Согласовано:
Протокол педагогического Совета
Протокол № 2 от 04.10.2021 г.

Гришина Анна Владимировна
Подписано цифровой подписью: Гришина Анна Владимировна
Дата: 2021.10.08 13:59:10 +05'00'

Приложение 3
Утверждено:
Директор МБОУ «СОШ № 146 г. Челябинска»
_____ А.В. Гришина
Приказ № 82.1-О от 04.10.2021 г.

Правила по безопасной работе в сети Интернет
В МБОУ «СОШ № 146 г. Челябинска»

1. Используйте нетривиальные пароли и контрольные вопросы.
2. Не используйте один и тот же пароль на все свои ресурсы.
3. Старайтесь не оставлять свой e-mail на разных сайтах.
4. Не переходите по ссылкам, которые приходят с письмами в вашу почту.
5. Любые письма, связанные с деньгами и перерегистрациями где-либо, должны вызывать повышенную осторожность.
6. Не запускайте присланные почтой программы с расширением exe, com, bat, scr, pif, vbs.
7. Не открывайте присланные с почтой вложенные файлы от неизвестных отправителей.
8. Старайтесь не сохранять пароли доступа к ресурсам в браузерах.
9. Пользуйтесь «аналогами» популярных, программ.
10. Не злоупотребляйте «бесплатным» софтом в Интернете,
11. Используйте эффективный антивирус.
12. Не ставьте на компьютере более одного антивируса.
13. Периодически делайте резервную копию самой ценной для вас информации.

Комментарии по правилам безопасности:

1. *Используйте нетривиальные пароли и контрольные вопросы,* когда открываете собственный электронный почтовый ящик или аккаунт на ресурсе в сети (блоги, ресурсные сайты).

Помните, что существует список наиболее часто используемых слов для паролей, они известны и активно используются хакерами. Также не нужно поддаваться своему желанию придумать наиболее простой вопрос и ответ на него в системе регистрации. Помните, что, к примеру, имя вашей собачки не будет тайной, если сами же выложите его в собственный блог.

Советы: используйте пароли длиной не менее 6 символов, комбинируйте символы с цифрами; заведите дома блокнот, куда стоит записывать логины и пароли, чтобы не бояться их забыть.

2. *Не используйте один и torn же пароль на все свои ресурсы.*

Если хакер подобрал пароль к одному из ресурсов, где вы уже зарегистрированы, в случае одинаковых паролей ему станут доступны и другие ваши ресурсы.

3. *Старайтесь не оставлять свой e-mail на разных сайтах.*

Существуют специальные программы-роботы, которые сканируют сайты и собирают электронные адреса. Затем эти адреса попадают в базы данных и распространяются в среде спамеров, хакеров, которые обязательно начнут присылать вам письма. Чем меньше ваш электронный адрес появляется на разных сайтах, тем меньше нежелательной почты (спама) будете получать.

Советы: старайтесь избегать указывать электронный адрес; если адрес указать всё же необходимо, заведите для таких целей отдельный электронный адрес, к письмам на который будет изначально низкий уровень доверия; если ваш электронный адрес нужно опубликовать на каком-то сайте, но хотите избежать роботов-сборщиков, адрес можно разместить в виде картинки или использовать понятную для человека модификацию адреса: «ddd@домен.ру» можно записать как «ddd_собака_домен.ру».

4. *Не переходите по ссылкам, которые приходят с письмами в вашу почту.* Все приходящие письма можно разделить на следующие группы:

- Рекламный мусор (спам).
- Письма с вредоносным кодом (вирусы, трояны и т.д.).
- Письма-обманки (фишинг).
- Нужные письма с адресов, заслуживающих доверие. Задача хакеров заставить вас перейти по нужной им ссылке, где ваш компьютер будет атакован специально подготовленными программами.

Даже простой заход на сайт может заразить компьютер вредоносной программой.

Советы:

1. все незнакомые отправители - группа риска, что бы они ни писали;
2. старайтесь игнорировать любую «интересную» рекламу и странные обращения неизвестных, как будто человек давно с вами знаком или что-то о вас знает - чаще всего это делается чтобы привлечь внимание и заставить вас перейти по ссылке;
3. если всё же решили перейти по ссылке от неизвестного адресата, удостоверьтесь предварительно, что у вас работает антивирус;
4. если компьютер вашего знакомого заразился вредоносным кодом и начал самостоятельную рассылку писем по его списку знакомых (стал ботом, роботом), то вы наверняка получите письмо от бота с адреса знакомого. Важно обращать внимание на содержание и предложения перейти по ссылке, запустить что-то. Если сомневаетесь, лучше свяжитесь со знакомым и удостоверьтесь, что письмо отправлял именно он.
5. *Любые письма, связанные с деньгами и перерегистрациями где-либо, должны вызывать повышенную осторожность.*
6. *Не запускайте присланные почтой программы с расширением exe, com, hat, scr, pif, vbs.*

Уже давно стало нормой не посылать почтой такие программы, своеобразный этикет. Это связано с волной эпидемий вирусов и троянов, которые прошли в своё время. Так что, если вам прислали файл с расширением exe, com или иным вышеуказанным расширением - смело удаляйте письмо. Если вы этого не сделаете, то почти наверняка будете заражены каким-либо вредоносным кодом, либо ваш компьютер превратится в бот.

Компьютеры-боты часто используются хакерами в атаках на разные ресурсы в Интернете. К примеру, обычный домашний компьютер может быть использован как один из множества таких же для атаки па серверы Пентагона, и при этом владелец компьютера не будет даже догадываться об этом.

7. *Не открывайте присланные с почтой вложенные файлы, особенно от неизвестных отправителей.*

Любые вложенные в письмо файлы, особенно от незнакомых адресатов - зона риска. Зачастую файлы, кажущиеся картинками или архивами в письме, на самом деле являются исполняемыми программами (прячут расширения, используют привычные иконки и уязвимости в операционной системе, браузерах, почтовых программах). Поэтому, прежде чем открыть присланный файл, стоит серьёзно задуматься об уровне доверия к адресату, содержанию письма.

Совет: если всё же принято решение открывать, перед тем как сделать это, присланный в электронной почте файл лучше всего предварительно сохранить на компьютере, проверить антивирусом.

8. *Старайтесь не сохранять пароли доступа к ресурсам в браузерах.*

Если пользуетесь компьютером, к которому имеете доступ не только вы, ни в коем случае не сохраняйте пароли при входе в почту или какой-то другой важный ресурс. Пароль может быть сохранён системой для постоянного входа и ваша почта, редактирование записей блога или ещё что-нибудь в этом роде станут доступны другим пользователям компьютера. Особенно это касается интернет-кафе и интернет-клубов. В таких местах не забывайте: при входе в свой почтовый ящик ставить галочку «чужой компьютер»; после просмотра почты выйти из почтового ящика (нажать ссылку «Выход»).

9. *Пользуйтесь «аналогами» популярных программ.*

Любое программное обеспечение имеет свои ошибки и «непродуманности». Этим часто пользуются хакеры и вирусописатели. Естественно, чтобы достичь максимального эффекта в своих нехороших делах, в первую очередь вредоносный код пишется для самых распространённых программ: операционные системы MS Windows, браузеры Internet Explorer, почтовые программы, пейджер ICQ,

Для того чтобы усложнить задачу хакерам, старайтесь не использовать стандартный софт, пользуйтесь аналогами. Приведем простые примеры:

- браузеры - Opera, Mozilla, FireFox и т. д.;
- пейджеры, совместимые с ICQ - QIP, Triilian и т.д.;
- почтовые программы - Mozilla Thunderbird, The Bat и т. д.

Для пользователей ОС Windows актуально постоянно обновлять систему через Интернет, поскольку уязвимости в системе обнаруживаются постоянно, заплатки к ним выходят также постоянно.

10. *Не злоупотребляйте «бесплатным» софтом в Интернете.*

Вспомним хорошую пословицу: «Бесплатный сыр бывает только в мышеловке». Не будем заблуждаться, что в Интернете много самаритян (хотя есть и такие) - основная масса «бесплатно» выложенного софта на варезных сайтах заражены вредоносным кодом, который зачастую даже не детектируется антивирусами.

Варез (англ., warez — сленговая версия «wares», сокращённого множественного числа от «software» — «программное обеспечение») — программа, распространяемая незаконным путём с нарушением прав автора. Часто содержит изменения и/или дополнения, позволяющие использовать её бесплатно. Это классика троянских коней - запускаете одно, а параллельно запускается другое. После установки такого софта на компьютер, специальная подпрограмма, дописанная к тому, что было нужно, вполне может:

- собрать логины и пароли доступа в Интернет, доступа к почте и сайтам, отправить всё это хакерам-авторам вредоносного кода или их заказчикам;
- превратить компьютер в рассадник вирусов или бот, который будет незаметно для вас управляться извне, рассылать письма, отправлять SMS-ки или сообщения в ICQ;
- перехватить управление компьютером на себя.

Практика показывает, что сайты с пиратскими серийными номерами и «вскрывалками» в большинстве своём пытаются заразить своих посетителей ещё на стадии входа на сам сайт.

11. *Используйте эффективный антивирус.*

Каждый специалист обязательно предложит вам свой вариант «лучшего» антивируса. Не стоит опираться на это, поскольку у каждого специалиста своё субъективное мнение, свой опыт. Поэтому при выборе антивируса стоит обратить внимание на результаты независимых тестов. Такие тесты проводятся периодически, среди них наибольшим авторитетом пользуется Virus Bulletin. Для тех, кто не хочет копаться в технических тонкостях, резюмируем: первую тройку в тестах обычно занимают антивирусы Eset NOD32, Symantec Norton Antivirus и Антивирус Касперского.

12. *Не ставьте на компьютере более одного антивируса.*

Периодически у некоторых возникает идея установить на своём компьютере 2 и более антивируса, чтобы максимально повысить свою защиту. Это не только не повышает эффективность, но и мешает установленным антивирусам работать и даже может привести к критическому сбою всей системы. Кроме того, при двух и более антивирусах нагрузка на систему увеличивается, что серьёзно сказывается на работоспособности компьютера.

13. *Периодически делайте резервную копию самой ценной для вас информации.*

Если всё же вирус попал на ваш компьютер, или же «рухнула» система, сгорел компьютер, заблокировали доступ к ресурсам злобные хакеры, украли ноутбук или произошло что-нибудь ещё - поможет резервная копия самого необходимого, которую нужно периодически записывать на внешние носители информации (CD, DVD, Flash-memory и т. д.). Частоту создания резервных копий каждый определяет для себя сам, в зависимости от ценности той информации, которая хранится на компьютере. Можно делать резервную копию как вручную (выбирая нужные файлы и копируя их на внешний носитель), так и через специально предназначенные для этого программы. Такой программой является Acronis True Image. Она позволяет собирать архивы не только из отдельных файлов, папок и разделов диска, но и сохранять только настройки отдельных приложений. Например, этой программой можно сохранить только саму почту и настройки почтовой программы MS Outlook.