

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



Работу выполнила:
ученица 11 А
МБУ «Школы №62»
г.о Тольятти
Азизова Тамара

Как защитить собственную информацию от несанкционированного доступа, или как не попасть впросак!



Приятного ознакомления!
Надеюсь, в моей презентации Вы
почерпнете для себя что-то новое
или хотя бы поднимете себе
настроение ☺



- Какого-какого доступа?...

От несанкционированного. Несанкционированный доступ, уважаемый читатель, это чтение, изменение, разрушение и прочее шаманство с Вашей информацией без Вашего ведома.

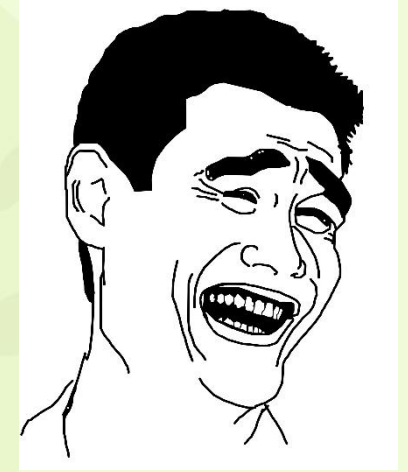


Такой доступ можно осуществить с помощью чужого имени, изменения физических адресов устройств, модификаций программного и информационного обеспечения, хищения носителя информации, установки аппаратуры записи и многого-многого другого – как видно, арсенал у людей, охочих до чужой информации, весьма и весьма обширный... и впечатляющий, нельзя не признать этого.



- Пф, да со мной никогда такого не случится!

...сказал очередной ПК-юзер. Подумать только, какое огромное множество людей, придерживаясь такой позиции, совершенно не заботится о безопасности своих данных, и в результате рядовые пользователи навлекают на себя беды.



Однако, даже при впечатляющем наборе средств, имеющемся у злоумышленников, мы можем помешать им завладеть тем, что предназначено уж точно не для них!



- Хорошо, я поверил... А что я, обычный пользователь, могу потерять?

Конечно, не всякий пользователь – это продвинутый бизнесмен\директор компании\руководитель отдела, который использует Облачное хранилище и т.п как склад документов предельной важности (порой – и секретности) – тогда ущерб был бы гораздо очевиднее и серьезнее.



Однако Вам, уважаемый пользователь прежде всего Всемирной Паутины (в большинстве своем, опасности в виде вирусов, ворующих данные, приходят как раз оттуда) тоже есть что терять. Это Ваши логины и пароли от страниц соцсетей, электронных почт, аккаунтов информационно-развлекательных сайтов – завладев ими, злоумышленник может накурлесить от Вашего имени такого, что честь восстанавливать придется еще очень долго.

- Боже-Господи! Звучит ужасно! Что мне нужно сделать, чтобы защитить свою информацию?!

Для начала успокойтесь и не паникуйте. Вы можете принять ряд мер, уделив при этом вопросу безопасности всего полчаса своего драгоценного времени. Итак, по пунктам:

1) Неспроста много раз повторяют: при регистрации придумывайте сложные пароли! Вирусная программа «Брутфорс» - наиболее частая виновница хищения паролей - за секунду разгадает твой «12345» или «qwerty», зато с «VragamNeSdaetsyaNashGordiyVaryag1029» она изрядно помучается! Ах да, при наборе пароля можете пользоваться экранной клавиатурой. Это тоже своего рода защитная мера.

Ну, попытка - не пытка 😊



KASPERSKY
SECURE PASSWORD CHECK

⚠ НЕ ВВОДИТЕ НАСТОЯЩИЙ ПАРОЛЬ. ЭТОТ СЕРВИС ПРЕДНАЗНАЧЕН ТОЛЬКО ДЛЯ ОЗНАКОМИТЕЛЬНЫХ ЦЕЛЕЙ - KASPERSKY LAB НЕ СОБИРАЕТ И НЕ ХРАНИТ ВАШИ ПАРОЛИ.

qwerty12345 *

⚠ Распространённый пароль или слово

Для подбора вашего пароля на обычном компьютере потребуется

1 СЕКУНДА

Ой! Ваш пароль взломают быстрее, чем вы скажете "Ой!"



KASPERSKY
SECURE PASSWORD CHECK

⚠ НЕ ВВОДИТЕ НАСТОЯЩИЙ ПАРОЛЬ. ЭТОТ СЕРВИС ПРЕДНАЗНАЧЕН ТОЛЬКО ДЛЯ ОЗНАКОМИТЕЛЬНЫХ ЦЕЛЕЙ - KASPERSKY LAB НЕ СОБИРАЕТ И НЕ ХРАНИТ ВАШИ ПАРОЛИ.

JeSdaetsyaNashGordiyVaryag1029 *

⚠ Распространённый пароль или слово ⚠ Простые последовательности символов

Для подбора вашего пароля на обычном компьютере потребуется

10000+ ВЕКОВ

Бендер Родригез успеет спереть все сущее в этой галактике, включая ваш пароль

Использовался <https://blog.kaspersky.ru/password-check/>

2) Порадуйте компьютер установкой Антивируса, а Антивирус – регулярным обновлением антивирусных баз. Однако установка – это только пол дела: не поленитесь почитать инструкции от других, опытных пользователей и настройте программу под себя. Регулярно проводите проверку компьютера!

Широкий выбор!



3) Избегайте сомнительных сайтов и не скачивайте неизвестные вам программы. В некоторых поисковиках появляются сообщения «Сайт может угрожать безопасности вашего **компьютера**». Не искушайте судьбу, не заходите на эти сайты. Кроме того, не посещайте сайты, адреса которых приходят к вам на электронную почту (лучшее вообще игнорировать такие письма, не открывая их). Будьте бдительны! **TRUST NO ONE!**

4) Ограничьте доступ к вашему компьютеру. Блокировка входа в компьютер посредством пароля оградит от доступа к Вашей информации. Хранить пароль необходимо в недоступном для непосвященных месте.



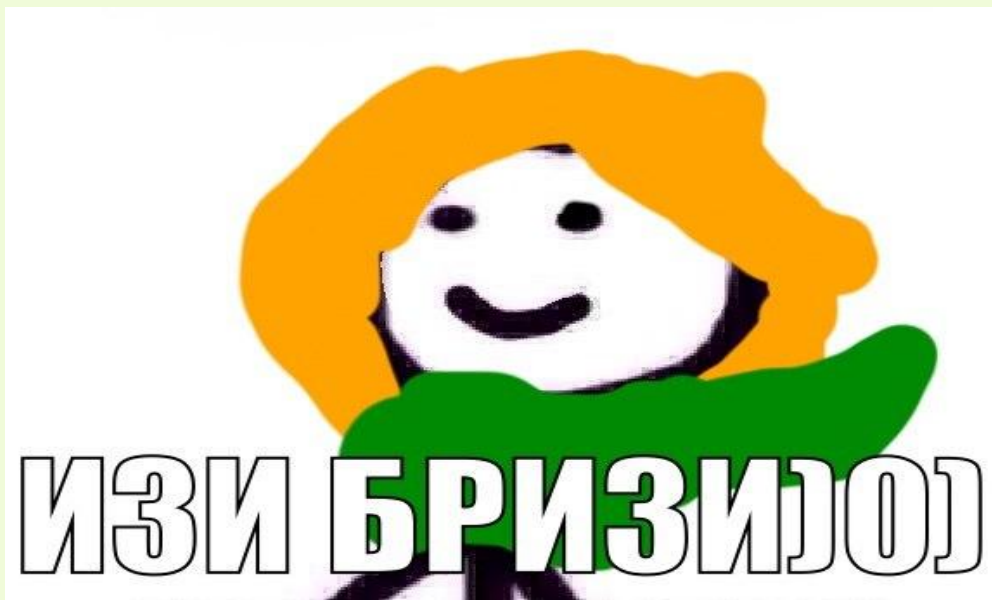
Надежнее ящика Пандоры места не найти! Никто не позарится на Ваши данные, гарантированно ☺



- И что, это... все?

Рядовому пользователю вроде нас с Вами этого хватит с лихвой!

Теперь Вы сами убедились, что защитить свой компьютер и информацию на нем **ОЧЕНЬ ПРОСТО!**



Однако если Вам и с этим не хочется повозиться, могу посоветовать только одно средство... Оно очень дорогостоящее, но так же и очень действенное...



Интрига раскрывается в следующей серии... Тьфу, в следующем слайде!



А НАЙМИТЕ ПЕНТАГОНЩИКА!



Вот он Вам
защиту
сделает, на
зависть всем 😊



СПАСИБО ЗА ВНИМАНИЕ!

ЗАЩИТИТЬ СВОИ ДАННЫЕ ПРОСТО!

До новых встреч
в интернете!



ИСПОЛЬЗУЕМЫЕ РЕСУРСЫ:

- <http://compsam.ru/uroki/login-i-paroli.html>
- <http://www.electrosad.ru/Jornal/avz.htm>
- <http://www.kakprosto.ru/>
- Яндекс картинки

