Урок
по интернет-безопасности
"Семь простых привычек на пути к безопасному Интернету"
в 4-х классах
МБОУ СОШ № 111
г.Новосибирска

Учителя:
Прохорова А.А.
Щетинина М.А.
30.10.2014 г.

1. Полюбите обновления

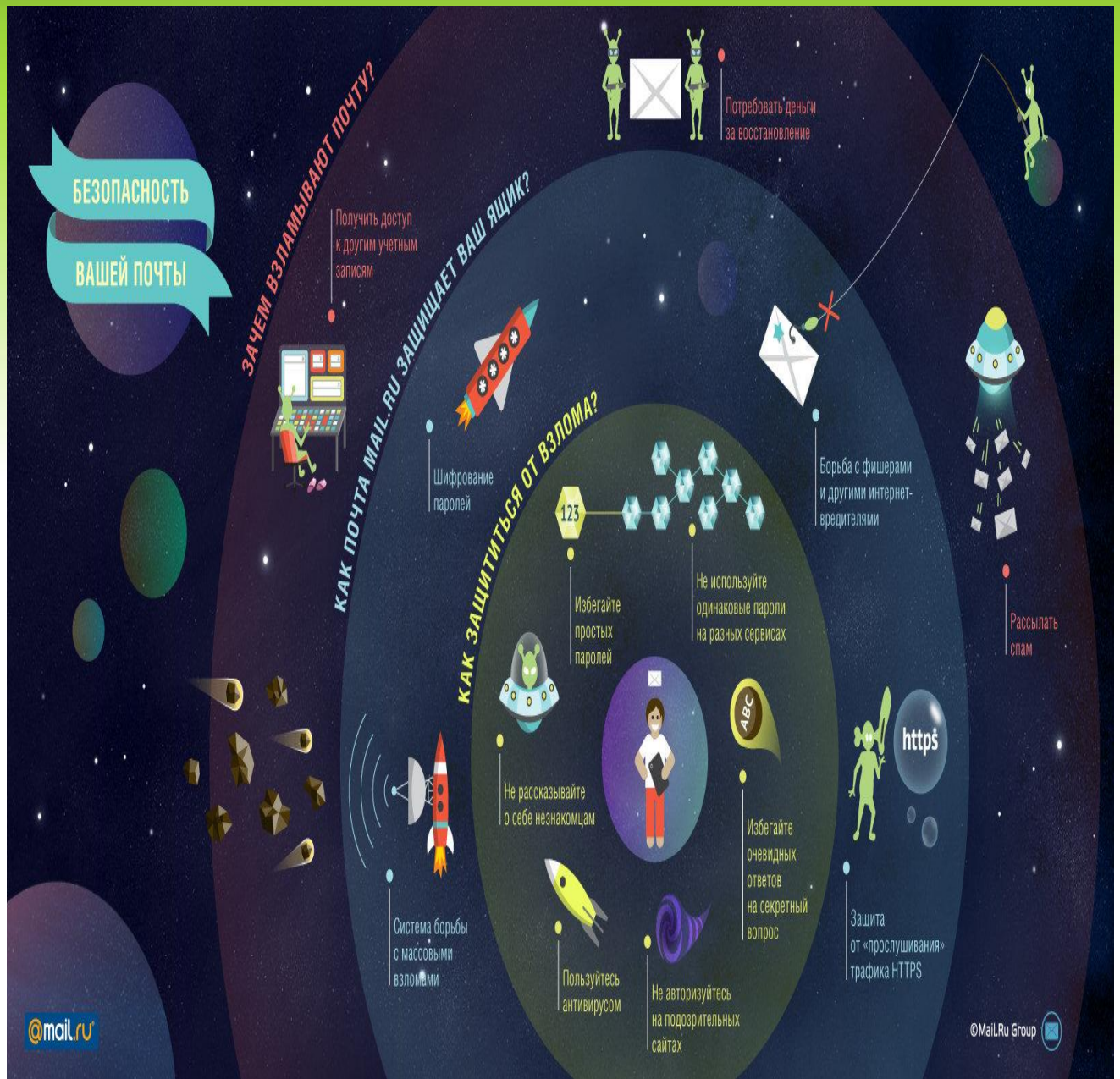
Включите автоматическое обновление во всех приложениях, которыми пользуетесь повседневно. Прежде всего это операционная система, веб-браузер, клиенты обмена почтой и сообщениями. Также это касается программы просмотра PDF, воспроизведения Flash и Java. Это надо сделать один раз, займет процедура три минуты, а защищенность вашего компьютера от разного рода вирусов и других вредоносных приложений возрастет очень заметно.

2. Соблюдайте правила сетевой гигиены

Точно так же, как вы не начнете есть, не помыв руки, не стоит приступать к работе на «грязном» компьютере. Если речь о собственной машине, в числе первых установленных на ней программ должен быть надежный, современный антивирус. А лучше — комплексная защита класса Internet Security. Когда приходится работать на чужом компьютере, неплохо проверить в самом начале, работает ли на нем антивирус, когда выпускались антивирусные базы и когда запускалась последняя проверка. Если давно — потратьте пять минут на сканирование, перед тем как вводить свои ценные пароли к рабочей почте, онлайн-банку и социальной сети. А вдруг клавиатурный шпион сразу отправит их злоумышленникам?

3. Смартфон тоже компьютер

Повторяйте это чаще. Важно не само признание смартфона компьютером, а понимание того, что на нем тоже запускаются программы и некоторые из них — вредоносные. Поэтому все меры защиты — обновления, антивирус, запрет установки сомнительных программ — так же актуальны на смартфоне, как и на компьютере. Преимущество комплексной защиты смартфона еще и в том, что она защищает не только от вирусов, но и от спама,



4. Опасные ссылки

Вообще-то веб-ссылки придумали, чтобы упростить жизнь пользователя. Одно касание — и ты на нужном сайте. Увы, этим блестяще пользуются злодеи, заманивая доверчивых пользователей на сайты, распространяющие зловредный софт или выманивающие платежные данные. Вывод — не стоит тренировать зоркость, пытаясь отличить «хорошую» ссылку от плохой. Если в почте, сообщении социальной сети или SMS вам пришла ссылка — не нажимайте, если только сами не просили, чтобы вам ее прислали. Простой пример — банк прислал важное оповещение и предлагает прочитать его на сайте. Не жмите на ссылку, откройте браузер и зайдите в онлайн-банк, введя адрес сайта вручную.

5. Заведите менеджер паролей

Вы быстро устанете запоминать пароли к десяткам сайтов, которые требуют регистрации. И все закончится тем, что везде будете применять один и тот же пароль. Кстати, самый популярный пароль прошлого года — «123456». Чтобы не пополнять своим взломанным аккаунтом печальную сетевую статистику, поставьте себе приложение, которое само создает пароли к разным сайтам, само их «подставляет» в браузер, а хранит пароли в зашифрованной базе. И вам действительно надо помнить всего один пароль — к этой базе. Кстати, стандартный «хранитель паролей» из браузера на эту роль не советуем — в половине популярных браузеров все сохраненные пароли легко прочитать без каких-либо технических ухищрений.

6. Научитесь жаловаться

- **Интернет-угрозы — это не только вирусы и мошенники. Ничуть не менее приятны грубияны, провокаторы, сетевые «тролли». Особенно тяжело приходится детям и подросткам, они часто не умеют ни эффективно противостоять словесным атакам, ни спокойно проходить мимо. Переходить на личности и вспоминать, кто чью маму в каких обстоятельствах узнал, совсем не обязательно. Почти в любой социальной сети, форуме или чате есть кнопка «Заблокировать пользователя», а также кнопки «Пожаловаться на спам» и «Пожаловаться на оскорбление». Ими нужно пользоваться без лишних колебаний — первым делом жалуемся на оскорбительный комментарий, вторым — блокируем атакующего, чтобы не читать его дальнейших излияний. То же касается случаев, когда вам напоказ вывешивается откровенно провокационный контент, будь то насилие, пропаганда наркотиков или**

7. Говорите с родителями

Все вышеописанные правила просты, но они часто неочевидны самым неопытным пользователям Сети — детям и пожилым людям. Поэтому все перечисленное им нужно пересказывать много раз. Кроме правил «компьютерной гигиены», которые помогают защититься от вредоносных приложений и мошенничества, хорошо бы привить им мысль о том, что в Интернете очень часто пишут неправду. Как правило, не со зла, а по неосведомленности, но это не меняет дела — информацию надо тщательно проверять. Достаточно задать нужный вопрос «Яндексу» или Google, чтобы первые же ссылки дали ответ — правда ли, что Барак Обама разводится, помогает ли оциллококцинум при гриппе и давно ли маленькому ребенку на самом деле нужна была донорская кровь (подобные сообщения о поисках донора часто «путешествуют» в соцсетях месяцами.

Это просто

- **Регулярно повышайте уровень компьютерной грамотности:**
- Используйте удобные возможности повышения уровня компьютерной и интернет-грамотности, например, посещение курсов, чтение специальной литературы, консультации с экспертами.
- Знакомьте всех членов вашей семьи с базовыми принципами безопасной работы на компьютере и в Интернете.
- Горячая линия помощи при возникновении угроз в интернете:

  8 800 25 000 15

Желаем удачи!!!

Материал взят с сайтов:

- digit.ru
- newsland.com
- helpline@detionline.com
- www.mlg.ru
- blog.kaspersky.ru
- http://www.odnoklassniki.ru
- http://festival.1september.ru