

Библиотечный урок «Безопасность в сети интернет»

**Какие опасности подстерегают
нас в интернете?**

Как этих опасностей избежать?

- Всемирный день безопасного Интернета отмечается ежегодно во второй вторник февраля. В 2020 году он приходится на 11 февраля. Это международный праздник. В торжествах участвуют деятели общественных организаций и фондов, официальные лица и представители правительства, сотрудники компаний сферы информационной безопасности, работники учреждений, которые защищают личные данные и борются с вредоносными программами.
- Цель праздника – информировать людей об ответственном и безопасном использовании Интернета.

История праздника.

- Всемирный день безопасного Интернета возник в январе 2004 года. Его инициатором выступила Европейская Комиссия. В России Всемирный день безопасного Интернета впервые прошел в 2005 году.
 - **Традиции праздника**
 - Ежегодно назначается тема Всемирного дня безопасного Интернета. Она касается актуальных проблем в сфере защиты пользователей Сети и внедрения новых программ. В этот день проходят образовательные акции, проводятся конференции и семинары. Участники общественных организаций рассказывают о способах защиты личных данных. Презентуются проекты повышения безопасности, памятки и правила пользования глобальной сетью Интернет. На телевидении транслируют тематические программы и фильмы.
 - В России к празднику приурочивают акцию «Неделя безопасного Рунета». В это время проходят форумы, круглые столы, конференции, на которых эксперты обсуждают вопросы угрозы в Сети, защиты от вредоносных программ, киберзависимости.
-



Преступники в интернете.

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ.

- Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера.
 - Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.
-



Вредоносные программы.

- А) Никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла.
 - Б) Скачивайте файлы из надежных источников и обязательно читайте предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности.
 - В) Регулярно устанавливайте на компьютере последние обновления безопасности и антивирусные средства.
-

Интернет-мошенничество и хищение данных с кредитной карты

- А) Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.
- Б) Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют многие банки в России.



Азартные игры.

- Помните, что нельзя играть на деньги. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей/выигрышей



Онлайн пиратство.

Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать.



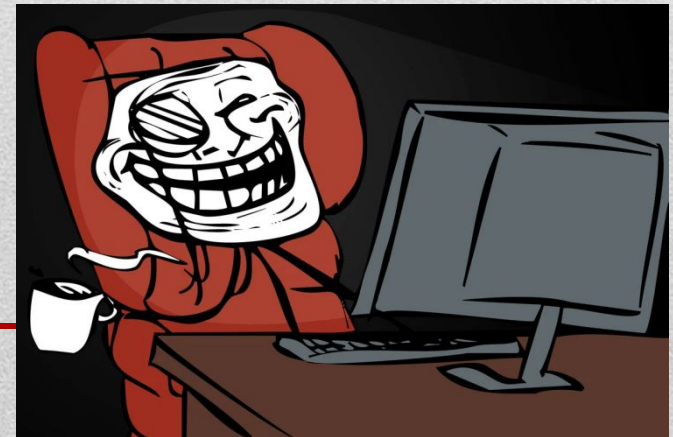
Интернет-дневники.

- Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения. Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверяйте, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

Интернет-хулиганство.

Хейтеры- это люди, которые сознательно или бессознательно производят негативный контент или допускают отдельные негативные высказывания в отношении конкретного человека или конкретного явления.

- Игнорируйте таких хулиганов. Если вы не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.



Недостоверная информация.

- Всегда проверяйте собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ – газетам, журналам и книгам.
-

Материалы **нежелательного** **содержания.**


- Используйте средства фильтрации нежелательного материала (например, MSN Premium'sParentalControls или встроенные в InternetExplorer®). Научитесь критически относиться к содержанию онлайн-материалов и не доверять им.
-

Викторина



**Какие существуют опасности при
работе в сети?**

- широкая торговля базами данных о частных лицах и предприятиях
 - кража личной информации об абонентах мобильных сетей
 - нарушение законодательства об охране авторских прав
 - одна из важных проблем - вирусы
 - спам - это различные рекламные объявления, которые приходят по электронной почте, забивая ящик и мешая загружать нормальные письма
-



Какие существуют средства профилактики и борьбы с опасностями при работе в сети?

- чтобы обезопасить себя, необходимо пользоваться антивирусными программами
 - не следует загружать программы с сайтов, не заслуживающих доверия
 - если в тексте сайта множество грамматических ошибок, и весь он забит рекламными баннерами, то загрузка с такого сайта может быть чревата последствиями
 - не открывайте подозрительных писем от неизвестных вам авторов
 - осторожно относитесь к адресу своего ящика вводите свой e-mail только в том случае, если он гарантирует вашу конфиденциальность
 - заведите два почтовых ящика: адрес одного говорите только друзьям и знакомым, а для регистрации в Интернете, пишите адрес второго.
 -
-

**Какие правонарушения,
связанные с работой в сети
вам известны?**

- **РАСПРОСТРАНЕНИЕ ЭКСТЕМИСТСКИХ МАТЕРИАЛОВ В СЕТИ ИНТЕРЕТ**
- **ПРОПАГАНДА, НЕЗАКОННАЯ РЕКЛАМА НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ**
- **КЛЕВЕТА В СЕТИ ИНТЕРНЕТ**
- **МОШЕННИЧЕСТВО, СВЯЗАННОЕ С БЛОКИРОВАНИЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРОВ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ**
- **ХИЩЕНИЯ, СОВЕРШАЕМЫЕ С ПОМОЩЬЮ СЕТИ ИНТЕРНЕТ И КОМПЬЮТЕРНОЙ ТЕХНИКИ**
- **РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И СВЕДЕНИЙ О ЧАСТНОЙ ЖИЗНИ В СЕТИ ИНТЕРНЕТ**
- ~~• **НАРУШЕНИЕ АВТОРСКИХ ПРАВ В СЕТИ ИНТЕРНЕТ**~~

**Кто назовёт больше правил
этикета в интернете?**

- Обращаться к незнакомым людям можно при условии, что адрес был опубликован его владельцем.
 - К незнакомым людям можно обращаться с просьбами о консультации и вежливыми предложениями, не претендуя на получение ответа. Если ответ не пришел, повторять обращение не следует.
 - При обращении к незнакомым людям надо воздерживаться от просьб использовать другие средства связи, например, выслать по почте автограф. Такие просьбы оставляют без ответа, а повторение рассматривают как спам.
 - Отправляемое электронное письмо всегда должно быть подписано и указана тема сообщения.
 - Если у вас нет возможности сразу ответить на полученное письмо, сообщите, что вы его получили и ответите позже.
 - Не забудьте ответить позже, не затягивайте с ответом.
 - Будьте вежливы, не отправляйте *флеймов*- написанных в запале писем.
 - Шутки принято обозначать явным образом при помощи смайликов: ©, ®, и др.
 - В тексте сообщения не принято выделять текст прописными БУКВАМИ. Такое выделение рассматривается как крик. В лучшем случае - как неграмотность в вопросах этикета.
 - Большие файлы-вложения нужно архивировать. А для обмена очень большими файлами есть другие способы.
 - Нельзя посылать рекламу в не предназначенные для этого места. Это грубое нарушение.
 - Нельзя посылать незатребованную корреспонденцию. Это тоже нарушение этикета.
-

**Какие профессии служат
для сохранения
информации,
регулирования её
использования?**

- системный администратор, модератор, криптограф.
 - **Криптогра́фия** (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта).
-

Клавиатурный шпион – это:

- Агент спецслужб, в служебные обязанности которого входит просмотр переписки пользователей
 - Сотрудник, ведущий протокол собраний и набирающий текст сразу на клавиатуре удаленно подключенной к компьютеру
 - Программа, отслеживающая ввод пользователем паролей и пин-кодов
 - Юридический термин, используемый для обозначения правонарушений, связанных с информационной безопасностью
-

Какую цель преследует такая угроза как фишинг?

- Перенаправлять любые запросы пользователя в браузере на хакерский сайт о рыбалке.
 - Довести пользователя до самоубийства путем постоянного вывода сообщения «купи рыбу!»
 - Обманным путем выудить у пользователя данные, позволяющие получить доступ к его учетным записям
-

Троянская программа опасна тем, что:

- Проникает на компьютер под видом полезной программы и выполняет вредоносные действия без ведома пользователя
 - Ищет на диске какого-то коня, снижая производительность системы
 - Постоянно читает вслух «Илиаду» Гомера без выражения
 - Обладает всеми вышеперечисленными возможностями.
-

Как определить, что ваш компьютер заражен?

- Друзья получают от вас по электронной почте сообщения, которых вы не посылали
 - Компьютер часто зависает либо программы начинают выполняться медленнее обычного
 - На диске исчезают или изменяют название файлы и папки
 - Компьютер издает неожиданные звуки, воспроизводимые в случайном порядке
 - Все вышеперечисленное
-

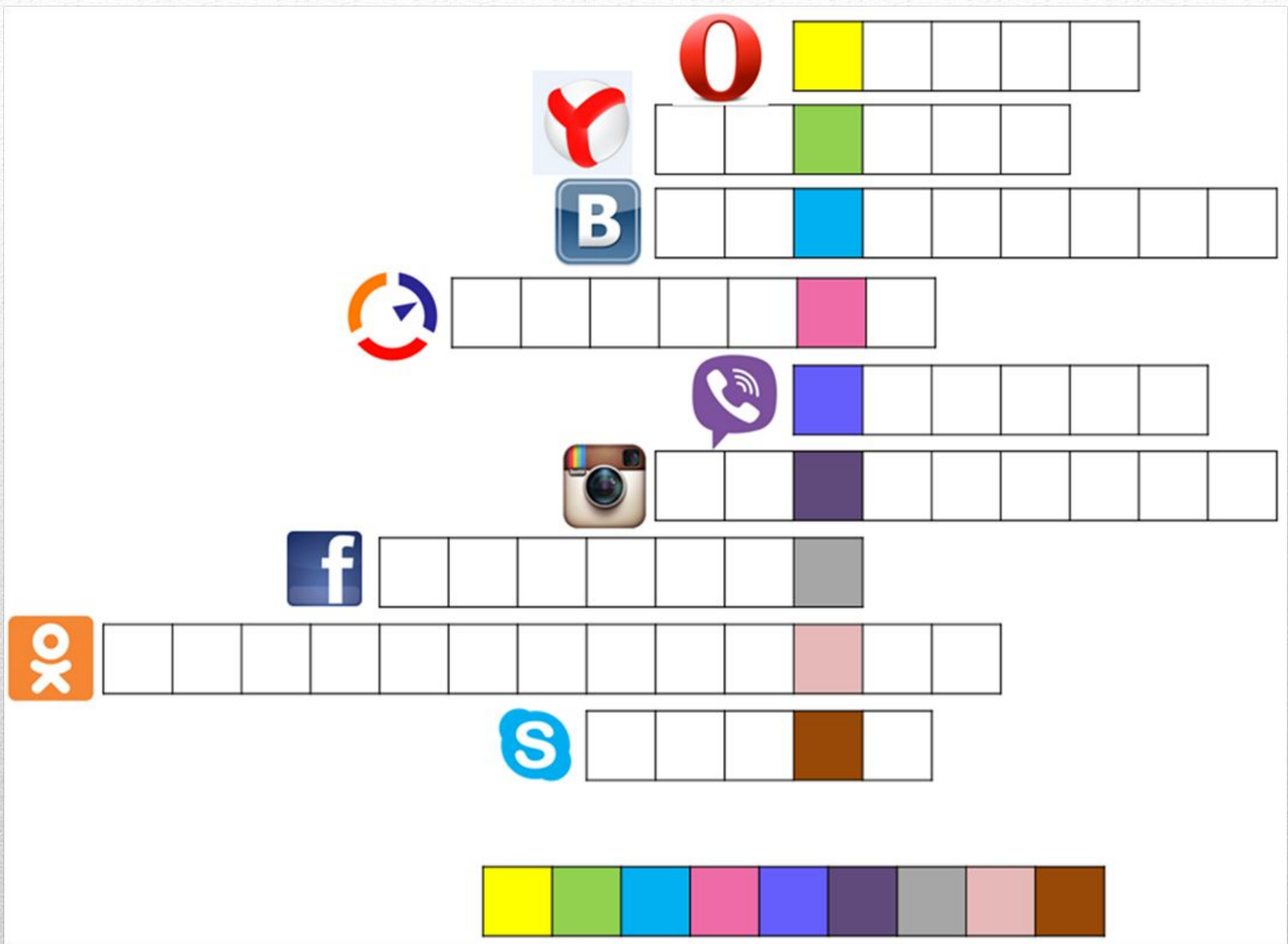
Что нужно сделать в первую очередь, если компьютер подвергся атаке?

- Сделать несколько глубоких вдохов и принять витамины
 - Вызвать милицию и скорую помощь, в особенно сложных случаях еще и пожарных
 - Отключить компьютер от интернета
 - Выключить до приезда специалистов монитор
-



Всемирная сеть стала неотъемлемой частью жизни в развитых и развивающихся странах. В течение пяти лет Интернет достиг аудитории свыше 50 миллионов пользователей. Другим средствам коммуникации требовалось гораздо больше времени для достижения такой популярности. Например, телевидению потребовалось 13 лет, радио – 38 лет. А с 22 января 2010 года прямой доступ в Интернет получил даже экипаж Международной космической станции.

Оказывается, русский писатель, философ и общественный деятель 19 века * в романе «4338-й год», написанном в 1837 году, похоже, первым предсказал появление современных блогов и Интернета: в тексте романа есть строки: «между знакомыми домами устроены магнетические телеграфы, посредством которых живущие на далёком расстоянии общаются друг с другом». Заполните кроссворд и узнайте фамилию этого философа.**





Спасибо за внимание!
