

СОВЕРШЕНИЕ НЕСОВЕРШЕННОЛЕТНИМИ
КИБЕРПРЕСТУПЛЕНИЙ ПРЕДУСМОТРЕННЫХ СТ.222 УК РБ

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

**РОДИТЕЛИ!
научите детей
пользоваться
интернетом
правильно!**

**ГЛАВНЫЕ
ПРАВИЛА
ЦИФРОВОЙ
ГИГИЕНЫ**



**НЕ встречайся с людьми,
с которыми знаком только
в интернете**

За маской онлайн-собеседника
может скрываться злоумышленник



**НЕ сообщай в интернете
свой реальный
адрес и телефон**

Злоумышленник может встретить
тебя с недобрыми намерениями



**НЕ отправляй личные данные
для участия в конкурсах
на малоизвестных сайтах**

Информацией могут завладеть и
воспользоваться недоброжелатели



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

не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер **102**

Все чаще в социальных сетях и мессенджерах пользователям стали приходить сообщения с предложениями без особых усилий заработать до 100 долларов за день. Что для этого нужно? Всего ничего, оформить на себя банковскую карту в банке, на который укажет мнимый работодатель, и передать сообщением в сети Интернет полученные реквизиты карты потенциальному работодателю.

Человек, согласившийся на такие условия сделки, становится так называемым «дропом» (подставное лицо, используемое кибермошенниками в серых схемах). «Дроп» – человек, который соглашается, чтобы его банковская карта стала «транзитной» для денежных средств, украденных мошенниками. «Дроп» переводит полученные незаконным путем денежные средства с одного счета на другой. Такая цепочка переводов нужна для того, чтобы запутать следы киберпреступников и усложнить работу милиции.

«Дропы» бывают «разводные» и «неразводные». Отличие их только в том, что «неразводные» осознают всю тяжесть совершаемых ими деяний и умышленно занимаются этим. В большинстве своем это студенты и школьники, испытывающие нужду в финансах. «Разводные дропы» не знают, что идут на преступление, думают, что они действительно работают, получая заработную плату и т.д.

Так, несовершеннолетние в социальных сетях под предлогом заработка 5-20 рублей НБ Республики Беларусь, сообщают свои аутентификационные данные, с помощью которых на их имена мошенниками создаются электронные-кошельки, через которые переводятся похищенные денежные средства.

В каких схемах могут участвовать подростки?

- Обналичивание денег в банкоматах: действия – принять деньги, снять деньги, взять себе процент, остальное переслать заказчику. Вот по такой нехитрой схеме и работают дропы.

- Банковский перевод: предоставь мнимому работодателю свои реквизиты банковской карты, подождать когда на нее зачислят украденные деньги, переслать деньги на счет который укажет заказчик, оставить себе процент на банковской карте.

- Пересылка товара: действия такие: дать свой адрес, принять посылку, переслать посылку на нужный адрес отдать в руки (и такие есть), получить вознаграждение. Главное – наличие паспорта и прописки.

Дропы могут понадобиться и для других дел. Например, покупка симкарт с помощью которых в дальнейшем совершаются преступления.

Ответственность за такие действия наступает по **статье 222 Уголовного Кодекса Республики Беларусь** (незаконный оборот средств платежа и (или) инструментов) с 16 летнего возраста.

1. Изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных

данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, – наказываются штрафом или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от двух до шести лет.

2. Те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере, – наказываются ограничением свободы на срок от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.

Рекомендации по профилактике киберпреступлений среди несовершеннолетних.

Первое и самое главное правило: установите с ребёнком доверительные отношения и положительный эмоциональный контакт в вопросе использования сети Интернет.

Расскажите ребенку об ответственности, которая может наступить за совершение им киберпреступлений, а также о возрасте, с которого наступает уголовная ответственность за данные деяния.

Разъясните подростку, что есть и другие не менее негативные последствия совершения ими преступлений или правонарушений. Привлечение к административной или уголовной ответственности является основанием для постановки несовершеннолетнего на учет в Инспекцию по делам несовершеннолетних, занесения информации в общереспубликанскую единую государственную базу данных о правонарушениях, которая содержится там на протяжении всей жизни, что впоследствии может послужить препятствием для получения визы, поступления в специализированный ВУЗ (Академия МВД, Военная академия), прохождения службы в правоохранительных органах, занятия высших должностей и т.п.

Рекомендации для безопасного использования Интернета.

Для детей от 10 до 13 лет.

- создайте ребенку на компьютере собственную учетную запись с ограниченными правами;
- используйте средства фильтрации нежелательного контента;
- приучайте ребенка спрашивать разрешение при скачивании файлов из Интернета;
- поощряйте желание детей сообщать Вам о том, что их тревожит или смущает в Интернете;
- расскажите об ответственности за недостойное поведение в сети Интернет.

На данном этапе могут активно использоваться программные средства родительского контроля, к которым можно отнести следующие инструменты:

- услуга родительского контроля провайдера, оказывающего услугу доступа в сеть Интернет, позволяющая ограничить доступ к Интернет сайтам, содержащим нежелательный контент;

- функции родительского контроля, встроенные в операционную систему (ограничение времени работы компьютера, ограничение запуска программ, в том числе игр);

- функции родительского контроля, встроенные в некоторые антивирусы (например KasperskyInternetSecurity, NortonInternetSecurity), позволяющие контролировать запуск различных программ, использование Интернета (ограничение по времени), посещение веб-сайтов в зависимости от их содержания, пересылку персональных данных;

- специализированное программное обеспечение, предназначенное для выполнения функций родительского контроля, например, КиберМама, KidsControl, TimeBoss и другие.

Подростки в возрасте 14-17 лет.

- интересуйтесь, какими сайтами и программами пользуются Ваши дети;

- настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета;

- напоминайте о необходимости обеспечения конфиденциальности личной информации;

- предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности.

В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей рекомендуем родителям не умалчивать данные факты, а сообщать о них в зависимости от ситуации классному руководителю, педагогу социальному учреждения образования, в правоохранительные органы по месту жительства.

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

