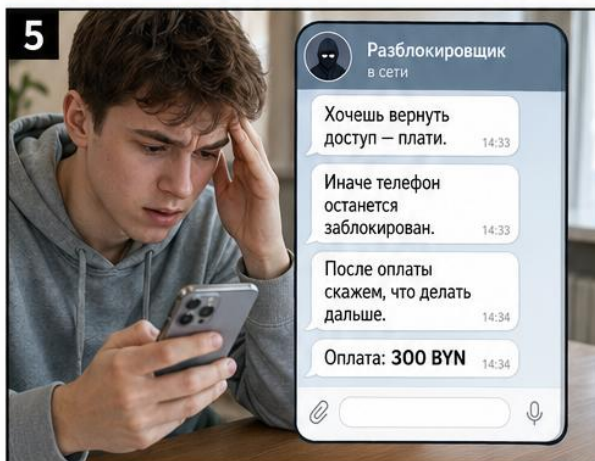
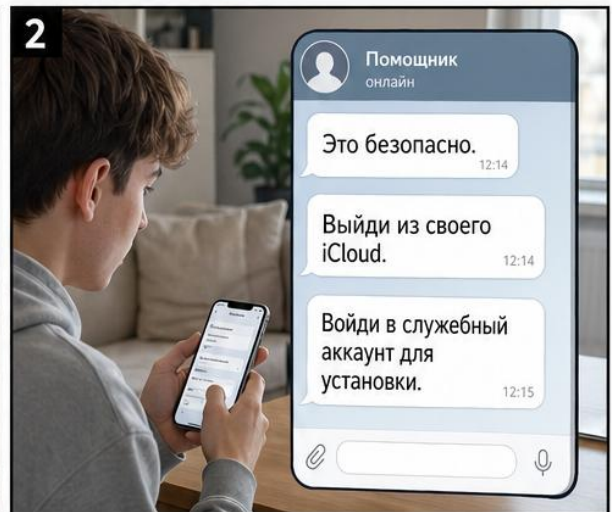
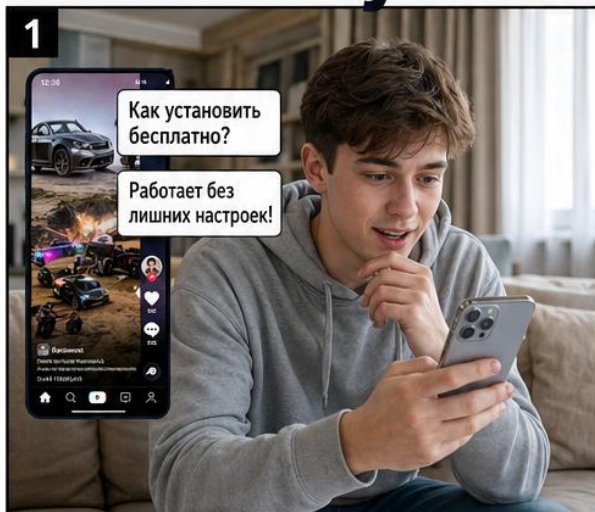


Квартира по предоплате



- ❗ Не переводите предоплату за аренду жилья незнакомым лицам.
- 🔍 Не соглашайтесь на “бронирование” без личного осмотра квартиры и проверки документов.
- ⚠ Если вас торопят с оплатой — это может быть мошенничество.

Чужой iCloud



- ✓ Не выходите из своего iCloud по совету незнакомцев.
- ✓ Не входите в “служебные” или “файловые” Apple ID.
- ⚠ Если вас просят сменить iCloud ради установки — это мошенники.



ОПАСНЫЙ ЗВОНОК

1

Добрый день, это Энергосбыт. Проводится проверка счётчиков. Нужно уточнить ваши данные для оформления заявки.



2

Назовите, пожалуйста, фамилию, имя, отчество.

Подтвердите ваши данные.

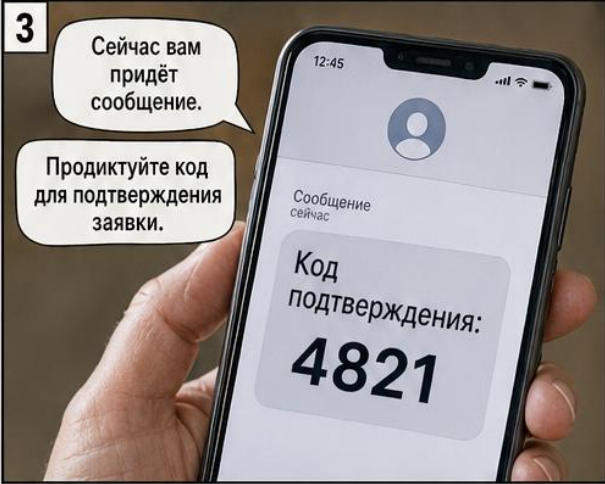
Хорошо... сейчас скажу.



3

Сейчас вам придёт сообщение.

Продиктуйте код для подтверждения заявки.



Сообщение сейчас

Код подтверждения:
4821

4

Неизвестные получили доступ к интернет-банкингу. Со счёта начали исчезать деньги.

Операции по счёту	
Перевод средств	-150 BYN 12:48
Перевод средств	-320 BYN 12:49
Перевод средств	-200 BYN 12:50
Баланс:	350 BYN



5

Все сбережения были сняты. Мошенники использовали коды для входа в банк.

Операции по счёту	
Перевод средств	-500 BYN 12:51
Перевод средств	-1 200 BYN 12:52
Перевод средств	-350 BYN 12:53
Перевод средств	-800 BYN 12:54
Баланс:	20 BYN



6

Я думала, что это обычная проверка...





Не сообщайте по телефону персональные данные и коды из SMS.



Сотрудники коммунальных служб не просят коды подтверждения.



Если вас торопят и просят назвать код – это мошенники.

Код для домофона



Не сообщайте коды из SMS.



Правоохранительные органы и банки не требуют переводить деньги на "безопасный счёт".



Когда вас пугают и торопят — это мошенники.

“Выгодная покупка”



Не переходите по сомнительным ссылкам при онлайн-покупках.



Не вводите данные карты на непроверенных сайтах.



Слишком выгодная цена и спешка — частые признаки мошенничества.

ВЫГОДНАЯ ПОКУПКА

История о том, как мошенники обманывают при покупке онлайн

1

Нашла отличный телефон по низкой цене

Объявление

Новый смартфон

350 BYN

вместо 700 BYN!

Цена слишком хорошая, но я напишу продавцу...

2

Торопит с оплатой...
Ладно, переведу предоплату.

Продавец
был(а) сегодня в 10:15

Товар в наличии!
Оплатите сейчас — отправлю сегодня.

10:15

Хорошо, готова оплатить.

10:16

Только предоплата.
Без предоплаты не бронирую.

10:16

Сообщение

3

Перевод по номеру карты

Сумма

120 BYN

Оплатить

Перевела предоплату 120 BYN

4

Ссылка выглядит странно...
Наверное, это ошибка?

Продавец
был(а) сегодня в 10:20

Для получения товара перейдите по ссылке для отслеживания доставки и подтвердите оплату доставки.

10:20

Внешняя ссылка для оплаты доставки

Нажмите здесь

5

Объявление удалено

Пользователь недоступен

Чат недоступен

Продавец исчез!
Деньги не вернули...

6

Сохранила переписку, чек и обратилась в милицию.

МИЛИЦИЯ
служим и защищаем



Не переводите предоплату
незнакомым лицам



Не вводите данные карты
по внешним ссылкам
и сомнительным сайтам



Если деньги похищены —
обратитесь в милицию

ОПАСНЫЙ ЗВОНОК



Безопасных
счетов
не существует



Не сообщайте
коды и данные
карты



Прекратите
разговор и сами
позвоните в банк

ВНИМАНИЕ ЗАЩИТИТЕ СВОИ МЕССЕНДЖЕРЫ



WhatsApp

- ОТКРОЙТЕ "WHATSAPP";
- ВКЛАДКА ":" ИЛИ "НАСТРОЙКИ";
- КОНФИДЕНЦИАЛЬНОСТЬ;
- ВЫЗОВЫ И СООБЩЕНИЯ;
- ВКЛЮЧИТЕ ОПЦИЮ "ЗАЩИТА ОТ ЛИШНИХ ЗВОНКОВ";
- ВО ВКЛАДКЕ "АККАУНТ" УСТАНОВИТЕ "ДВУХШАГОВУЮ ПРОВЕРКУ".



- ОТКРОЙТЕ "VIBER";
- ВКЛАДКА "ЕЩЁ";
- "НАСТРОЙКИ";
- ВЫЗОВЫ И СООБЩЕНИЯ;
- "ЗАЩИТА ОТ ЛИШНИХ ЗВОНКОВ";
- ВО ВКЛАДКЕ "КОНФИДЕНЦИАЛЬНОСТЬ" УСТАНОВИТЕ "ДВУХЭТАПНУЮ ПРОВЕРКУ".



- ОТКРОЙТЕ "TELEGRAM";
- ВКЛАДКА "НАСТРОЙКИ";
- КОНФИДЕНЦИАЛЬНОСТЬ;
- ДЛЯ ВСЕХ ВКЛАДОК (НОМЕР ТЕЛЕФОНА, ЗВОНКИ, СООБЩЕНИЯ) УСТАНОВИТЕ НАСТРОЙКУ "КОНТАКТЫ";
- УСТАНОВИТЕ "ОБЛАЧНЫЙ ПАРОЛЬ".



**ЗАЩИТИТЕ СЕБЯ РАНЬШЕ, ЧЕМ ДО ВАС
ДОБЕРУТСЯ МОШЕННИКИ**



ЛЕНИНСКИЙ РОВД Г. ГРОДНО

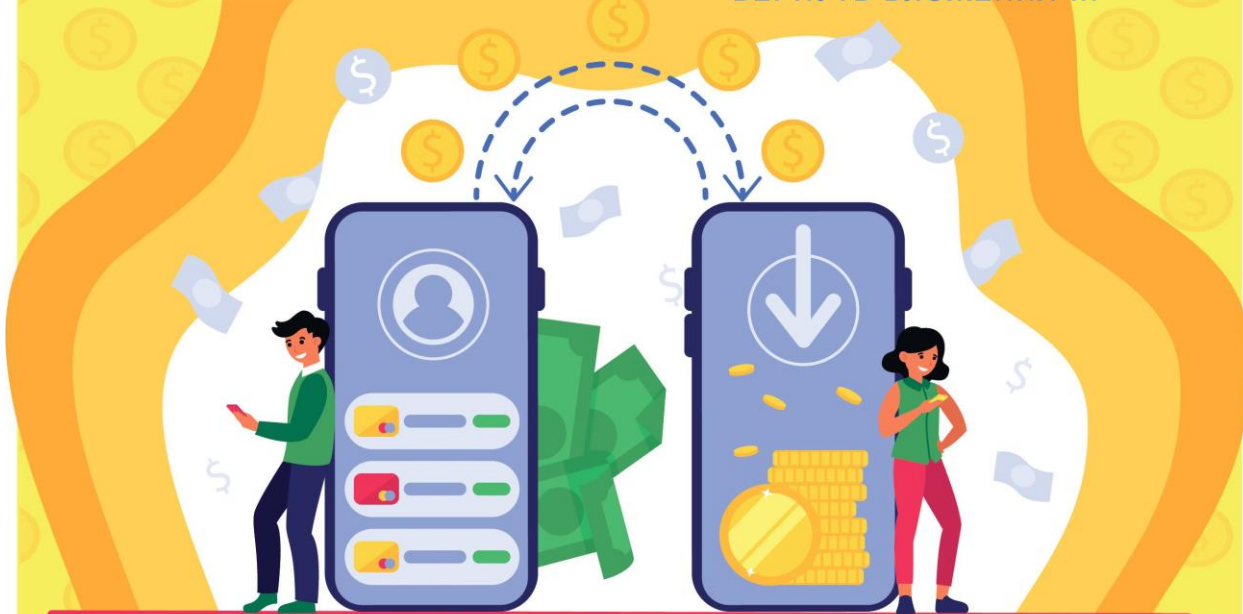
ИНВЕСТИРОВАНИЕ

ИНВЕСТИРОВАТЬ БЕЗОПАСНО ЗНАЧИТ БЫТЬ УМНЫМ И ОСТОРОЖНЫМ!

Перед тем как вложить
свои деньги,
обязательно посмотри,
кому ты их доверяешь.

ПЕРЕД ТЕМ КАК
ПЕРЕВОДИТЬ СБЕРЕЖЕНИЯ
НА СТОРОННИЕ СЧЕТА -
ПРОВЕРЬ ИНФОРМАЦИЮ
О РЕСУРСЕ В ИНТЕРНЕТЕ!!!!

ПРОВЕРИТЬ РЕСУРС 1 МИНУТА
ПЕРЕВОД ДЕНЕГ 1 КЛИК
ВЕРНУТЬ ВЛОЖЕНИЯ ...



Будь осторожен с объявлениями, которые обещают тебе быстро
заработать много денег.



УВД ГРОДНЕНСКОГО
ОБЛИСПОЛКОМА



MVD.GOV.BY

**НЕ ПОЗВОЛЯЙ МОШЕННИКАМ
ЗАБРАТЬ ТВОИ МЕЧТЫ!**

ТРЕЙДИНГ

КОГДА ТЫ СОБИРАЕШЬСЯ ЧТО-ТО КУПИТЬ,
БУДЬ ОЧЕНЬ ОСТОРОЖЕН!

ЕСЛИ ТЫ КУПИШЬ ЧТО-ТО НА «ПОДОЗРИТЕЛЬНОМ» САЙТЕ,
ЭТО МОЖЕТ ОКАЗАТЬСЯ ЛОВУШКОЙ, И ТЫ МОЖЕШЬ ПОПАСТЬ В БЕДУ.

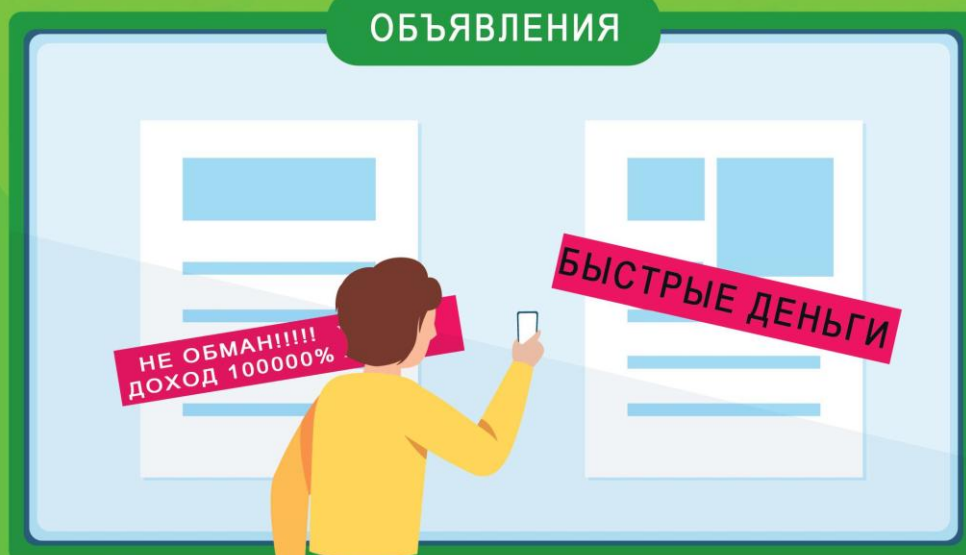
Проверяй сайты!

Будь в безопасности!

Выбирай только
проверенные места!

Используй надежные
источники информации!

ОБЪЯВЛЕНИЯ



УВД ГРОДНЕНСКОГО
ОБЛИСПОЛКОМА



MVD.GOV.BY

ПОМНИ, БЫТЬ УМНЫМ ПОКУПАТЕЛЕМ – КРУТО!
ТАК ТЫ СМОЖЕШЬ НАСЛАЖДАТЬСЯ СВОИМИ
ПОКУПКАМИ И НЕ ПЕРЕЖИВАТЬ О НЕПРИЯТНОСТЯХ.

КАРДИНГ

ДУМАЙ ПЕРЕД ТЕМ, КАК ДЕЙСТВОВАТЬ!

**БЕРЕГИ СВОИ ДАННЫЕ
И ВЫБИРАЙ ПРАВИЛЬНО!**

Не делись своими
личными данными!

Не открывай
подозрительные ссылки!

Легкие деньги
– это ловушка!



УВД Гродненского
облисполкома



MVD.GOV.BY

**ЛЕГКИЙ ЗАРАБОТОК
В ИНТЕРНЕТЕ – ЭТО ЧАСТО ОБМАН!**



УВД ГРОДНЕНСКОГО
ОБЛИСПОЛКОМА

БезОпасность



Чек-лист кибергероя



Сложный пароль



Создавайте уникальные и сложные пароли для каждого из своих аккаунтов. Используйте комбинацию букв, цифр и специальных символов, а также избегайте очевидных паролей.



Антивирус



Установите и регулярно обновляйте антивирусное программное обеспечение и брандмауэры, чтобы защитить свою систему от вирусов, троянов и других вредоносных программ.

Онлайн- покупки



Покупайте только у надежных продавцов и используйте безопасные платежные системы. Закажите отдельный счёт и банковскую карту для покупок в Интернете.



Исчезающие сообщения



Обеспечивают безопасность в мессенджере. Эффективный способ избежать попадания деликатной информации в чужие руки. Особенно важно для групповых чатов.



Подготовил JatkazhIrovichI

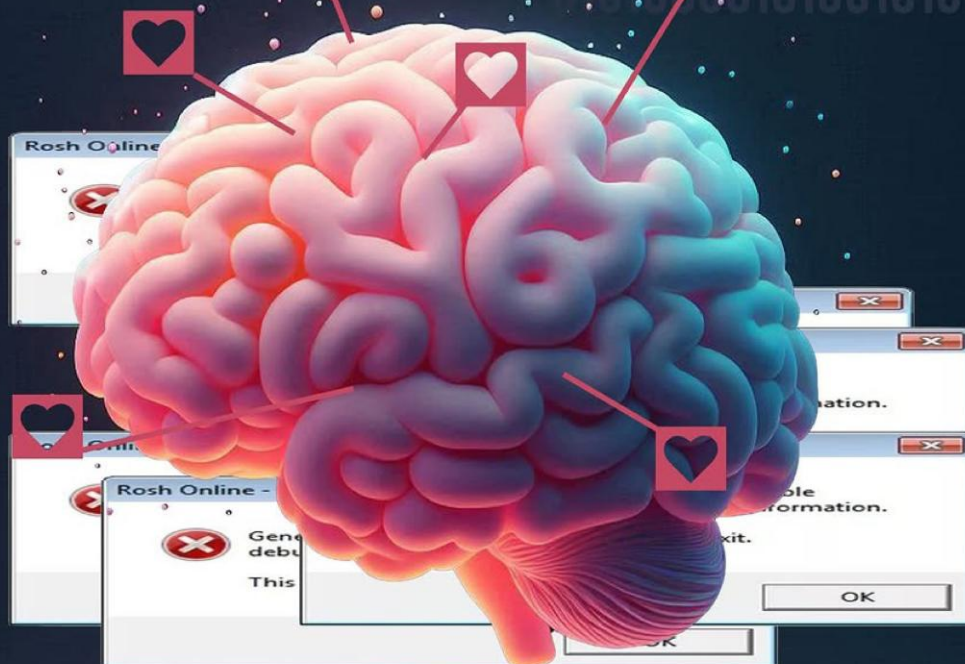


УВД ГРОДНЕНСКОГО
ОБЛИСПОЛКОМА

Интернет Все

Все что попадает в Интернет, там и остается.

ПОМНИТ



БЕЗОПАСНОСТЬ ДЕТЕЙ

- Не доверяй всему, что **ВИДИШЬ**: **СПРОСИ РОДИТЕЛЕЙ**, перед тем как кликать!
- Шутя в Интернете **ПОМНИ** о последствиях.
- Конфликт в Интернете? Взрослые знают, как помочь.
- Не секрет, а безопасность: сообщая родителям о своих покупках.
- Не рассказывай в Интернете информацию о себе и сведения о членах семьи.

Подготовил sstwsy

БЕЗОПАСНОСТЬ ДЕТЕЙ

НЕ ДОВЕРЯЙ ВСЕМУ, ЧТО ВИДИШЬ -
**СПРОСИ РОДИТЕЛЕЙ,
ПЕРЕД ТЕМ КАК КЛИКАТЬ!**



Шутя в Интернете
ПОМНИ о последствиях.

Конфликт в Интернете?
Взрослые знают, как помочь.

Не рассказывай в Интернете
информацию о себе и сведения
о членах семьи!

Не секрет, а безопасность:
сообщая родителям о своих покупках.



УВА ГРОДНЕНСКОГО
ОБЛІСПОЛКОМА



MVD.GOV.BY

**ВСЕ ЧТО ПОПАДАЕТ
В ИНТЕРНЕТ, ТАМ И ОСТАЕТСЯ!**

ВИШИНГ



СОТРУДНИКИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ НИКОГДА НЕ БУДУТ

Звонить вам в мессенджере
и спрашивать ваши
личные данные!

Просить установить
какие-то другие
приложения на телефон!

Звать вас участвовать
по телефону в программах
по ловле преступников!

Просить перевести деньги
на какие-то "безопасные
счета!"



УВД ГРОДНЕНСКОГО
ОБЛИСПОЛКОМА



MVD.GOV.BY

× × × ×

ОСТРОЖНО – МОШЕННИКИ

**ВАМ ЗВОНЯТ НЕИЗВЕСТНЫЕ, ПРЕДСТАВЛЯЮТСЯ СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ ИЛИ ФИНАНСОВЫХ ОРГАНОВ И ПРОСЯТ ПЕРЕВЕСТИ ДЕНЬГИ НА “БЕЗОПАСНЫЙ СЧЕТ” ИЛИ ПЕРЕДАТЬ ИХ КУРЬЕРУ ДЛЯ “ДЕКЛАРИРОВАНИЯ” – НЕ ВЕРЬТЕ!
ВАС ПЫТАЮТСЯ ОБМАНУТЬ!**

НЕ ПЕРЕДАВАЙТЕ СВОИ ЛИЧНЫЕ ДАННЫЕ НЕИЗВЕСТНЫМ!

**ПОГОВОРИТЕ СО СВОИМИ РОДНЫМИ
РАНЬШЕ, ЧЕМ ЭТО СДЕЛАЮТ МОШЕННИКИ**

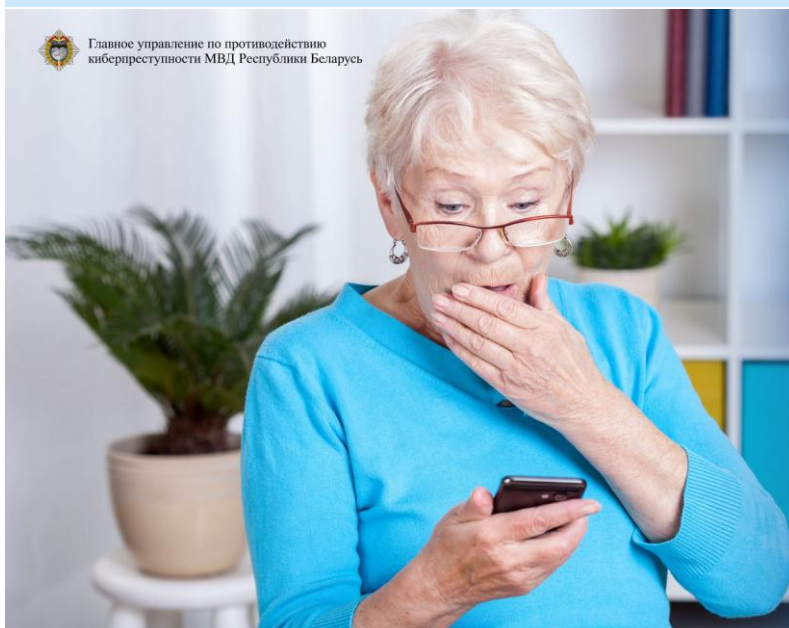
ПОМНИТЕ! СОТРУДНИКИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ НИКОГДА НЕ ЗВОНЯТ ЧЕРЕЗ МЕССЕНДЖЕРЫ И НЕ ТРЕБУЮТ ОТ ГРАЖДАН ПРОВОДИТЬ ОПЕРАЦИИ, СВЯЗАННЫЕ С ДВИЖЕНИЕМ ДЕНЕЖНЫХ СРЕДСТВ!



ЛЕНИНСКИЙ РОВД Г. ГРОДНО



Главное управление по противодействию
киберпреступности МВД Республики Беларусь



**НАУЧИТЕ
РОДИТЕЛЕЙ
ФИНАНСОВОЙ
ГРАМОТНОСТИ**

**ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ**

**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ**

**НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ**

10 правил безопасности в Интернете

Опасайся незнакомцев в Интернете.

Не все, что ты читаешь или видишь в Интернете, правда, задавай вопросы родителям, уточняй.

Не делись своими личными данными и данными членов семьи (полное настоящее имя, адрес, район проживания, номер телефона, фото паспорта и прочие данные) в Интернете.

Ни в коем случае не встречайся с людьми, знакомство с которыми состоялось в Интернете, так как эти люди могут оказаться совсем не теми, за кого себя выдают.

Играя в онлайн игры, соблюдай осторожность, не указывай реальные данные в профиле.

Соблюдай правила хорошего тона в Интернете, они ничем не отличаются от тех, которые действуют в реальном мире.

Не заходи на незнакомые сайты, не переходи по ссылкам, полученным в мессенджерах.

Не делай в Интернете того, что не сделал бы в реальной жизни.

Обязательно рассказывай взрослым о проблемах или подозрительных действиях в Интернете – они всегда помогут.

Помни: всё, что попадает в Интернет, там и остаётся (даже если было удалено).

РАСПИСАНИЕ ЗАНЯТИЙ

Понедельник

Вторник

Среда

Четверг

Пятница



«Управление К»
Министерства внутренних дел Республики Беларусь

MTE
Мультимедийный Информационный
www.mte-cyber.by



ТЕЛЕФОННЫЕ МОШЕННИКИ

МОГУТ ПРЕДСТАВИТЬСЯ
РАБОТНИКАМИ БАНКА или
ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

- НЕ** сообщайте данные карты и коды из СМС
- НЕ** оформляйте кредиты по просьбе третьих лиц
- НЕ** устанавливайте программы по просьбе третьих лиц
- НЕ** переводите деньги на «защищенный счет»
- НЕ** переходите по ссылкам от незнакомцев



Больше информации
на сайте
<https://mvd.gov.by>

ПЕРЕЗВОНИТЕ В БАНК!

- ☒ если убеждают установить программу на ваше устройство
- ☒ если просят назвать данные для отмены якобы оформленной доверенности на операции по вашему вкладу
- ☒ если предлагают отменить расходную операцию, которую вы не совершали
- ☒ если убеждают оформить кредит и перевести деньги на «защищенный» счет
- ☒ если вам одобрен кредит, который вы не оформляли

ПЕРЕЗВОНИТЕ В МИЛИЦИЮ!

- ☒ если просят поучаствовать в «разоблачении недобросовестного сотрудника банка»

УСТАНОВИТЕ В VIBER
ЗАЩИТУ ОТ ЛИШНИХ ЗВОНКОВ



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь



ПОЛЬЗУЙСЯ БЕЗОПАСНО

«банк».by



Пользуйтесь мобильными приложениями банка



Переходите в интернет-банкинг только с официального сайта банка



Проверяйте адрес интернет-банкинга в адресной строке, между последней точкой и первой наклонной чертой должно быть только так .by/



Активируйте на карте, используемой для онлайн-платежей, услугу 3-D Secure (подтверждение платежей SMS-кодом)



Не переходите в интернет-банкинг по ссылкам в поисковых системах



Не используйте SMS-коды от банка и код с обратной стороны карты для получения денежных средств



Не переходите по ссылкам из сообщений для доступа к интернет-банкингу и иным сервисам или услугам



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь



Больше информации
на сайте
<https://mvd.gov.by>

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!

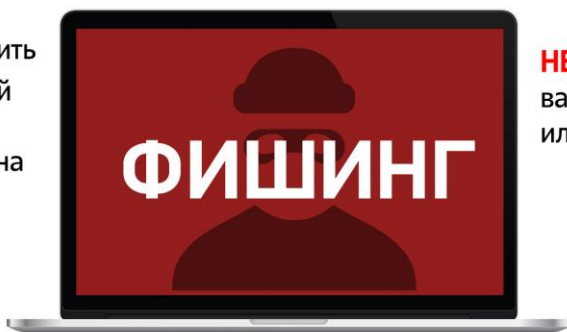
МОШЕННИКИ В ИНТЕРНЕТЕ



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 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! **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

БЕЗОПАСНЫЙ ИНТЕРНЕТ 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 важное о твоей жизни
- НЕ встречайся с людьми, с которыми знакомишься только в интернете**
За маской онлайн-общения 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 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 твоим родственником
- 3** он говорит, что сын/дочь/мама или из-за него попал в ДТП
- 4** он просит денег как компенсацию вреда или чтобы оплатить авто
- 5** затем звонит, благодарит и просит передать привет
- 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

ВАМ ЗВОНЯТ ПО ТЕЛЕФОНУ И СООБЩАЮТ



ВАЖНО!

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 НАВЕРНЯКА 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

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.

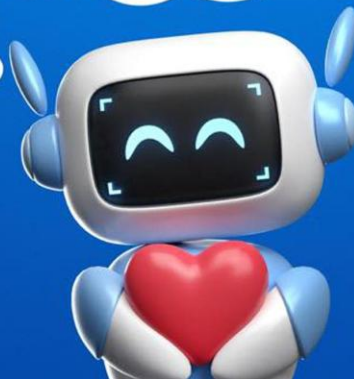


Будь осторожен, как на
минном поле!
Скачивай приложения только
из официальных магазинов.
Антивирус - твой верный
друг!



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



ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:



Получить кредит, чтобы отменить якобы оформленный неизвестными на ваше имя другой кредит и перевести деньги на специальный счет

Установить программное обеспечение, якобы для предотвращения мошеннической атаки на ваш счет

Перевести накопления на якобы безопасный счет, чтобы не изъяли при обыске

Передать личные данные и код из СМС, такие сведения предоставляют мошенникам доступ к счету или сервису

ОСТОРОЖНО! МОШЕННИЧЕСТВО!

В СОЦИАЛЬНЫХ СЕТЯХ И НА ТОРГОВЫХ ПЛОЩАДКАХ:

Перевести предоплату за несуществующий товар в лжемагазине или по измененным реквизитам банка

Перейти по поддельной ссылке банковской системы и ввести личные данные (логин и пароль, номер и трехзначный код с оборотной стороны банковской карты, код из СМС, кодовое слово)

Перечислить деньги на карту или оплатить родственнику, другу, любящему человеку

На поддельной бирже вложить деньги в проект, якобы для получения пассивного дохода

МОШЕННИКИ УБЕЖДАЮТ, представляясь продавцами, друзьями, партнерами по бизнесу, руководителями инвестиционных проектов



Больше информации
на сайте
<https://mvd.gov.by>



Главное управление
по противодействию киберпреступности
КМ МВД Республики Беларусь

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



! 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



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 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 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