Занятие первое

Правило пароля

1. Выбери сложный пароль, который будет затруднительно угадать преступникам.
2. Надежные пароли содержат 8 и более знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п.
3. Используй разные пароли для разных аккаунтов.
4. Выбирай двух- или трехступенчатую систему авторизации на сайтах (например, пароль в игре и код, приходящий на мобильный телефон).
5. Отключи функцию сохранения паролей в браузере.
6. Твои пароли от сайтов и приложений знаешь только ты и твои родители.
7. При регистрации на ресурсах, которые сами генерируют пароль, постарайся сразу же после регистрации сменить его на новый, придуманный самостоятельно.
8. Если без твоего запроса тебе пришло письмо по электронной почте о том, что пароль от твоего аккаунта на сайте был изменен, как можно скорее зайди на этот сайт и смени пароль.

Как создать надежный пароль

Источник: Интернет: возможности, компетенции, безопасность : метод. пособие для работников системы общего образования. — М. : Google, 2013. — 137 с.

1. Выбираем любое имя прилагательное. Например, «зажаренный».
2. Выбираем любое имя существительное. Главное, чтобы это существительное по смыслу не сочеталось с выбранным прилагательным. Например, «снежок».
3. Берем цифру, которую легко запомнить (любимую цифру, дату рождения, последние четыре номера мобильного телефона и т. д.). Например, «2004».
4. Берем любой знак препинания. Например, «!».
5. Запишем выбранные слова, цифры и символы в одну строку без пробелов. Получится: «зажаренныйснежок1984!».
6. Поменяем в этой строке какую-нибудь строчную букву на прописную. Например, так: «Зажаренныйснежок1984!».

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Занятие второе

«Пиратом» можешь ты не быть, а риски знать – обязан!

1. «Пиратские» файлы игр, фильмов, музыки и прочего почти всегда содержат вредоносные элементы – вирусы, трояны. Они постараются испортить твой компьютер, планшет или мобильный телефон.

2. Для скачивания «пиратского» ресурса зачастую требуется отправлять СМС с мобильного телефона, закрывать огромное количество всплывающих окон. Каждое из этих действий может заразить твой компьютер или потратить деньги со счета твоего телефона. Прибыль от твоих ошибок получат владельцы «пиратского» сайта.

3. «Пиратство» мешает автору заработать на своем произведении, на которое было потрачено много времени, денег и сил. Как бы ты себя чувствовал на месте автора?

4. Есть много по-настоящему бесплатных и интересных интернет-программ и медиаресурсов – фильмов, книг, музыки и т. д. Попроси родителей, опекунов или учителя показать их тебе.

5. Устанавливая приложение на планшет или смартфон, обращай внимание, сколько и каких разрешений на доступ к твоим данным приложение запрашивает. Если в списке есть разрешения на ненужные функции, это тревожный знак. Например, запрашивается использование микрофона, но в приложении нет взаимодействий с голосом (петь, давать голосовые команды). То же самое с камерой и определением местоположения. В таких случаях лучше отказаться от установки.

6. Пусть на твоем компьютере или мобильном устройстве (планшете, телефоне) всегда будет включена антивирусная программа. Даже когда ты играешь в компьютерную игру, твой компьютер могут заразить. Во многих антивирусах есть на этот случай «игровой режим».

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Занятие третье

Кибербуллинг. Что за слово такое? А что делать в трудной ситуации?

Кибербуллинг – намеренные оскорбления, угрозы, сообщение другим секретных данных о тебе с помощью Интернета. Эти атаки повторяются, обычно, много раз в течение долгого времени. Чтобы остановить кибербуллинг, **обязательно обратись за помощью к родителям, учителю или на «линию помощи» детям.**

Похожие слова: кибермоббинг, интернет-моббинг, троллинг, флейм(инг), интернет-травля, кибертравля.

Что делать в трудной ситуации

• Игнорируй одноразовые оскорбительные сообщения. Часто агрессия прекращается на начальной стадии.

• Уходи от драки. Лучший способ: посоветоваться, как себя вести, а также вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то лишь усложнишь ситуацию.

• Если ты будешь спокоен и сдержан – весь «труд» злоумышленника пропадет зря. Скорее всего, ему быстро надоест «заниматься» именно тобой.

• Бан агрессора. В программах обмена сообщениями, в социальных сетях есть возможность блокировки плохих сообщений. На многих сайтах есть кнопки «пожаловаться на сообщение».

• Если ты свидетель кибербуллинга, твои действия: сообщить человеку, которому ты доверяешь, – родителям, или учителю, или школьному психологу, о факте агрессивного поведения в интернете.

• Если ты жертва кибербуллинга, расскажи родителям, учителю, школьному психологу – тому, кому ты доверяешь, чтобы они могли принять меры. Распечатай сообщение с угрозами. Используй кнопку «Print Screen» или программу для фотографирования кадра на экране компьютера и затем сохрани этот файл где-то в безопасном месте. Если у тебя есть телефон или планшет, используй функцию для создания снимка экрана и также сохрани эти изображения.

• Делай выбор в пользу такого, безвредного для тебя и других и разумного варианта поведения, который тебе обеспечит ощущение безопасности, счастья и покоя.

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Занятие четвертое

Как защитить свои персональные данные?

Персональные данные – это набор точных данных о конкретном человеке. Эти данные помогают выделить его среди всех других людей. Например, фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, возраст и другие. Только имя или только фамилия тебя не выделят, а вот если добавить к фамилии номер школы, класс, домашний адрес, то сразу будет понятно, о ком говорится.

- Ограничь в Интернете информацию о себе. Убери лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
- Если в Интернете кто-то просит предоставить твои персональные данные, например, место жительства или номер школы, класса и т.п., вначале посоветуйся с родителями или другим взрослым человеком, которому доверяешь.
- Отправляя кому-либо свои персональные данные или другую секретную информацию, убедись лично или по телефону, что адресат действительно тот, за кого себя выдает.

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Занятие пятое

Как сберечь репутацию в интернете

Овершеринг *(от англ. overshare — чрезмерно много делиться)* — стремление человека рассказывать окружающим больше, чем стоило бы. Подобное поведение чаще всего вызывает у собеседника чувство неловкости. В отдельных случаях, может даже шокировать или привлечь внимание мошенников.

• Откажись от размещения в открытом доступе того, что может навредить твоей репутации сейчас или в будущем. Хотя бы один или два раза в год внимательно просматривай всю информацию своих профилей в социальных сетях.

• В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей». Если по каким-либо причинам ты не желаешь или не можешь этого сделать — еще строже оценивай информацию, которую размещаешь.

• Пословица «Слово не воробей, вылетит — не поймаешь» работает и в Интернете.

• Выкладывай информацию в Интернет, находясь в спокойном состоянии. Рискованно идти на поводу у эмоций, как отрицательных, так и положительных.

• Размещение информации, которая может кого-либо оскорблять или обижать, запрещено законом.

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Телефоны доверия для детей (звонок бесплатный)

8 800 2000 122

Всероссийский детский телефон доверия. Обращайся в трудной жизненной ситуации. Работает с понедельника по пятницу с 9 до 20 часов

8 800 25 000 15

линия помощи «Дети онлайн». Можно обратиться в с понедельника по пятницу с 9 до 17 часов), по электронной почте helpline@detionline.com или через сайт http://detionline.com, чтобы получить квалифицированную помощь и психологическую поддержку

Телефоны государственных служб – звонить в трудной жизненной ситуации

02

экстренный вызов полиции

112

экстренный вызов спецслужб

(4012) 576-860

дежурная часть Прокуратуры Калининградской области

(4012) 214-639

дежурная часть Управления Министерства внутренних дел по Калининградской области

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Тестовые вопросы

1. Кому можно отправить логин и пароль от аккаунта ВКонтакте или другой социальной сети?

1.1 Администрации ВКонтакте.
1.2 Близким друзьям, если им это зачем-то очень нужно.
1.3 Любым государственным органам при запросе по любым каналам.
1.4 Никому.

2. Кто может знать пароли от твоих аккаунтов в интернете или приложений на компьютере, планшете, мобильном телефоне?

2.1 Никто не знает моих паролей, но я использую специальную электронную систему хранения паролей
2.2 Никто, кроме меня
2.3 Мой лучший друг/подруга

3. В каком случае нарушается закон?

3.1 При чтении сказок А. С. Пушкина в Интернете
3.2 При использовании материалов Википедии для подготовки реферата со ссылкой на источник
3.3 При размещении на YouTube собственного видеоролика с концерта любимой группы

4. С кем можно дружить в социальных сетях?

4.1 С кем угодно – и с реальными знакомыми, и с онлайновыми.
4.2 С детьми – и с реальными знакомыми, и с онлайновыми.
4.3 Только с теми детьми, кого знаешь в реальной жизни.
4.4 С теми, кого знаешь в реальной жизни.

5. Что делать, если тебя обижают в интернете?

5.1 Постоять за себя!
5.2 Попросить родителей поговорить с обидчиками!
5.3 Удалить везде свои страницы и перестать пользоваться интернетом.
5.4 Игнорировать обидчиков, стараться больше общаться с настоящими друзьями и родителями.

6. Кто должен иметь возможность посмотреть твой аккаунт в соцсети?

6.1 Кто угодно – я хочу, чтобы мне ставили много лайков даже те, кого нет у меня в друзьях.
6.2 Только мама и папа.
6.3 Все мои друзья и их друзья, на случай если кто-то из них и мой друг тоже.
6.4 Только те, кто есть у меня в друзьях.

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

7. Что может компьютерный вирус?

7.1 Заставить тебя заболеть.
7.2 Заставить компьютер кашлять.
7.3 Сломать компьютер.
7.4 Украсть наличные деньги из твоего кошелька.

8. Что может помочь от компьютерных вирусов?

8.1 Внимательность и антивирусная программа.
8.2 Антивирусная программа.
8.3 Внимательность.
8.4 Лекарства.

9. Какую информацию о себе нельзя сообщать у себя в аккаунте?

9.1 Можно любую, ведь он доступен только для тех, кого я знаю лично.
9.2 Нельзя вообще никакую.
9.3 Опасно оставлять адрес, номер школы, номер телефона и другие данные, с помощью которых меня можно найти или обмануть.
9.4 Опасно использовать свою фотографию.

10. Что является признаком достоверности информации в интернете?

10.1 Красивое оформление сайта.
10.2 Возможность перепроверить эту информацию на надежных сайтах.
10.3 Информация кажется правдоподобной.
10.4 Информация написана грамотно.
10.5 Есть ссылки на официальные и надежные источники.

Источники: https://kids.kaspersky.ru/, http://www.razbiraeminternet.ru

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Список участников «___» _____ 20___ г.

Учебное заведение _____

Преподаватель _____

_____

Класс _____

1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	
16.	
17.	
18.	
19.	
20.	
21.	
22.	
23.	
24.	
25.	
26.	
27.	
28.	
29.	

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Придумываем настольную игру

5-10 ходов или карточек с заданиями

1. Определяем стиль игры: каждый за себя или все вместе против игры.

2. Выбираем сцену/тему игры (космос, город-призрак, каменный век, заповедник и т.п.).

3. Делаем игровое поле и/или игровые карточки.

4. Ставим цели для играющих (условия победы). Например, первым дойти до финиша или первым набрать 100 очков.

5. Выбираем одно! действие, которое приведет к достижению цели. Например, кинь кубик и передвинь фишку на выпавшее число ходов.

6. Как будет выглядеть начало игры (где, что, кто находится)?

7. Задаем препятствия и другие трудности на пути к победе.

8. Пишем правила.

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.

Придумываем комикс или сказку

2, 3 или 4 панели/страницы

1. Определяем тему.
2. Решаем, кто будут главные герои.
3. Должны быть положительные герои и хотя бы один отрицательный.
4. Где происходит действие?
5. С чего оно начинается (загадка, тайна, конфликт, необычная ситуация, проблема)?
6. А чем закончится?
7. Дополняем историю чудесными превращениями, волшебными предметами и помощниками.
8. Пишем диалоги героев и текст «от автора».
9. Рисуем свою историю.
10. Соединяем диалоги, текст «от автора» и картинки.

Мастер-класс проводится с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов для реализации проекта «Интернет полезный, Интернет вредный» АНО «Балтийский центр социальных инноваций» https://baltcsi.ru.