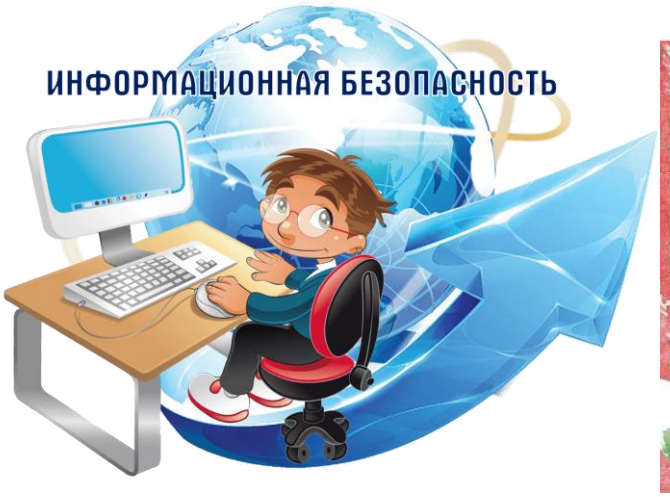
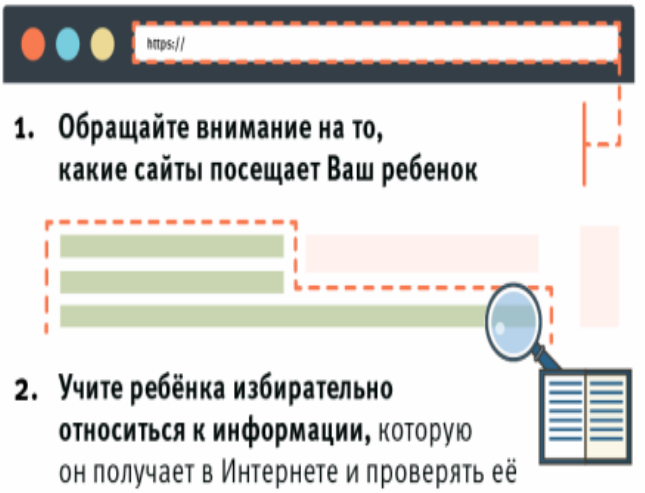
Профилактика киберпреступностит против несовершенолетних



ПРОЕКТ РОССИИ ВАЖЕН КАЖДЫЙ РЕБЕНОК

5 ПРАВИЛ БЕЗОПАСНОСТИ ДЕТЕЙ В ИНТЕРНЕТЕ

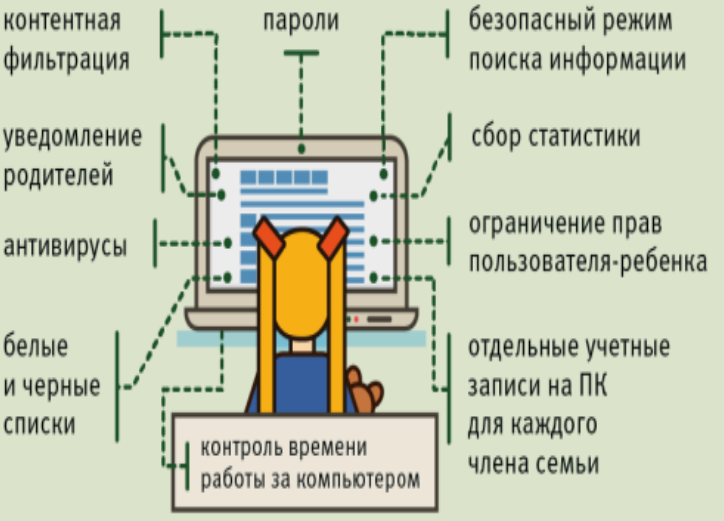


1. **Обращайте внимание на то, какие сайты посещает Ваш ребенок**

2. **Учите ребёнка избирательно относиться к информации,** которую он получает в Интернете и проверять её

3. **Объясняйте ребенку, как правильно реагировать** на возможного агрессора и конфликтные ситуации в Интернете

5. **Используйте технологии родительского контроля на всех устройствах с выходом в Интернет:**



4. **РАССКАЖИТЕ РЕБЕНКУ О ТОМ, КАКУЮ ИНФОРМАЦИЮ РАЗМЕЩАТЬ НА СТРАНИЦАХ СОЦИАЛЬНЫХ СЕТЕЙ ОПАСНО:**

- О СВОЁМ МЕСТОПОЛОЖЕНИИ
- О ПЛАНАХ НА ДЛИТЕЛЬНЫЕ ПОЕЗДКИ
- ФОТО ДОРОГИХ ВЕЩЕЙ И ПОДАРКОВ
- ФОТО КВАРТИРЫ ИЛИ ДОМА
- СВОЙ ДОМАШНИЙ АДРЕС
- ФОТО ЛИЧНЫХ ДОКУМЕНТОВ И БАНКОВСКИХ КАРТ

t.me/proektyER

Безопасный интернет

Типы угроз кибербезопасности

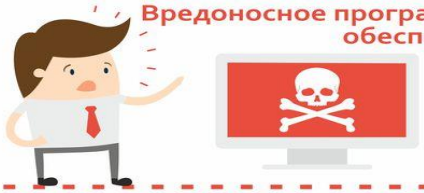
Фишинг

Рассылка поддельной электронной корреспонденции, которая выглядит как сообщения от надежных источников. Целью является кража конфиденциальных данных, таких как номера кредитных карт и информация об учетных записях. Это самый распространенный тип кибератак. Обеспечить защиту можно с помощью изучения необходимой информации или установки технологический решений, которые могут отфильтровать вредоносные электронные письма.

Социальная инженерия

Тактика, которую используют злоумышленники, чтобы склонить пользователя к раскрытию конфиденциальной информации. Они могут обратиться с просьбой о денежном платеже или о получении доступа к конфиденциальным данным. Способы социальной инженерии могут применяться вместе с другими угрозами, чтобы с большей вероятностью вынудить пользователя нажать на ссылку, загрузить вредоносное ПО или поверить злонамеренному источнику.

Вредоносное программное обеспечение

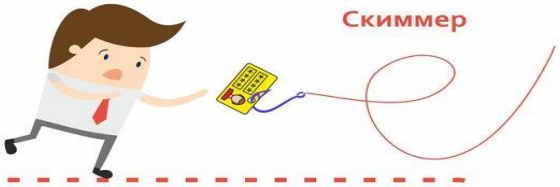


Вредоносное программное обеспечение предназначено для получения несанкционированного доступа или повреждения компьютерной системы.

Вишинг

Вишинг – (vishing –Вишинг – (vishing –voice phishing-голосовой фишинг) — вид социальной инженерии, при котором мошенники так или иначе задействуют телефон.

Скиммер



Вид мошенничества с банковскими картами, который предусматривает использование различных устройств типа – скиммер.
С помощью таких устройств мошенники считывают информацию, содержащуюся на магнитной полосе карты.

Программа-вымогатель

Разновидность вредоносного программного обеспечения. Они предназначены для вымогательства денег посредством блокировки доступа к файлам компьютерной системы до поступления выкупа.
Перечисление выкупа не гарантирует восстановление файлов или работоспособности системы

Безопасность в интернете

Не указывай свою личную информацию, настоящее имя, адрес, телефон и места, где ты часто бываешь.

Относись с осторожностью к публикации личных фото. Не выкладывай фото других людей без их согласия.

Не доверяй всей информации, размещенной в Интернете. Не доверяй незнакомым людям, они могут выдавать себя за других.

Не переходи по сомнительным ссылкам (например, обещающим выигрыш). Не посещай сомнительные сайты. Они могут нанести вред твоей психике.

Помни, что незаконное копирование авторских материалов преследуется по закону.

Не встречайся в реальной жизни с людьми, с которыми ты познакомился в Интернете. Сообщи родителям, если друзья из Интернета настаивают на личной встрече.

Помни, что в виртуальном мире действуют те же правила вежливости, что и в реальном.

Не отправляй смс, чтобы получить какую-либо услугу или выиграть приз.

Обращайся за советом к взрослым при малейшем сомнении или подозрении.

МАУ Дом культуры «Энергетик»

ВНИМАНИЕ! БЕЗОПАСНЫЙ ИНТЕРНЕТ!

БЕЗОПАСНЫЙ ИНТЕРНЕТ

СТАРТ

Храни в тайне свои: фамилию, номер телефона и школы, адрес, где ты живешь, дату твоего рождения, пароли и другую личную информацию!

Сообщишь свои данные?

ДА

НЕТ

Рассказывай родителям о своих друзьях в сети и советуйся, прежде чем добавить кого-то нового «в друзья» - незнакомец в Интернете также опасен, как и на улице.

Добавишь незнакомцев в «друзья»?

НЕТ

ДА

Нажмешь без спроса неизвестные кнопки?

ДА

НЕТ

Всегда спрашивай родителей о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.

Посоветуешься со взрослыми прежде чем играть?

ДА

НЕТ

Показывай взрослым, в какие интернет-игры ты играешь, – это поможет сберечь компьютер от вирусов, а тебя и твою семью от мошенников.

Согласишься на личную встречу?

ДА

НЕТ

Если тебя приглашают встретиться твои интернет-знакомые - соглашайся прийти только вместе со своими родителями.

ФИНИШ

Советы родителям по детской кибербезопасности

Посещайте сеть вместе с детьми, пусть они делятся с вами опытом использования Интернета

Научите детей доверять интуиции. Если их в Интернете что-либо беспокоит, пусть сообщат вам

Попросите ребёнка регистрироваться в программах, требующих личную информацию, только в вашем присутствии

Детям никогда не следует встречаться с друзьями из Интернета, так как эти люди могут оказаться совсем не теми, за кого себя выдают

Настаивайте, чтобы дети никогда не давали своего адреса, номера телефона или другой личной информации

Настаивайте, чтобы дети уважали чужую собственность, расскажите, что незаконное копирование музыки, компьютерных игр и других программ - кража

Скажите детям, что не вся информация из Интернета - правда.
Научите их проверять информацию из сети

Научите детей уважать других. Убедитесь, что они знают о том, что правила хорошего тона действуют везде - даже в виртуальном мире

Используйте программы родительского контроля, которые блокируют вредоносный контент, фиксируют какие сайты посещает ребенок

Федеральный проект Информационная безопасность
Департамент цифрового развития Вологодской области
Уполномоченный по правам ребенка в Вологодской области
Цифровое развитие Вологодской области

ПАМЯТКА ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

В Интернет ты заходишь через компьютер или мобильное устройство. Это может быть школьный или библиотечный компьютер, твой личный или твоей семьи. Любому устройству могут повредить вирусы. Они могут уничтожить важную информацию или украсть деньги через Интернет.

НЕ ЗАХОДИ НА ПОДОЗРИТЕЛЬНЫЙ САЙТ

Если антивирусная защита компьютера или мобильного устройства не рекомендует, не заходи на сайт, который считается «подозрительным».

НИКОМУ НЕ СООБЩАЙ СВОЙ ЛОГИН С ПАРОЛЕМ

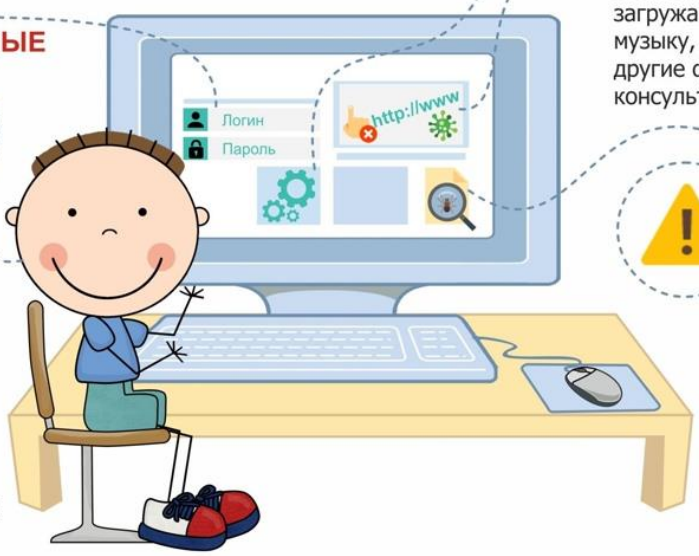
Никому не сообщай свой логин с паролем и не выкладывай их в Интернете - относись к ним так же бережно, как к ключам от квартиры.

НЕ МЕНЯЙ НАСТРОЙКИ ГАДЖЕТА

Для защиты компьютера на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!

НЕ СОХРАНЯЙ ПОДОЗРИТЕЛЬНЫЕ ФАЙЛЫ И НЕ ОТКРЫВАЙ ИХ

Не устанавливай и не загружай программы, музыку, видео или другие файлы без консультаций с родителями.



НЕ СООБЩАЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Никогда не сообщай свои имя, номер телефона, адрес проживания или учебы, пароли, любимые места отдыха или проведения досуга, чтобы этой информацией не смогли воспользоваться в своих преступных целях злоумышленники.

ПОМНИ!

Не вся информация в сети Интернет достоверна!

РАССКАЖИ ВЗРОСЛЫМ

Всегда сообщай взрослым обо всех случаях в Интернете, которые вызвали у тебя смущение или тревогу.

Памятка

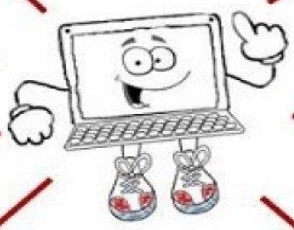
безопасного поведения и общения в сети Интернет

Придумай безопасные пароли, держи их в секрете, не сообщай свой телефон и электронный адрес!

Будь вежливым и дружелюбным, не груби, нельзя использовать сеть для хулиганства и угроз!

Используй псевдоним (логин), не сообщай своё имя и фамилию, не высылай фотографии!

Помни о личной безопасности, веди себя осторожно: никогда не сообщай информацию о себе!



Не загружай сомнительные файлы – это вирусы, черви, программы-шпионы, которые приносят вред!

Нельзя встречаться с виртуальными знакомыми – это могут быть злоумышленники!

Не ходи по незнакомым сайтам и ссылкам, можно попасть в «небезопасную зону»!

Прекрати общение и не возобновляй, если тебя оскорбили, сообщи об этом взрослым!

Игнорируй нежелательную почту и рассылки – это спам (ненужные сообщения программ-роботов)!

Уважай авторские права, указывай источник информации! (Часть 4 Гражданского кодекса Р.Ф.)

Не открывай сообщения без взрослого, если не знаешь кто их отправил!

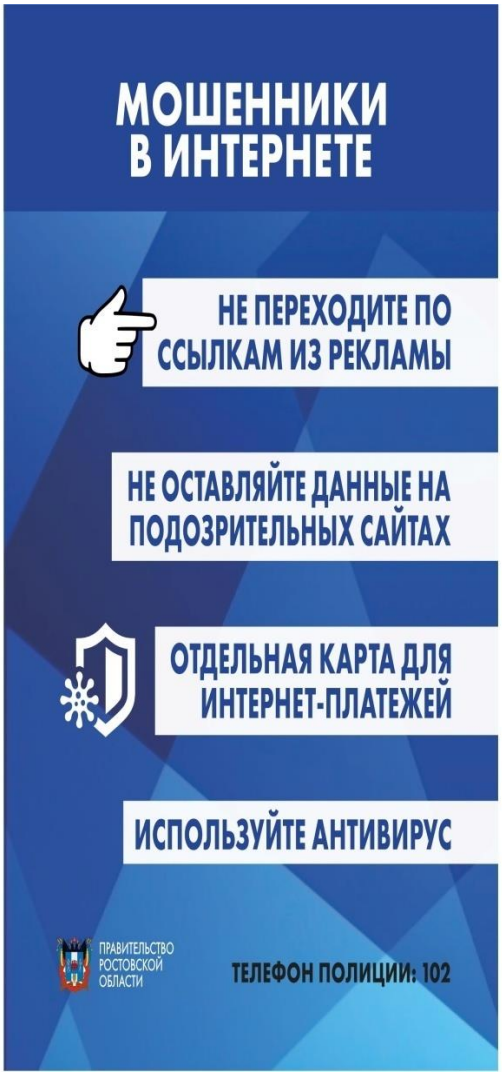
Твои защитники – антивирусные программы, установи их и регулярно обновляй!

Безопасного путешествия в сети!

Осторожно - мошенники!

Как не стать жертвой киберпреступника

Помните! Никому нельзя сообщать: номер, срок действия, коды подтверждения на обороте карты, коды из СМС-сообщений, логины и пароли.



Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТЫ

Наиболее распространенные методы работы злоумышленников

выманивание реквизитов банковских платежных карт с использованием взломанных аккаунтов знакомых в социальных сетях

ЛЖЕПОКУПАТЕЛЬ - под видом покупателя злоумышленник связывается с продавцом, предлагает внести залог перед покупкой товара, а для получения денежного перевода предоставляет ему ссылку на мошеннический сайт, визуально похожий на официальный сайт банка

ВИШИНГ - представляясь по телефону сотрудником банка, злоумышленник пытается узнать у держателя карты конфиденциальную информацию (ее реквизиты, а также номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды)

НЕ СООБЩАЙТЕ НИКОМУ

- информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код
- цифровые или буквенные коды
- паспортные данные

ЕСЛИ ВАМ ПОСТУПИЛ СОМНИТЕЛЬНЫЙ ЗВОНОК

- немедленно завершите разговор
- обратитесь в контакт-центр банка, выпустившего карту
- следуйте рекомендациям сотрудника банка