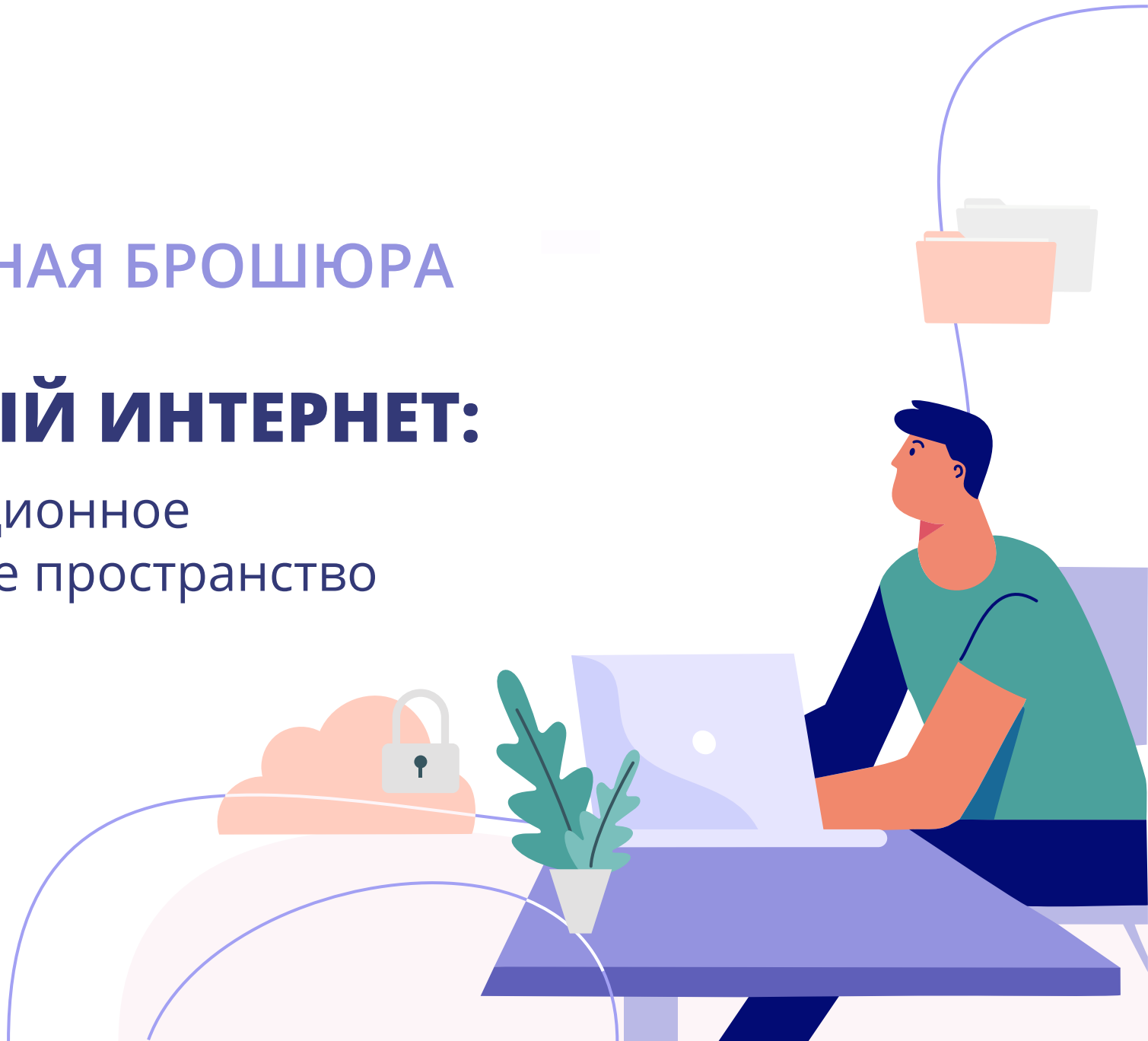
МЕГА ТАЛАНТ

от проекта mega-talant.com

ИНТЕРАКТИВНАЯ БРОШЮРА

БЕЗОПАСНЫЙ ИНТЕРНЕТ:

создаём дистанционное образовательное пространство



СОДЕРЖАНИЕ:

01

ИНТЕРНЕТ-УГРОЗЫ: КАК ЗАЩИТИТЬСЯ

Современное образование, как и мир в целом, трудно представить без различных гаджетов, соцсетей и общения на расстоянии.
А в условиях пандемии и самоизоляции дистанционное обучение и коммуникация – это уже необходимость.

Интернет, безусловно, дает нам доступ к огромному количеству информации и позволяет оставаться на связи в любое время суток.

Однако на просторах виртуального мира кроется множество опасностей, с которыми может столкнуться каждый из нас.
Давайте попробуем разобраться, что это за опасности, и как их можно избежать.

Спам

СПАМ

ЧТО НУЖНО ПРЕДПРИНЯТЬ, ЧТОБЫ ЗАЩИТИТЬСЯ ОТ СПАМА

Каждый пользователь хоть раз в жизни сталкивался с надоедливой рекламой, которая выскакивает на странице, или приходит на почту в виде письма. Эта бомбардировка рекламной корреспонденцией получила название «спам».

И хоть эти письма не всегда содержат ценную информацию, они вовсе не безвредны.

Иногда спам может оказаться интернет-вирусом, который попадает в компьютер, как только любопытный пользователь открывает злополучное письмо.

1. НЕ УКАЗЫВАТЬ СВОЙ ЭЛЕКТРОННЫЙ АДРЕС НА ПОДОЗРИТЕЛЬНЫХ САЙТАХ И ВЕБ-СТРАНИЦАХ
2. ОТПРАВЛЯТЬ НЕЖЕЛАТЕЛЬНЫЕ ПИСЬМА С ЭЛЕКТРОННОЙ ПОЧТЫ В РАЗДЕЛ «ЭТО СПАМ»
3. НЕ ПОДПИСЫВАТЬСЯ НА ИНТЕРНЕТ-РАССЫЛКИ
4. В СОЦИАЛЬНЫХ СЕТЯХ ОТМЕЧАТЬ СООБЩЕНИЯ РЕКЛАМНОГО, ПОРНОГРАФИЧЕСКОГО ИЛИ ОСКОРБИТЕЛЬНОГО ХАРАКТЕРА ОТМЕТКОЙ «ЭТО СПАМ»

Овершеринг

ОВЕРШЕРИНГ

ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СЕБЯ ОТ КИБЕРМОШЕННИКОВ

Современные пользователи уже привыкли к тому, что в Интернете можно получить любую информацию. Возраст, дата рождения, номер телефона и даже адрес – всё это легко найти и отследить, если в этом есть необходимость.

Многие интернет-пользователи беспокоятся о своей приватности и всячески защищают персональную информацию. Однако есть и те, кого не сильно заботит чрезмерная открытость в сети. Люди спешат поделиться новостями о дорогих покупках, корпоративных праздниках и путешествиях, и тем самым привлекают кибермошенников.

Более того, чрезмерная открытость в социальных сетях часто становится причиной агрессии среди подростков и приводит к онлайн-травле, или кибербуллингу.

1. ДОБАВЛЯТЬ «В ДРУЗЬЯ» ТОЛЬКО ЗНАКОМЫХ ЛЮДЕЙ
2. БЛОКИРОВАТЬ ПОДОЗРИТЕЛЬНЫЕ И НЕПРОВЕРЕННЫЕ АККАУНТЫ
3. ПУБЛИКОВАТЬ ТОЛЬКО ОБЩУЮ ИНФОРМАЦИЮ О СЕБЕ И НЕ РАСПРОСТРАНЯТЬ В СЕТИ ФОТО, ВИДЕО О СВОЕЙ ЖИЗНИ
4. ИЗБЕГАТЬ ОБЩЕНИЯ С НЕИЗВЕСТНЫМИ ПОЛЬЗОВАТЕЛЯМИ
5. ПРОВОДИТЬ БОЛЬШЕ ВРЕМЕНИ «ОФФЛАЙН»

Вирусы

ВИРУСЫ

В ИНТЕРНЕТЕ ЭТИХ «ПАРАЗИТОВ» ПРУД-ПРУДИ И НУЖНО ЗНАТЬ, КАК ЗАЩИТИТЬСЯ ОТ НИХ

Сегодня даже самый неопытный пользователь знает, что такое компьютерный вирус.

Эти вредоносные программы проникают в компьютер и нарушают его работу, удаляя и форматируя различные файлы.

Они активно потребляют ресурсы компьютера, а также провоцируют ошибки, которые приводят к системным сбоям, тем самым значительно усложняя жизнь многим пользователям.

1. ОБЯЗАТЕЛЬНО УСТАНОВИТЬ АНТИВИРУСНУЮ ПРОГРАММУ. НЕ СКАЧИВАТЬ И НЕ ОТКРЫВАТЬ НЕИЗВЕСТНЫЕ ФАЙЛЫ
2. РЕГУЛЯРНО ПРОВЕРЯТЬ СВОЙ КОМПЬЮТЕР НА НАЛИЧИЕ ВИРУСОВ С ПОМОЩЬЮ РАЗЛИЧНЫХ ФИЛЬТРАЦИОННЫХ ПРОГРАММ
3. В СЛУЧАЕ БЛОКИРОВКИ КОМПЬЮТЕРА ВИРУСОМ – ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ К ОПЫТНОМУ СПЕЦИАЛИСТУ
4. СКАЧИВАТЬ НЕОБХОДИМУЮ ИНФОРМАЦИЮ ИЗ ТЕХ ИСТОЧНИКОВ, КОТОРЫЕ НЕ ЗАПРАШИВАЮТ ОТПРАВКИ СМС ИЛИ ПЕРЕХОДА ПО НЕЗНАКОМОЙ ССЫЛКЕ
5. ПУСТАНАВЛИВАТЬ ВСЕ ПРОГРАММЫ ВРУЧНУЮ, ВЫБИРАЯ ТОЛЬКО ТЕ «ГАЛОЧКИ», КОТОРЫЕ ДЕЙСТВИТЕЛЬНО НЕОБХОДИМЫ

Взлом аккаунтов

ВЗЛОМ АККАУНТОВ

КАК ЗАЩИТИТЬ СВОЙ АККАУНТ ОТ ВЗЛОМА

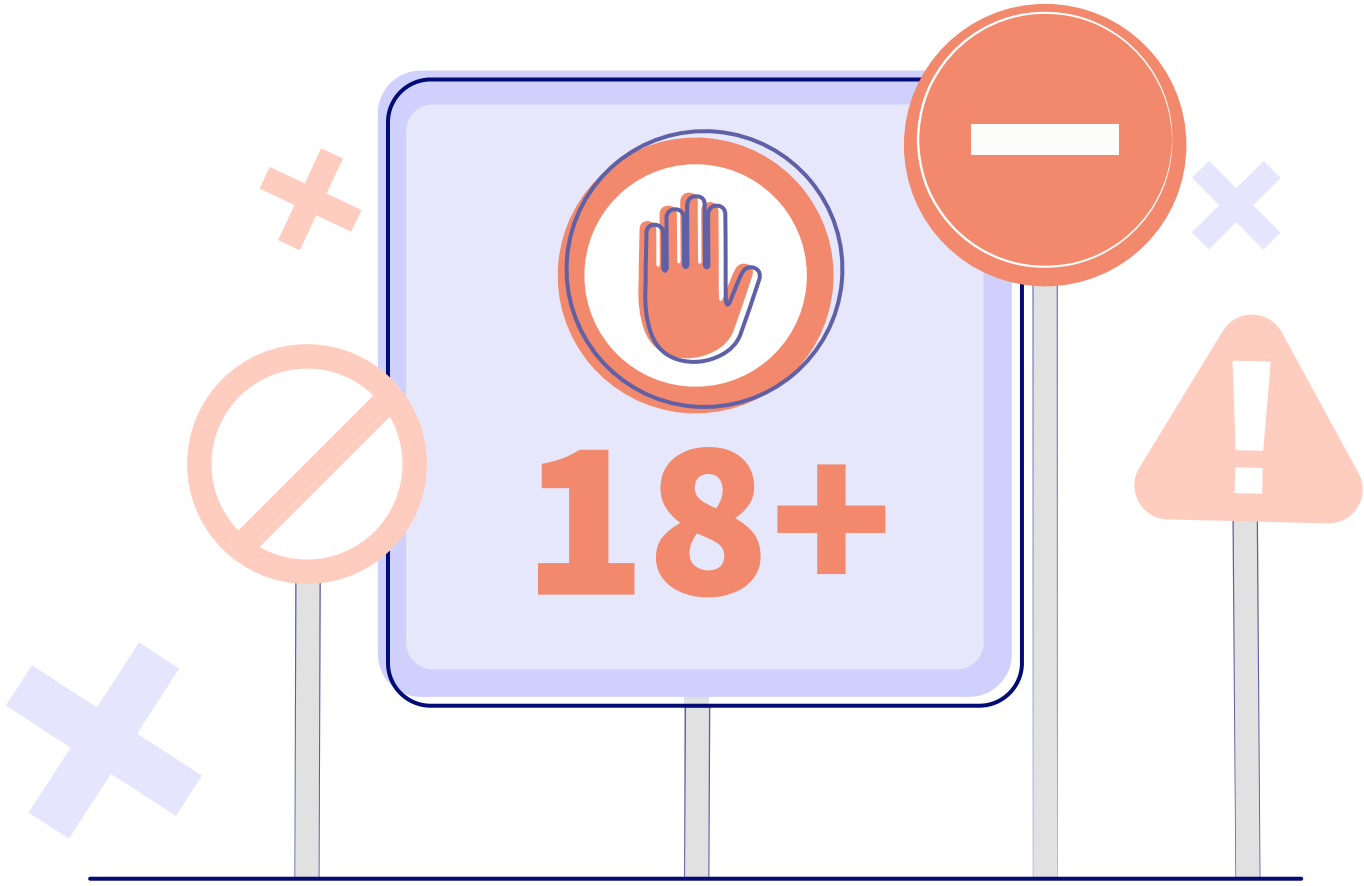
В Интернете можно найти тысячи сообщений и жалоб от пользователей, у которых взломали аккаунт. Сегодня это хоть и незаконный, но весьма прибыльный бизнес, поэтому множество злоумышленников спешат на нём заработать.

Иногда аккаунты взламывают на заказ с целью шантажа или получения информации. Ведь в переписках пользователей хранится столько ценных сведений и материалов!

Однако чаще всего взломанные аккаунты используют для перепродажи, спам-рассылок и вымогательства.

1. ПРИДУМЫВАТЬ СЛОЖНЫЕ ПАРОЛИ, СОСТОЯЩИЕ ИЗ ЦИФРОВЫХ И БУКВЕННЫХ СИМВОЛОВ
2. НЕ СООБЩАТЬ СВОЙ ПАРОЛЬ ПОСТОРОННИМ ЛИЧНОСТЯМ
3. ПЕРИОДИЧЕСКИ МЕНЯТЬ ПАРОЛИ И ХРАНИТЬ ИХ В НАДЁЖНОМ МЕСТЕ (А ЛУЧШЕ ВСЕГО ВЫУЧИТЬ НА ПАМЯТЬ!)
4. НЕ ИСПОЛЬЗОВАТЬ ОДИНАКОВЫЕ ПАРОЛИ ДЛЯ РАЗНЫХ САЙТОВ
5. ПО ВОЗМОЖНОСТИ ПРИМЕНЯТЬ ДОПОЛНИТЕЛЬНЫЕ МЕТОДЫ ЗАЩИТЫ (ОДНОРАЗОВЫЕ СМС-ПАРОЛИ, ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ И ТП.)

Недетский контент



НЕДЕТСКИЙ КОНТЕНТ

КАК ЗАЩИТИТЬ СЕБЯ И БЛИЗКИХ ОТ ВРЕДНОГО КОНТЕНТА

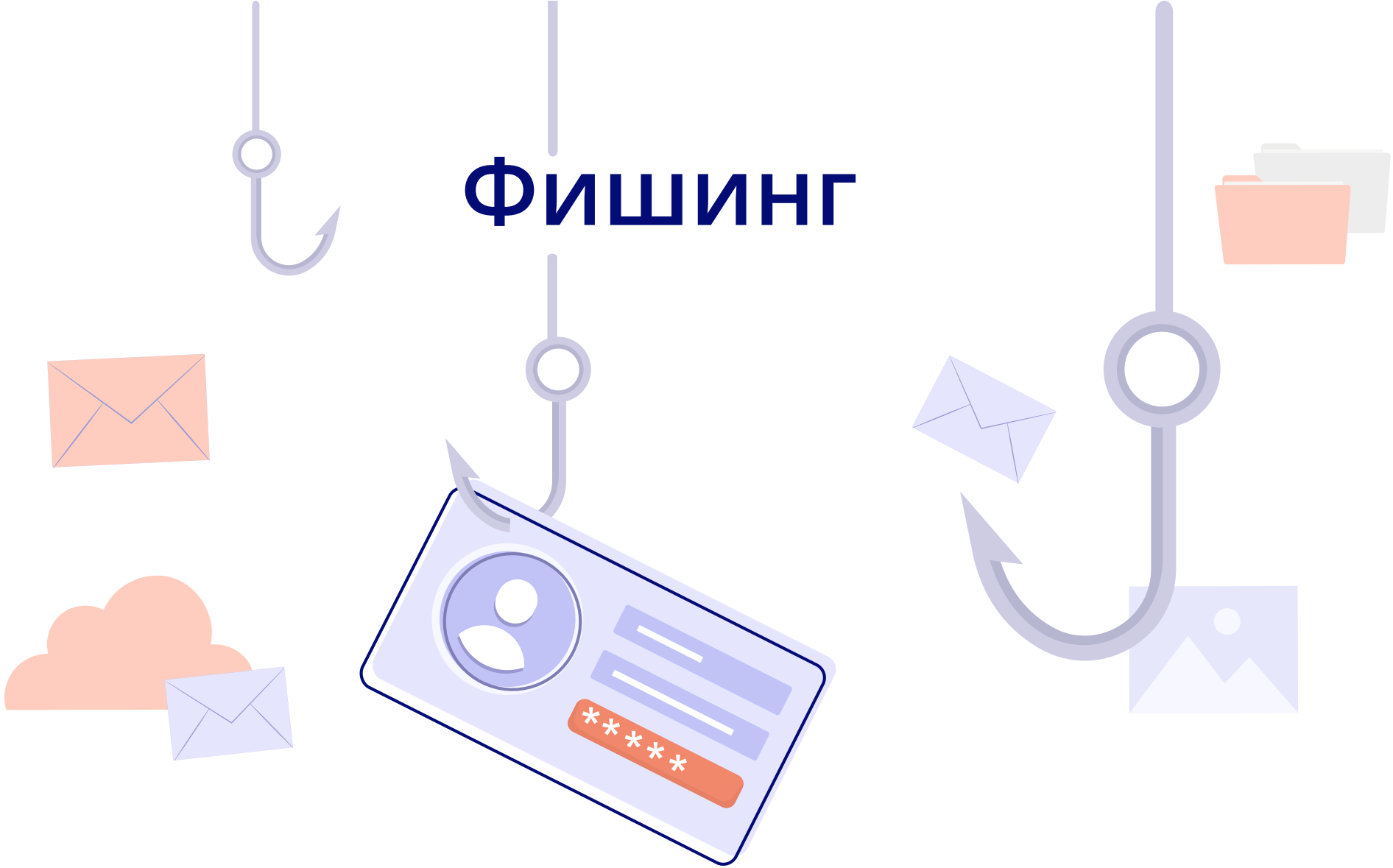
Этот тип угроз не нуждается в представлении. Все мы хотя бы раз натыкались в интернете на текст или картинки, которые потом хотелось «развидеть».

Чтобы оградить ребенка от нежелательного контента, нужно либо постоянно сидеть рядом с ним, либо использовать специальные программы родительского контроля.

1. ВКЛЮЧИТЬ НА УСТРОЙСТВЕ, КОТОРЫМ ПОЛЬЗУЕТСЯ РЕБЕНОК, «РОДИТЕЛЬСКИЙ КОНТРОЛЬ»

2. ПРОВЕСТИ ТЕМАТИЧЕСКОЕ РОДИТЕЛЬСКОЕ СОБРАНИЕ, ПОСВЯЩЕННОЕ БЕЗОПАСНОСТИ ДЕТЕЙ В СЕТИ (ИСПОЛЬЗУЙТЕ МАТЕРИАЛЫ ИЗ РАЗДЕЛА «ПОЛЕЗНЫЕ РЕСУРСЫ»)

Фишинг



ФИШИНГ

ЧТО НУЖНО ДЕЛАТЬ, ЧТОБЫ ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг – это ещё один вид мошенничества в Интернете, целью которого является «выуживание» конфиденциальных данных пользователей. Проще говоря, аферисты обманом заставляют людей сообщать свои личные данные: номера телефонов, коды банковских карт, пароли от электронной почты и социальных сетей.

Зачастую мошенники представляются социальными или банковскими работниками и предлагают различные «бонусные» услуги, для получения которых нужны конкретные данные пользователя.

Чтобы получить эту информацию, аферисты используют любые предлоги, например, восстановление доступа к якобы заблокированной карте или бесплатное тестирование нового приложения.

1. НЕ СООБЩАТЬ ЛИЧНЫЕ ДАННЫЕ ПОСТОРОННИМ ЛЮДЯМ
2. ПРОВЕРЯТЬ АДРЕСНЫЕ СТРОКИ И НАЗВАНИЯ САЙТОВ ПЕРЕД АВТОРИЗАЦИЕЙ
3. НЕ РЕАГИРОВАТЬ НА ЗАМАНЧИВЫЕ ПРЕДЛОЖЕНИЯ, ОСОБЕННО ЕСЛИ ОНИ «БОНУСНЫЕ» ИЛИ «БЕСПЛАТНЫЕ»
4. ПРОВЕРЯТЬ И ПЕРЕПРОВЕРЯТЬ ДОСТОВЕРНОСТЬ ПОЛУЧАЕМОЙ ИНФОРМАЦИИ ОТ ПОСТОРОННИХ ЛИЦ
5. ЗАПОМНИТЬ ПРОСТОЕ ПРАВИЛО: «БЕСПЛАТНЫЙ СЫР БЫВАЕТ ТОЛЬКО В МЫШЕЛОВКЕ!»

Анонимный недоброжелатель

АНОНИМНЫЙ НЕДОБРОЖЕЛАТЕЛЬ

КАК ЗАЩИТИТЬСЯ ОТ АНОНИМОВ

Каждый человек, который общается в интернете, зарегистрирован в соцсетях и использует мессенджеры, должен понимать, что не все виртуальные друзья – те, за кого себя выдают.

Например, часто под видом ровесников с детьми могут общаться взрослые, преследующие самые разные цели. Поэтому важно уметь критически оценивать все, что пишут незнакомые люди (в личных сообщениях, в комментариях, на форумах и в чатах).

1. НИ В КОЕМ СЛУЧАЕ НЕ РАЗГЛАШАТЬ ЛИЧНУЮ ИНФОРМАЦИЮ О СЕБЕ И О СВОИХ БЛИЗКИХ

2. ПРОВЕСТИ УРОК-ДИСКУССИЮ, ПОСВЯЩЕННЫЙ ИНТЕРНЕТ-УГРОЗАМ (ИСПОЛЬЗУЙТЕ МАТЕРИАЛЫ ИЗ РАЗДЕЛА «ПОЛЕЗНЫЕ РЕСУРСЫ»)

Троллинг

ТРОЛЛИНГ

КАК ЗАЩИТИТЬ СЕБЯ ОТ ТРОЛЛЕЙ

Что такое настоящий «троллинг» знают только самые заядлые рыбаки, ведь в реальной жизни именно так называют метод ловли рыбы на блесну. Однако большинство людей ассоциирует этот термин далеко не с рыбалкой.

В сети «троллингом» называют поведение, которое провоцирует конфликт и агрессию. Зачастую люди, которые занимаются подобными провокациями (их ещё называют троллями), стараются любыми способами обратить на себя внимание других пользователей, чтобы вступить с ними в словесную перепалку.

Такие споры практически всегда сопровождаются взаимными оскорблениями, открытой агрессией и даже угрозами, от чего тролли только выигрывают.

1. ПОБЕДИТЬ ТРОЛЛЯ В ЕГО ЖЕ ВОЙНЕ НЕВОЗМОЖНО, ТАК ЧТО НЕ СТОИТ КОРМИТЬ ЕГО ОСКОРБЛЕНИЯМИ
2. ВСЕГДА ЛУЧШЕ ПРОИГНОРИРОВАТЬ КОЛКИЙ КОММЕНТАРИЙ, ЧЕМ ПЫТАТЬСЯ ДОКАЗАТЬ ДУРАКУ, ЧТО ОН ДУРАК
3. НЕ НУЖНО ИДТИ У ТРОЛЛЯ НА ПОВОДУ И ВСТУПАТЬ С НИМ В ОТКРЫТЫЙ ДИАЛОГ, УКАЗЫВАЯ НА ЕГО ОШИБКИ И БЕССМЫСЛЕННЫЕ АРГУМЕНТЫ
4. ПОСТАВИТЬ ФИЛЬТР СООБЩЕНИЙ ИЛИ ДОБАВИТЬ АККАУНТ ПОЛЬЗОВАТЕЛЯ В ЧЕРНЫЙ СПИСОК, ЧТОБЫ БОЛЬШЕ НЕ ВИДЕТЬ ЕГО СООБЩЕНИЙ

Кибербуллинг

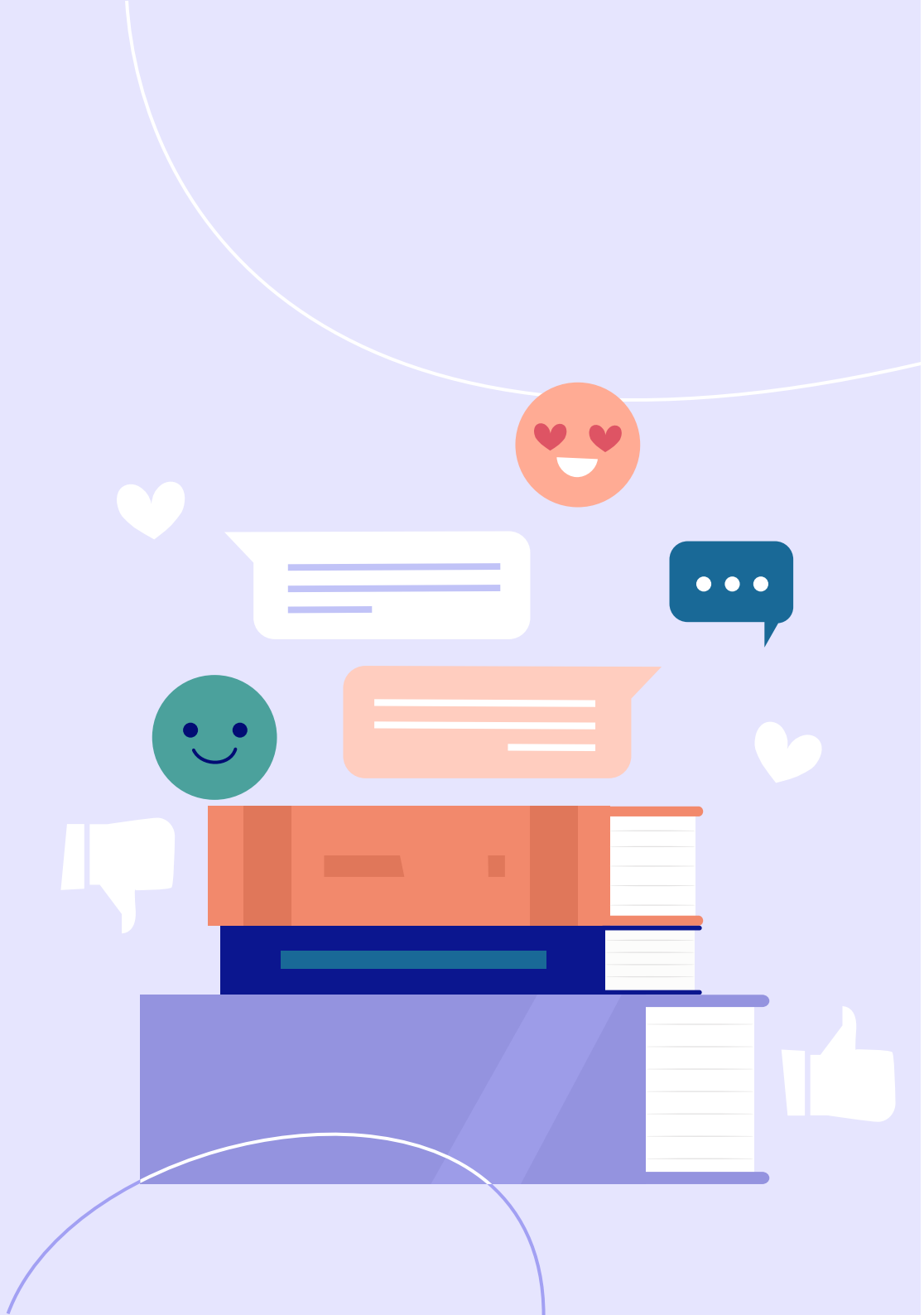
КИБЕРБУЛЛИНГ

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРБУЛЛИНГА

Кибербуллинг, к сожалению, стал распространенным явлением. Суть его близка к обычной травле, нередко возникающей в коллективе несовершеннолетних.

Жертвы кибербуллинга страдают от нападок в социальных сетях, угроз и оскорблений в личных сообщениях.

1. НЕ РЕАГИРОВАТЬ НА ОСКОРБЛЕНИЯ И ПРОВОКАЦИИ ПОЛЬЗОВАТЕЛЕЙ
2. СОХРАНЯТЬ СПОКОЙСТВИЕ И НАУЧИТЬСЯ ГОВОРИТЬ «СТОП!» АГРЕССИВНЫМ КОММЕНТАРИЯМ. НЕ ПОСЕЩАТЬ СТРАНИЦЫ, ГДЕ ВЫ ПОДВЕРГАЕТЕСЬ БУЛЛИНГУ
3. СРАЗУ БЛОКИРОВАТЬ ПОЛЬЗОВАТЕЛЕЙ, ПРИСЫЛАЮЩИХ УГРОЗЫ И ОСКОРБЛЕНИЯ
4. НАПИСАТЬ ЖАЛОБУ АДМИНИСТРАТОРУ САЙТА С ПРОСЬБОЙ ЗАБАНИТЬ АГРЕССИВНОГО ПОЛЬЗОВАТЕЛЯ. СООБЩИТЬ РОДИТЕЛЯМ О ТОМ, ЧТО ПРОИСХОДИТ
5. ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ К АДМИНИСТРАЦИИ ШКОЛЫ, ЕСЛИ ВЫ ИЛИ ВАШИ ОДНОКЛАССНИКИ СТАЛИ ЖЕРТВАМИ КИБЕРБУЛЛИНГА
6. ПРОВЕДИТЕ КЛАССНЫЙ ЧАС, ПОСВЯЩЕННЫЙ ТЕМЕ КИБЕРБУЛЛИНГА (ИСПОЛЬЗУЙТЕ СЛОВАРИК НЕТИКЕТА И МАТЕРИАЛЫ ИЗ РАЗДЕЛА «ПОЛЕЗНЫЕ РЕСУРСЫ»)



02

КРАТКИЙ СЛОВАРИК НЕТИКЕТА – ЭТИКЕТА ОБЩЕНИЯ В ИНТЕРНЕТЕ

Проверенные советы и полезные правила продуктивного интернет-общения по принципам уважения, информационной безопасности и психогигиены.

НЕТИКЕТ

ЭТИКЕТА ОБЩЕНИЯ В ИНТЕРНЕТЕ

Флейм – это неожиданно возникшее бурное обсуждение, в комментариях на сайте, в соцсетях, на форуме. Часто участники флейма забывают о начальной теме обсуждения, переходят к оскорблениям и негативным высказываниям в адрес оппонентов.

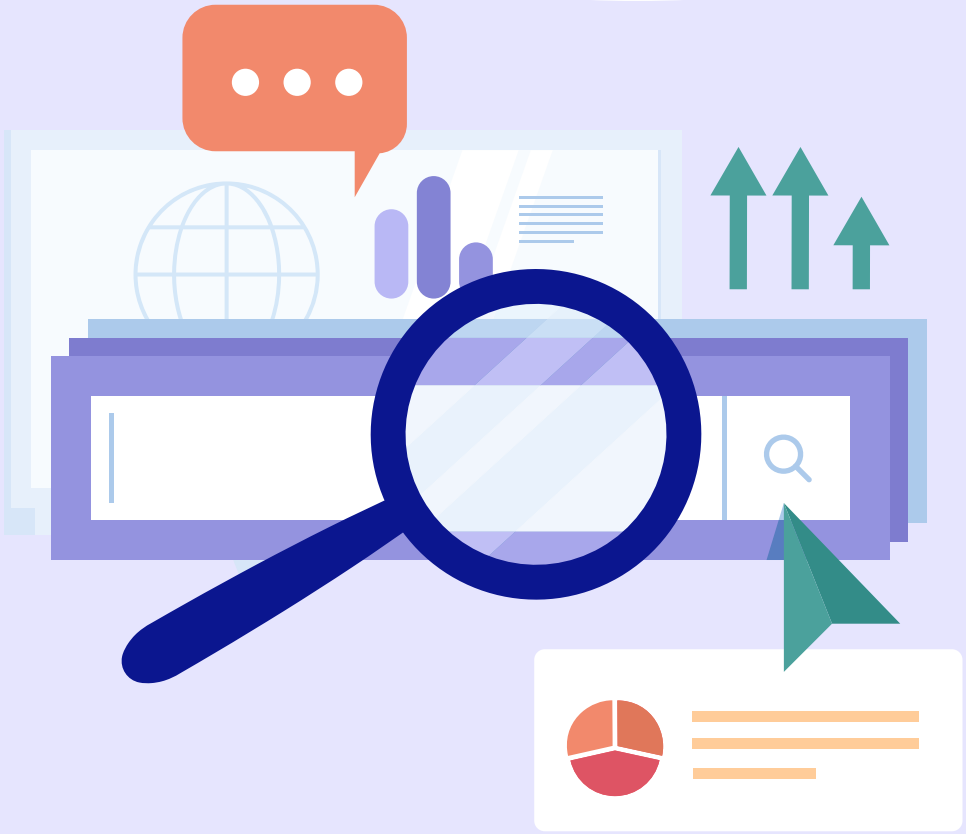
Флуд – (от англ. flood – наводнение) – сообщения на форуме или в чате, не несущие никакой пользы. Обычно флуд распространяют от нечего делать, но нередко и с целью троллинга.

Тролль – человек, который ведёт себя агрессивно по отношению к другим пользователям и всячески провоцирует конфликт в сети. Термин «троллинг» произошёл от метода рыбной ловли, а не от мифологических существ, как ошибочно считают многие люди.

Пруф – подтверждение сказанного, доказательство. В виде ссылки на источник, видео или фотоматериал.

Игнор – игнорирование собеседника. Может быть оправдан, если вы столкнулись с троллингом и флеймом.

Капс – злоупотребление использованием ЗАГЛАВНЫХ БУКВ при написании сообщений. Обычно, такие сообщения воспринимаются как фразы, произнесенные ПОВЫШЕННЫМ ТОНОМ ИЛИ ВООБЩЕ С ПЕРЕХОДОМ НА КРИК.



03

ПОЛЕЗНЫЕ РЕСУРСЫ

Используйте данные ресурсы, статьи, видео, инфографику для того, чтобы защититься от интернет-злоумышленников и рассказать о правилах интернет-безопасности своим коллегам, ученикам и их родителям.

ПОЛЕЗНЫЕ РЕСУРСЫ

РЕСУРСЫ, СТАТЬИ, ВИДЕО, ИНФОГРАФИКА

1. Генератор безопасных паролей

2. Рейтинг антивирусов 2020 – выбираем лучший антивирус

3. Видеоинструкция «Как настроить родительский контроль в Windows 8»

4. Видеоинструкция «Как настроить родительский контроль в Windows 10»

5. Kidslox – родительский контроль для Android и iOS

6. Социальный ролик «Безопасный интернет – детям!»

7. Социальный ролик «Дикий мир интернета»

8. Социальный ролик «История одного знакомства»

9. Статья «СТОП буллинг! Как остановить травлю в школе»

10. Статья «9 советов, как остановить насмешки над детьми с особенными потребностями»

от проекта mega-talant.com
2020