

# Профилактическая акция «Неделя кибербезопасности» с 9 по 15 сентября 2024 года

## «Как я могу пользоваться интернетом?»

### Что такое интернет

Интернет – это огромная сеть компьютеров, которые соединены между собой с помощью специальных устройств. Благодаря интернету люди из разных стран могут общаться друг с другом, делиться своими фотографиями, делать покупки, смотреть видео, учиться и даже работать удаленно. Для того, чтобы безопасно пользоваться интернетом, надо знать некоторые правила.

**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**

## Правила пользования интернетом

Общение в сети с друзьями и родственниками может быть классным и захватывающим, но, к сожалению, ты можешь встретиться и с трудностями. Чтобы не навредить себе и пользоваться интернетом безопасно, помни два основных правила:

**Правило ПРИВАТНОСТИ.** Знай, что твоя персональная информация может стать доступной для любого человека в любой точке мира. Она может быть использована не только твоими друзьями или членами семьи, но и незнакомцами.

**Правило ПОСТОЯНСТВА.** Если ты что-то размещаешь в интернете, то это может остаться там на очень долгое время. Даже сообщения и фотографии, которые ты удаляешь, сохраняются на специальных серверах.

# 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**

## Пусть личная информация останется личной

Информация, такая как полное имя, домашний адрес, название школы и т.д. является личной. Не доверяй ее другим пользователям социальных сетей.

### Храни логин и пароль при себе

Имя пользователя (логин) и пароль - это важная личная информация! Если твои данные попадут "не в те руки" ты можешь попасть в неприятную ситуацию.

Поделись информацией о логине и пароле только с родителями. Договорись, в каких ситуациях они могут использовать эту информацию (непредвиденные ситуации).

Твой пароль не должен быть слишком легким, не стоит выбирать паролем свое имя или год рождения, пусть это будет чем-то близким тебе, но не известным посторонним.

**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!**

научись пользоваться интернетом правильно!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный  
единый  
номер **102**

The infographic features a blue background with pink and red circular accents. It includes an illustration of three children sitting on a laptop screen, and a shield icon on the laptop display. A vertical banner on the left side contains the text 'научись пользоваться интернетом правильно!'.

## **Сделай свой профиль закрытым**

Сделай свой профиль видимым только для тебя и твоих друзей. Если твой профиль в социальных сетях будет закрытым, злоумышленнику будет сложнее получить доступ к вашим данным. Видимость можно изменить в настройках.

### **Мы несем ответственность за то, что размещаем в сети**

Информация, которую ты размещаешь, не должна смущать ни тебя, ни других.

Помни! Любое проявление жестокости, насилия в интернете недопустимо!

Относись уважительно к информации других пользователей.

Общаясь в социальных сетях, не стоит заниматься рассылкой сообщений незнакомым людям.

Перед тем, как добавлять кого-то в группы, спрашивай, хотят ли они этого.

Сначала подумай, потом подтверждай отметки на фото.

Всегда просматривай записи и фото, на которых тебя отметили. Активируй опцию одобрения публикаций с отметками. Так, ты сможешь избежать неловких ситуаций с неудачными фото, неприятными шутками и рассылками.

Если тебя беспокоит снимок, на котором есть ты, но нет отметки, поговори с человеком, который разместил фото, и попроси его удалить публикацию.

Всегда спрашивай разрешения, если хочешь разместить у себя чужие фотографии. Это проявление уважения к человеку и главный способ избежать нежелательных конфликтов.

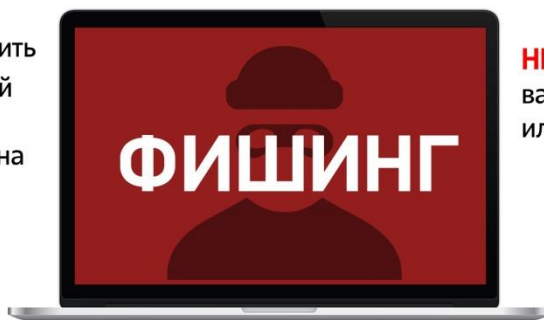
# ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ



**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**

## Несколько советов как себя защитить

Информация в интернете не всегда является достоверной и надежной, а иногда даже специально создается для кражи личной информации.

Например, Ты получаешь письмо: "Здравствуйтесь, отправляю вам фото". Во вложении, судя по картинкам, действительно фото.

Что случится, если ты кликнешь на картинку? Перед тобой откроется новая страничка, словно страничка с твоей почтой перезагрузилась.

Ты вводишь свои данные, чтобы вернуться в почту и автоматически отдаешь свою личную информацию злоумышленникам. Это называется **фишинг** – кража личной информации.

Всегда проверяй, с какого адреса пришло письмо. Если адрес кажется странным, и ты сомневаешься, стоит проверить адрес в интернете.

Внимание на «обезличенные» письма. Письма без личных обращений и личной информации подозрительны.

Осторожно с просьбами о немедленных решениях. Фишинговые письма любят пугать, заставляя немедленно совершать нас что-то делать. Злоумышленник не хочет, чтобы у нас было время подумать.

Внимание на адресную строку. Сайты мошенники содержат дополнительные символы, ошибки, цифры.

# ВНИМАНИЕ!

## БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

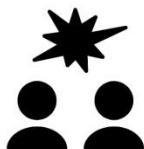


**Размещать** персональную и контактную информацию о себе в открытом доступе



**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**

## Что такое персональные данные и как с ними обращаться

Персональные данные – это любая информация, которая относится к тебе: имя, фамилия; дата рождения; номер школы; номер телефона; твой адрес и другая личная информация.

Персональные данные в интернете нужны для того, чтобы зарегистрироваться на сайте или в социальных сетях, для того чтобы делать покупки или играть в игры. Но, есть данные, которыми мы можем делиться случайно! Задумайся! Это тоже персональные данные, их нужно хранить от незнакомых людей: место нахождения; места учебы; пароли; данные банковских карт родителей; спортивные секции, или другие группы, в которых ты участвуешь.

# 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**

## Правила безопасности

**Всегда проверяй надежность сайта перед регистрацией.  
Обрати внимание на тревожные звоночки:**

- *Ошибки в названии сайта;*
- *В адресе сайта содержится много цифр и случайных символов;*
- *На сайте открывается множество дополнительных окон.*

## Оберегай свой компьютер

- *Для защиты своего компьютера необходимо регулярное обновление программного обеспечения, использование надежных антивирусных и антишпионских программ.*
- *Устанавливай такие программы только с официальных сайтов*
- *Постоянно обновляй антивирусные программы*
- *Познакомь с этими программами своих родителей, чтобы они помогли защитить твой компьютер*

# 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**



## **Будь внимателен, переходя по ссылкам**

- *Критически относись к сообщениям, которые прислали незнакомцы, к яркой рекламе, всплывающей на разных сайтах. Ты никогда не угадаешь, что на самом деле тебя там ждёт (вирусы, вредоносная и неприятная информация)*
- *Попадая случайным образом на такие странички следует немедленно их закрыть, ничего не загружать.*

### **Такие ссылки можно узнать по некоторым признакам:**

- Очень яркие баннеры;
- Сложные, непонятные адреса;
- Ошибки в названии;
- Нереалистичные обещания;
- Обещания бесплатной награды за переход по ссылке или скачивание;
- Необходимость отправлять СМС для скачивания.

### **Прояви осторожность в подключении к общественным сетям Wi-Fi:**

*Бесплатные и общественные сети часто бывают незащищенными, в них нет возможности ограничить себя от вредоносных программ и действий злоумышленников.*

*Подключайся к такой сети только в случае крайней необходимости.*

*Контролируй вход и выход из своих аккаунтов.*

*Всегда выходи из системы после завершения работы. Особенно если ты пользовался компьютером вне дома.*

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**

## Как безопасно скачать из интернета

Если ты хочешь скачать что-то в интернете – следуй этим простым правилам:

В первую очередь ты должен спросить разрешения у родителей или других взрослых.

Никогда не пиши в интернете свой номер телефона, настоящие имя и фамилию. Даже если такую информацию запрашивают для скачивания музыки или игры. Такой сайт, скорее всего, принадлежит обманщикам, которые хотят использовать твои персональные данные в корыстных целях. Например, хотят списать деньги с твоего баланса.

Никогда не вводи данные своих или чужих банковских карт. Чужими картами пользоваться незаконно, у тебя могут быть проблемы.

Прежде чем что-то скачать, удостоверься, что это надежный ресурс. Лучше всего скачивать игры с официальных источников (например, с App store, Google store).

На твоём компьютере должен быть установлен антивирус. В играх могут содержаться вирусы, которые испортят твой компьютер или планшет. Могут встретиться вирусы, которые похищают персональные данные.

## Можно ли размещать свою фотографию в интернете

Ты можешь размещать свои фотографии в интернете, но при этом надо помнить про свою безопасность.

### Несколько советов для тебя:

**Прежде всего**, попроси разрешения родителей или других взрослых.

**Перед тем**, как разместить фото, ответь себе на три вопроса:

*«Смущает ли это фото меня?»*

*«Может ли это фото смутить других?»*

*«Зачем я размещаю это фото?»*

**НИКОГДА** никому не отправляй свое фото или видео, на которых ты без одежды, или на которых видны интимные части твоего тела.

## **Можно ли размещать чужие фотографии в интернете?**

Прежде, чем размещать фотографии с другими людьми подумай, стоит ли это делать, даже, если на них есть что-то интересное или забавное.

### **Несколько советов для тебя:**

Всегда спрашивай разрешения у участников фото

Спрашивать разрешения нужно даже если ты пересылаешь фото в сообщениях.

Прежде чем разместить что-то, подумай, ты действительно хочешь, чтобы это увидели другие люди?

Никогда не пересылай фото или видео, на которых другие люди без одежды или на которых видны интимные части их тела.

Ты должен знать, что размещение изображений с насилием или обнаженными людьми, незаконно, и тебя могут привлечь к ответственности.

Помни, то, что ушло в Интернет, не вернется обратно!

## **Как делать безопасные покупки в интернете?**

Покупать в интернете очень удобно и иногда даже дешевле, чем в обычных магазинах. Но помни, что именно онлайн-покупками часто пользуются мошенники, чтобы украсть твои деньги.

### **Несколько советов для тебя:**

В первую очередь спроси разрешения родителей или других взрослых.

Если ты хочешь купить в онлайн магазине какую-то вещь, лучше всего выбирай оплату по факту получения товара. Так ты обезопасишь себя от обмана.

Никогда не вводи данные своих или чужих банковских карт. Чужими картами пользоваться незаконно, у тебя могут быть проблемы.

Если ты хочешь купить что-то у игрока в онлайн игре, не используй приложения для взлома покупок. **Модифицированные арк файлы** могут содержать вирус. Кроме того, это незаконно и у тебя могут быть проблемы.

Прежде чем купить что-то в интернете, ознакомься с характеристиками продавца. Посмотри, есть ли отзывы о нем. Почитай, что пишут другие покупатели, все ли получили свои заказы вовремя.

### **В интернете могут обмануть**

Обман в социальных сетях – очень распространенное явление. Общаясь в интернете следует помнить, что твои собеседники могут оказаться не теми, за кого они себя выдают. Нехорошие люди пишут под чужими профилями, взламывают аккаунты, создают поддельные страницы.

Если ты понимаешь, что собеседник не тот, за кого он себя выдает, обратись в службу технической поддержки, чтобы они заблокировали этот аккаунт. Сообщи другу, если понимаешь, что его страница взломана.

### **КАК РАСПОЗНАТЬ ЗЛОУМЫШЛЕННИКА?**

**Напрашивается** к тебе в «друзья», несмотря на то, что вы не знакомы в реальной жизни;

Есть основания думать, что это **взрослый человек**;

В социальной сети у него **мало друзей или их нет вовсе**;

У него **очень много друзей, но активности на странице нет**;

Он **настойчиво просит тебя о чём-то**, даже, на первый взгляд, безобидном: отправить своё фото, рассказать о чём-то, встретиться;

Просит сохранить твоё с ним **общение в секрете**;

Пытается **внушить тебе**, что кроме него, тебя никто не поймет или часто пишет что:

*«Я хочу знать о тебе всё»;*

*Слишком «идеальный» диалог;*

*«Слабо?»;*

*«Это наш с тобой секрет»;*

*«Ты уже взрослый/взрослая»;*

*«Нет времени объяснять...»;*

*«Если ты не согласишься, то я...ой, да я же шучу...».*

## **Если тебе не нравится то, что тебе пишут, есть пути решения**

### **Я МОГУ!!!:**

Заблокировать;

Закрывать доступ;

Сказать "НЕТ";

Рассказать родителям, педагогам;

Написать модераторам;

Игнорировать!

### **Что делать, если попался в ловушку?**

**СПОКОЙСТВИЕ!** Даже если с тобой случилась неприятность в сети ты можешь довериться взрослым ядом с тобой, они помогут тебе справиться! Злоумышленники тренируются в обмане, любой может стать их жертвой.

**ГОВОРИМ РОДИТЕЛЯМ!** Так они смогут тебе помочь.

Не поддавайся на манипуляции обманщиков в сети, их задача – не дать тебе подключить взрослых, поэтому они могут угрожать, шантажировать, брать тебя «на слабо».

**МЕНЯЕМ ВСЕ ПАРОЛИ!** Для того, чтобы обезопасить свою личную информацию, сделай это как можно скорее. Это поможет тебе ограничить влияние обманщика из интернета.

**ПРЕДУПРЕЖДАЕМ ДРУЗЕЙ В ИНТЕРНЕТЕ!** Для того, чтобы не попасть в неловкую ситуацию и не дать злоумышленникам использовать твои данные для обмана других сообщи всем, с кем общаешься, что твои данные украдены, говорить какие именно не стоит.

**СООБЩИТЬ МОДЕРАТОРАМ РЕСУРСА!** Это даст тебе дополнительную поддержку и поможет не допустить нового обмана.

### **Хочешь лайков и известности в социальных сетях?**

Когда листаешь Инстаграмм или VK, кажется, достигнуть славы известных блогеров так легко. Но лайки не сыпятся и репостить тебя никто не собираются. Что же делать? Может быть, попробовать легкие пути?

В сети часто встречаются сообщения об услугах по накрутке лайков и голосов, об увеличении числа подписчиков и комментариев. Всего-то надо перечислить деньги или отправить смс и удача у тебя в кармане. Можно доверять таким сообщениям? Нет! Потому что это обман. Все социальные сети выступают против накрутки и блокируют за такие действия.

А мошенник, получив деньги, исчезнет. Программы и аккаунты, которые предлагают такие услуги, часто похищают пароли и другие персональные данные (ссылка), а потом требуют за них выкуп. Поэтому в погоне за славой ты рискуешь многое потерять.

### **ВАЖНО!**

**Если тебя смущает ситуация, происходящая с тобой в сети:**

Расскажи родителям или другим взрослым, которым доверяешь!

Обратись за помощью в службу поддержки на сайте

Всегда можно обратиться за помощью по телефону  
8-801-100-16-11      **ДЕТСКАЯ ТЕЛЕФОННАЯ ЛИНИЯ**  
(КРУГЛОСУТОЧНО, БЕСПЛАТНО, АНОНИМНО)