Автор: Белоусова Виктория, 6 А класс,
Руководитель: Александрова З.В., учитель физики и информатики МБОУ СОШ №5 пгт Печенга, Мурманская область

2015 г.

Презентация подготовлена для конкурса «Интернешка» http://interneshka.org

Защита собственной информации от несанкционированного доступа

За безопасность необходимо платить, а за ее отсутствие расплачиваться.

Праздник — День безопасного Интернета

Праздник — День безопасного Интернета (Safer Internet Day) отмечается в мире с 2004 года, он был создан для того, чтобы привлечь внимание пользователей к этой проблеме.

Полной безопасности в Интернете, конечно, достичь не реально. Каждый человек может сделать свой интернет безопаснее, а помогут в этом «Золотые правила безопасности в интернете», которые откроют дорогу в безопасный интернет.

Защита информации

Защита от несанкционированного копирования — система мер, направленных на противодействие несанкционированному копированию информации, как правило представленной в электронном виде (данных или программного обеспечения).

При защите от копирования в интернете используются различные меры:

- организационные;
- юридические;
- физические.

Защита информации

Для защиты данных, хранящихся на компьютере, используются пароли. Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

Защита информации. полноценное использование программного продукта невозможно без соответствующей поддержки со стороны производителя: подробной пользовательской документации, «горячей линии», системы обучения пользователей и т.п. Организационные меры защиты применяются крупными разработчиками к достаточно большим и сложным программным продуктам.

Для защиты доступа к информации всё чаще используют биометрические системы идентификации: идентификация по отпечаткам пальцев, системы распознавания речи, системы идентификации по радужной оболочке глаза, по изображению лица, по геометрии ладони руки. Организационные меры защиты от несанкционированного копирования.

Золотые правила безопасности в интернете

1. ХОРОШИЙ КАЧЕСТВЕННЫЙ АНТИВИРУС.

Перед тем, как начать пользоваться компьютером, обязательно позаботьтесь об установке качественного и проверенного временем антивируса. Их очень много, и тут советовать можно уже по вашему усмотрению, отзывам и практическому подходу к этому вопросу. Когда вы подключаете какое-либо внешнее устройство к вашему компьютеру, например, флешку, то всегда проверяйте антивирусом, чтобы не заразить свой компьютер. Периодически проверяйте и ваш компьютер – запускайте сканирование.

Золотые правила безопасности в интернете

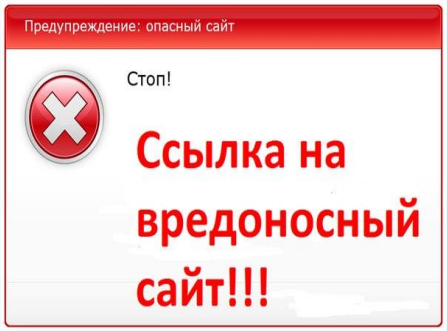
2. НЕ ЗАБЫВАЙТЕ ПРО ОБНОВЛЕНИЯ ВАШИХ ПРОГРАММ.

Активный человек всегда пользуется множеством программ и приложений. Каждый раз хакеры ищут «дыры и уязвимости», через которые можно взломать программу. Но, есть выход из этой ситуации. У программ есть обновления, про которые не следует забывать. С помощью обновлений исправляются уязвимости старых версий.

Это займёт не много времени, но защитит ваш компьютер от вирусов и вредоносных программ.

Золотые правила безопасности в интернете

3. ОХ, УЖ ЭТИ ОПАСНЫЕ ССЫЛКИ.



Ссылки придумали, чтобы на жилось легче в интернет жизни. Это те дороги, по которым ссылки, как трамвайчики доставляют нас к нужному месту.

Это происходит мгновенно. И тут только от вашей осторожности будет зависеть, где именно вы окажетесь – после такого мгновенного проезда- в нужном месте или в ловушке?

Но, этим умело пользуются всякие мошенники, обманным путём завлекая вас кликнуть по ссылке или баннеру и один миг, и вы уже оказались на сайте с вирусами.

Золотые правила безопасности в интернете

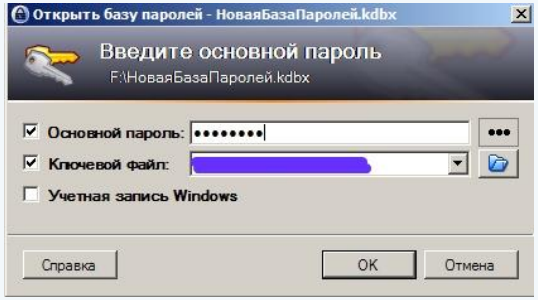
4. У ВАС ЕСТЬ СМАРТФОН? НЕ ЗАБЫВАЙТЕ – ЭТО ТОЖЕ КОМПЬЮТЕР!

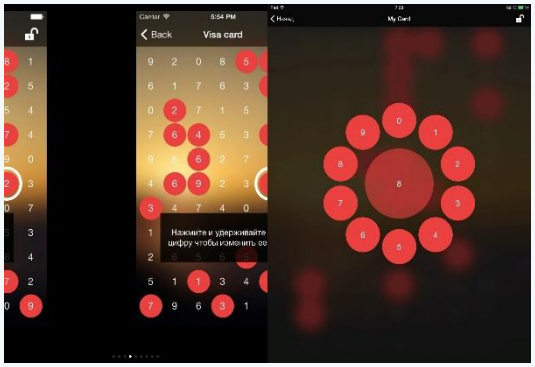
У него есть операционная система, его тоже нужно оберегать. С ним тоже надо соблюдать правила безопасности выхода в интернет. И антивирус хороший ему не помешает.

Не устанавливайте приложения сомнительного вида, скачивайте только с официальных источников и читайте отзывы. И всегда смотрите, какое право и куда имеет доступ приложение. Иногда там чётко бывает написано, что приложение имеет доступ к отправке платных смс.

Золотые правила безопасности в интернете

5. ЗАВЕДИТЕ ХРАНИТЕЛЬ ПАРОЛЕЙ. ПО ТЕХНИЧЕСКОМУ – МЕНЕДЖЕР ПАРОЛЕЙ.





Если вы обладаете отличной памятью на цифры и набор букв, то храните все пароли в своей голове. Хранить и запомнить их будет очень сложно, так как это на самом деле очень сложно. хранить их лучше в менеджере паролей, там придётся запомнить только один пароль для входа.

Или записывайте их в тетрадь, к которой доступ закрыт для остальных людей. Как сделать доступ тетради закрытым для других? Просто спрячьте её в сейфе или напишите пароли тоже при помощи шифра, придуманного вами.

Например, напишите пароль 5hdjrf587nvmm888, но запишите его в тетради в обратном порядке. Это правило шифровки можно применить для всех паролей. Об этом будете знать только вы и поэтому смело оставляйте тетрадь на виду.

Золотые правила безопасности в интернете

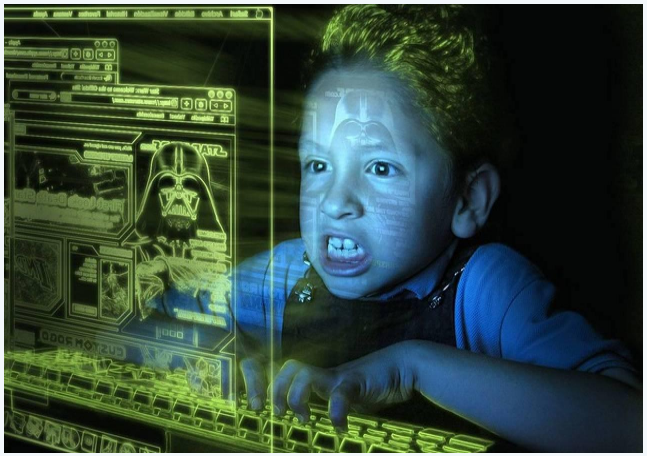
6. НАУЧИТЕСЬ СЕБЯ ЗАЩИЩАТЬ.

Если вдруг вас в социальной сети начинают забрасывать спамом, или заваливать комментариями или сообщениями такого характера, которые вам не по душе – то просто найдите кнопку «заблокировать пользователя»

Вам могут угрожать, вас могут шантажировать, над вами могут просто издеваться, вызывая вас на ответную агрессию. Это дело рук интернет троллей, которые получают от этого удовольствие и энергетическую подпитку своего жалкого Эго. Как и в реале, так и в виртуале – встречаются и плохие и хорошие люди. Обычно «достают» только спамеры. Поэтому, не забывайте про эти волшебные кнопки, которые есть везде: «Пожаловаться на спам», «Заблокировать пользователя».

Золотые правила безопасности в интернете

7. Какие ещё опасности могут подстерегать детей и школьников в Интернете?



Очень часто можно спокойно попасть на суицид-сайты. На этих сайтах могут так обработать сознание ребёнка, что он может не справившись с какой-либо проблемой психологического характера, свести счёты с жизнью.

И ему подскажут все способы ухода в иной мир. Это ужасно!!!

Золотые правила безопасности в интернете

7. Какие ещё опасности могут подстерегать детей и школьников в Интернете?

Следует боятся сайтов или форумов, где будет пропагандироваться польза наркотиков, сигарет и прочих вредных привычек. Не следует разрешать детям посещать сайты, на которых обсуждаются темы межнациональной розни, фашизма и также пропаганды порнографии. Подростка, как и взрослого человека могут «заманить» в различные секты. Взрослые должны контролировать школьника, чтобы он не засиживался за компьютерными играми, так как страшное понятие, как интернет зависимость к онлайн играм это в последнее время тяжелая болезнь психологического характера.

Иногда последствия бывают не предсказуемыми. Человек начинает путать виртуальную реальность с действительностью.

Золотые правила безопасности в интернете

8. НЕ ВЕРЬТЕ ТОМУ, ЧТО ЧИТАЕТЕ!

Если вы прочитали в интернете, что Алла Пугачёва вышла замуж за Барака Обаму, то прежде всего посмотрите, что это за сайт, который написал эту новость. Не относится ли он к «жёлтой прессе» или юмору.

Просто вбейте в поисковик этот запрос и прочитайте, что пишут об этом другие.

Так же не верьте первым попавшимся отзывам на какой-либо товар или продукт. Прочитайте несколько – всегда есть хорошие отзывы и нет. Проанализируйте, если покупка предстоит серьёзная. Часто комментарии бывают заказного характера.

Золотые правила безопасности в интернете

9. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.

Социальная инженерия – это такое понятие, которое можно охарактеризовать, как “взлом человеческого сознания”.

Это понятие относится к психологической манипуляции человеческого сознания, когда есть два человека: Жертва и Преступник.

Преступник вступает в контакт с жертвой и начинает его «вести», то есть, входя в доверие к вам – он может узнать про вас всё. Он не будет пытать вас раскалённым утюгом. Вы просто сами всё ему расскажите – потому что доверяете ему. Вы дадите ему пароль от сайта и аккаунта, вы дадите номер кредитки и пароль от неё. Есть и другие способы – например –звонки, якобы из отдела банка, с просьбой срочно поменять пароль и для этого надо сообщить данные и много других методов.

Времена, когда вирусы писали ради спортивного интереса, уже прошли и сегодня весь хакерский инструментарий используется ради получения коммерческой выгоды.

Вирусы могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество. В наше время получил распространение ФИШИНГ - создание поддельных сайтов — копирующих сайты известных фирм, сервисов, банков. Их цель — заманить Вас на такой поддельный сайт разными способами, чтобы украсть данные Вашего аккаунта (логин и пароль), которые Вы обычно вводите на странице настоящего сайта.


Я ИМЕЮ ПРАВО
НА БЕЗОПАСНЫЙ
ИНТЕРНЕТ

https://padlet-uploads.storage.googleapis.com/57906428/719e98f2249c81f8e4f2776edae2bc65fe38203b/24c7604651c9efb71bbd4a65501ebde9.jpg