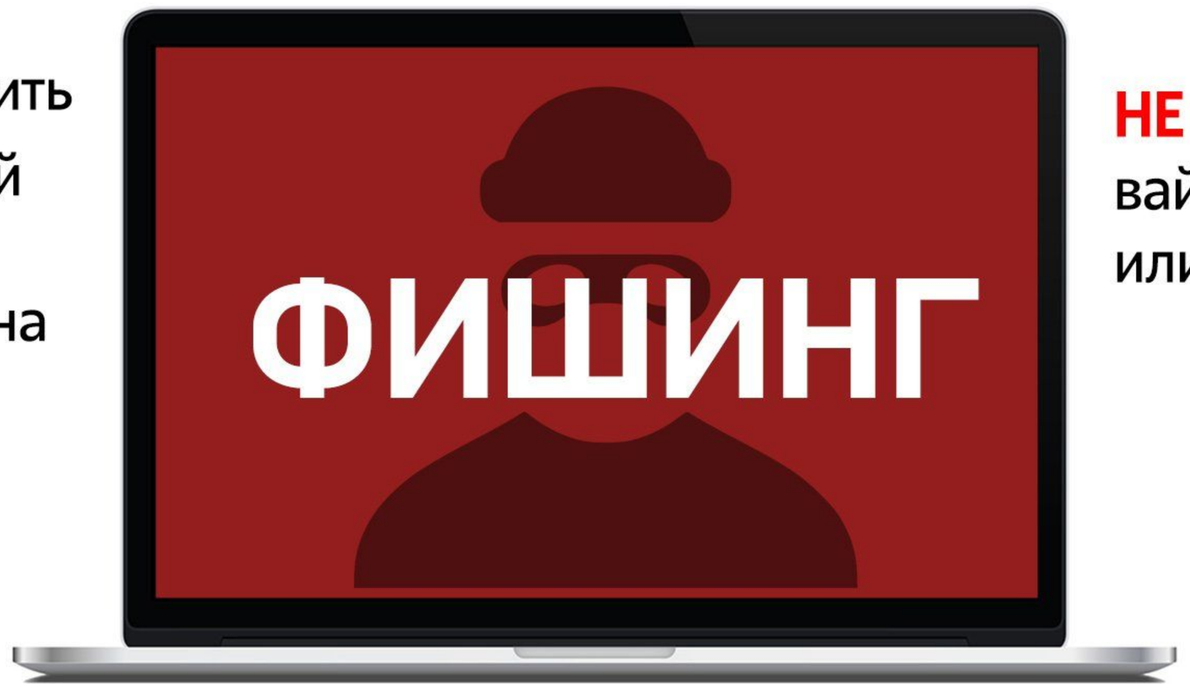
НЕ совершай никаких действий на смартфоне по просьбе посторонних лиц

НЕ переводи деньги незнакомым людям в качестве предоплаты

Сохрани эту информацию и поделись с другими

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

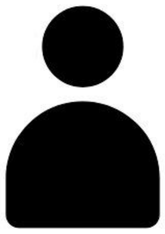
Фишинговая ссылка может прийти в мессенджере, по электронной почте, в смс-сообщении

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

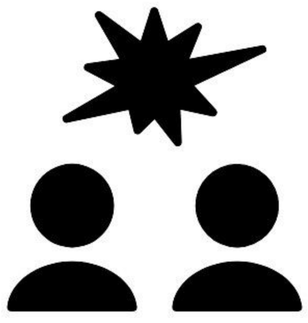
НЕЛЬЗЯ



Размещать персональную и контактную информацию о себе в открытом доступе

Реагировать на письма от неизвестного отправителя

Использовать указание геолокации на фото в постах



Отвечать на агрессию и обидные выражения

Открывать подозрительное вложение к письму

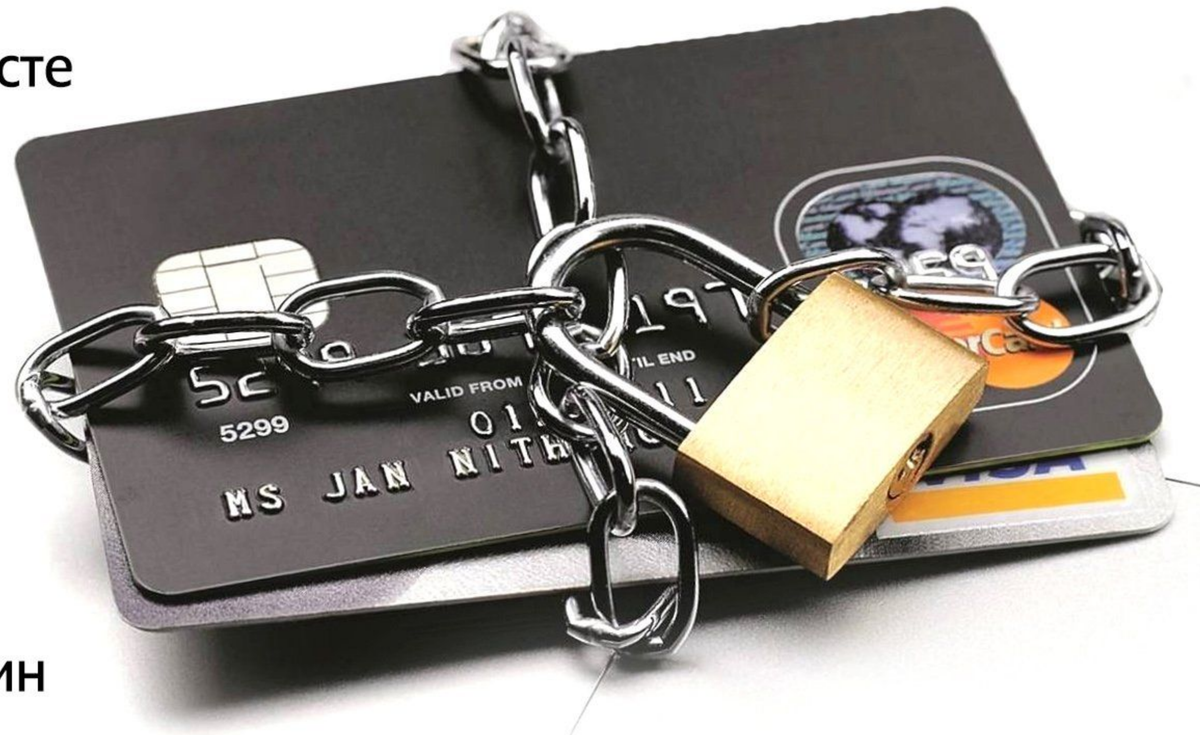
Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ

НЕЛЬЗЯ

Хранить пинкод вместе с картой



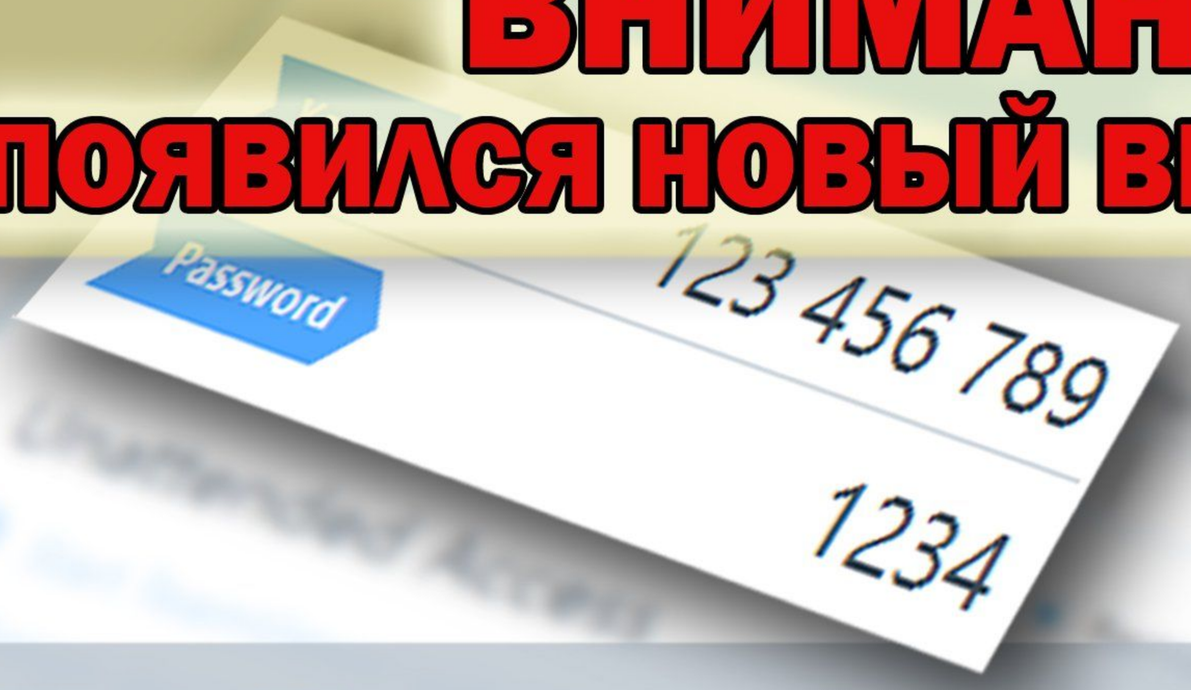
Сообщать CVV-код или отправлять его фото

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

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

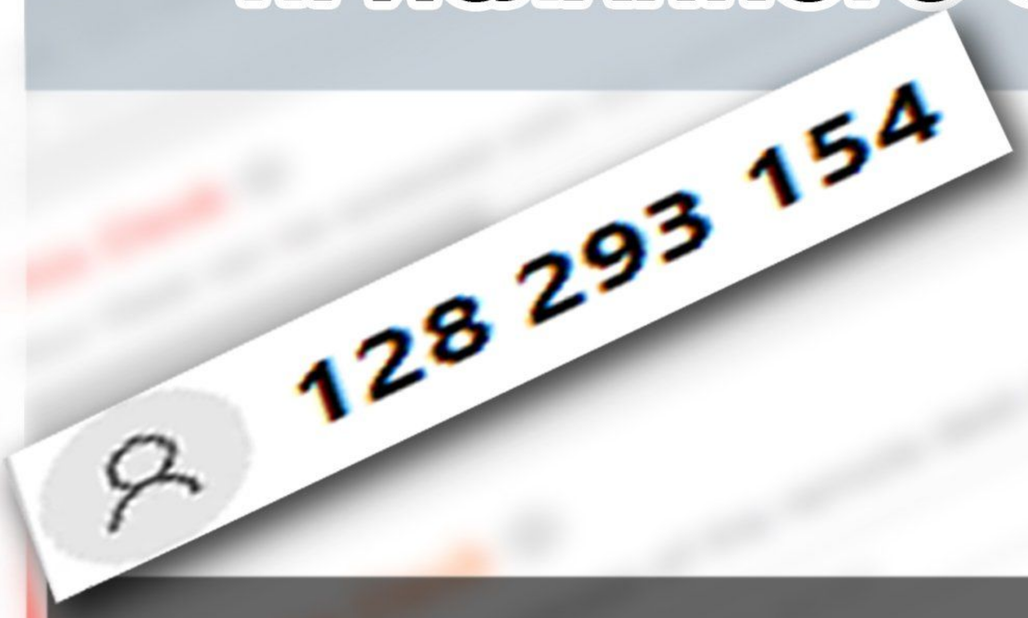
Сохрани эту информацию и поделись с другими

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



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

УПРАВЛЕНИЕ «К» МВД БЕЛАРУСИ

6 правил информационной безопасности

главное управление по противодействию киберпреступности КМ 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 🔒)

6 правил информационной безопасности

главное управление по противодействию киберпреступности КМ МВД Беларуси

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

ЧТО ТАКОЕ КИБЕРБЕЗОПАСНОСТЬ?

Безопасность коммуникации

Операционная безопасность

Безопасность информации

Кибербезопасность*

Военная безопасность

Физическая безопасность

*Определение European Union Agency For Network And Information Security

ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- **сотрудником Банка;**
- **сотрудником службы безопасности Банка;**
- **сотрудником Росфинмониторинга;**
- **сотрудником больницы;**
- **сотрудником благотворительной организации;**
- **родственником.**

И НАЗВАТЬ ПРИЧИНУ ЗВОНКА:

- **ваша карта заблокирована;**
- **в отношении вашей карты предпринимаются мошеннические действия;**
- **вашему родственнику нужна помощь или лечение;**
- **вам положена отсрочка по кредиту или пособие.**

ОН МОЖЕТ ПОПРОСИТЬ:

Данные карты:

- **номер карты;**
- **CVV/CVC-код;**
- **PIN-код;**
- **срок действия карты.**

Пароль:

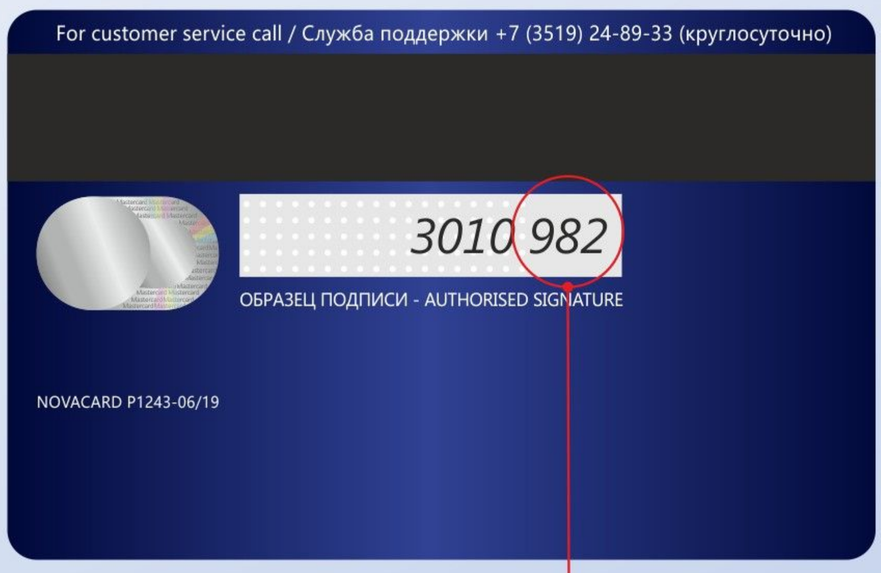
- **от интернет-банка;**
- **из SMS-сообщения** *(для входа в интернет-банк или подтверждения операции).*

Перевести деньги:

- **на специальный счет или карту, где они будут в безопасности.**

НЕ

- **сообщайте никому данные карты;**
- **сообщайте никому пароли и коды из SMS;**
- **выполняйте действия с банковской картой по просьбе третьих лиц.**



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 отправляй незнакомцам свои фото и видео

Злоумышленники могут узнать что-то нужное 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**

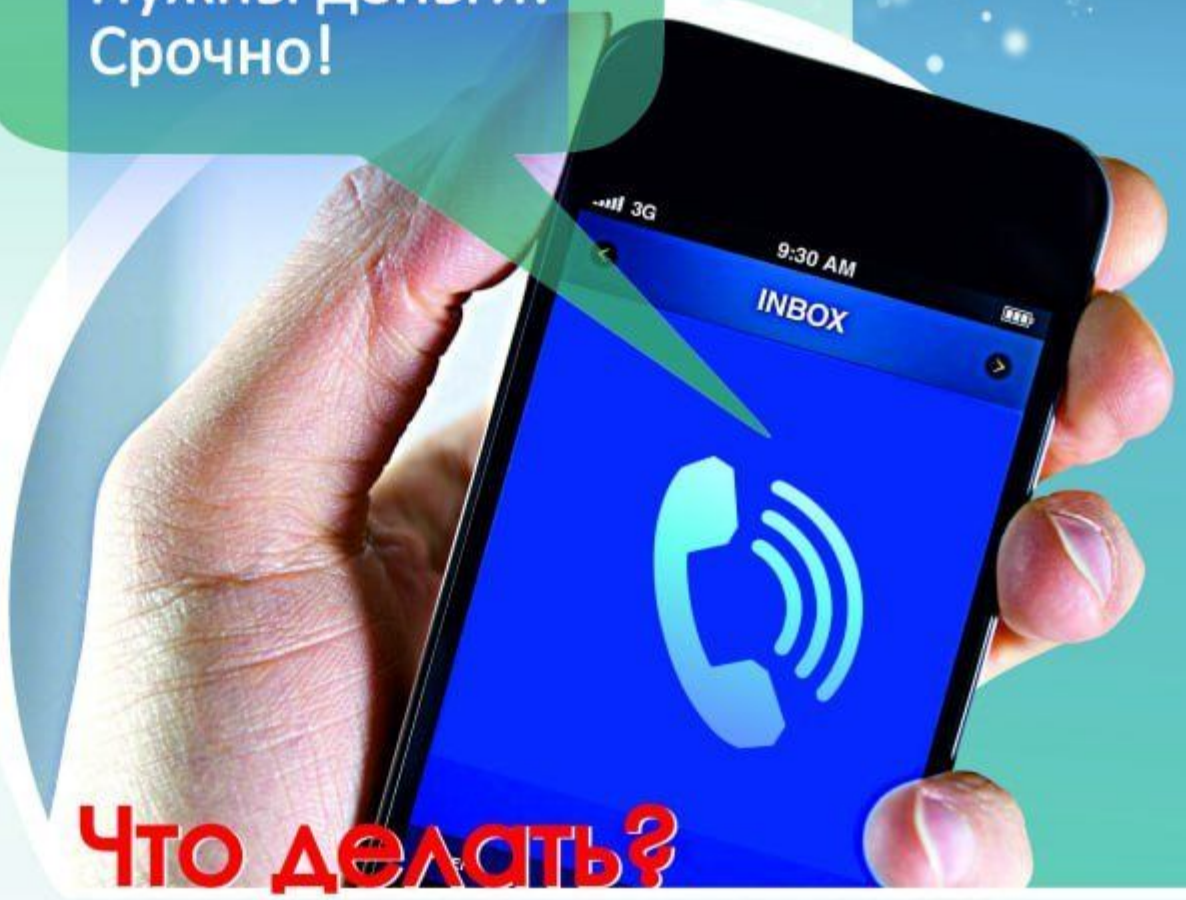
4 он просит **денег**, как **компенсацию вреда** или чтобы **«замять» дело**

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!

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

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.

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

РОДИТЕЛИ! научите детей пользоваться интернетом правильно!

ГЛАВНЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

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

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

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

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.

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

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 проиводействию 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

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**

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 ПОЗВОНИТЬ ПО ПОВОДУ ТОВАРА НА ТОРГОВОЙ ПЛОЩАДКЕ И ПРЕДЛОЖИТЬ СДЕЛКУ С ПРЕДОПЛАТОЙ

АФЕРИСТ МОЖЕТ ПРЕДСТАВИТЬСЯ БАНКОВСКИМ РАБОТНИКОМ И ВЫМАНИТЬ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ

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 ДАННЫЕ (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:

с 14 лет

Статья 212 УК Беларуси

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.

с 16 лет

Статья 349 УК Беларуси

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**.

Управление информации и общественных связей МВД Республики Беларусь

ВНИМАНИЕ! ОТКРЫТЫЙ WI-FI

УГРОЗА ДЛЯ ВЛАДЕЛЬЦЕВ WI-FI:

- 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

УГРОЗА ДЛЯ ПОЛЬЗОВАТЕЛЕЙ:

- 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

ФИШИНГ: КАК ЗАЩИЩИТЬ 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: SB.BY БЕЛАРУСЬ СЕГОДНЯ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ