



Types of security

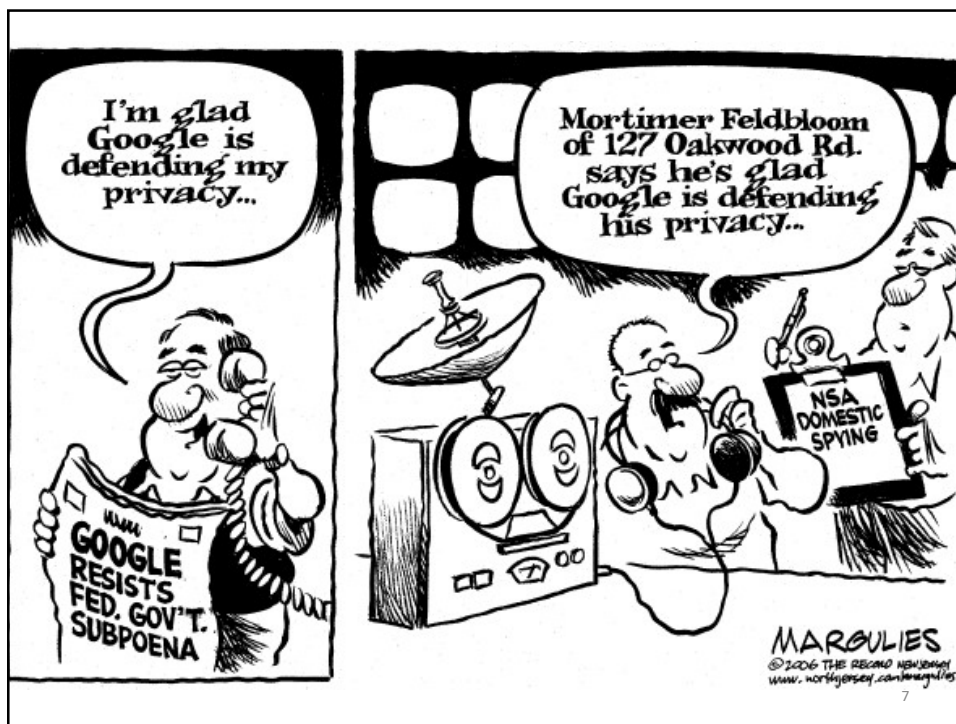
- Protect against outside attack or snooping
 - Use of open WiFi networks
- Protect you from consequences of doing something stupid
 - Be careful where you click!
 - Viruses, malicious programs and other malware
- Passwords
- Storing data safely – local or in cloud

3

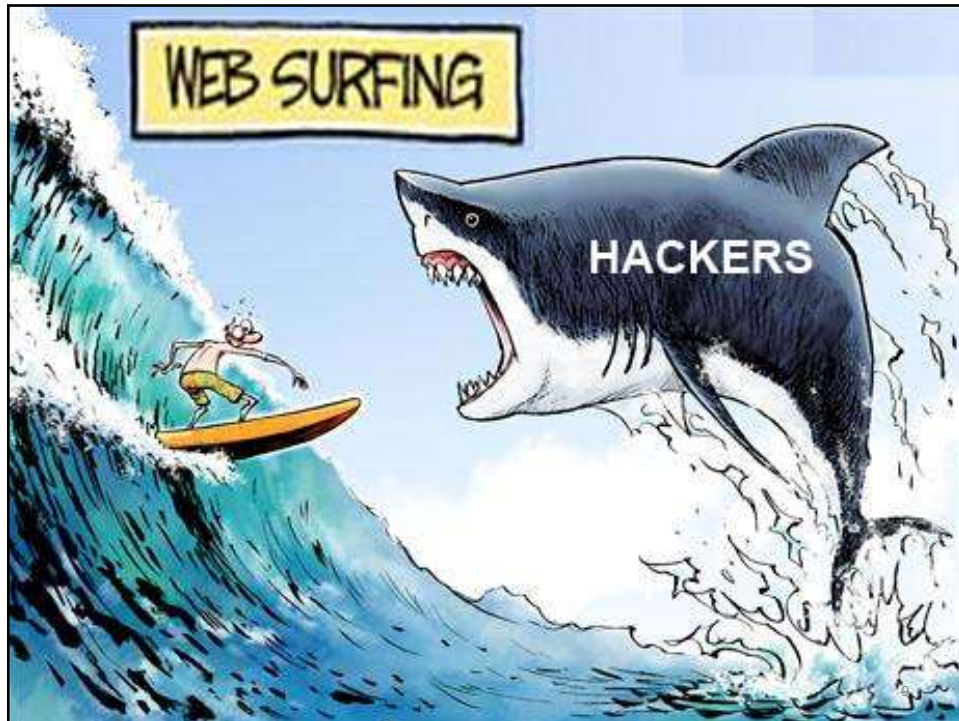
**Snooping
or
outside attack**

4





**Doing
something
stupid**



Michael's Security Add-ons

- EFF's HTTPS Everywhere (Chrome/Firefox)
 - <https://www.eff.org/https-everywhere>
- EFF's Privacy Badger (Chrome/Firefox)
 - <https://www.eff.org/privacybadger>
- For Firefox only:
 - Flashblock, <http://flashblock.mozdev.org/>
 - Noscript, <https://noscript.net/>

Michael's Security Add-ons



11

You installed what?!

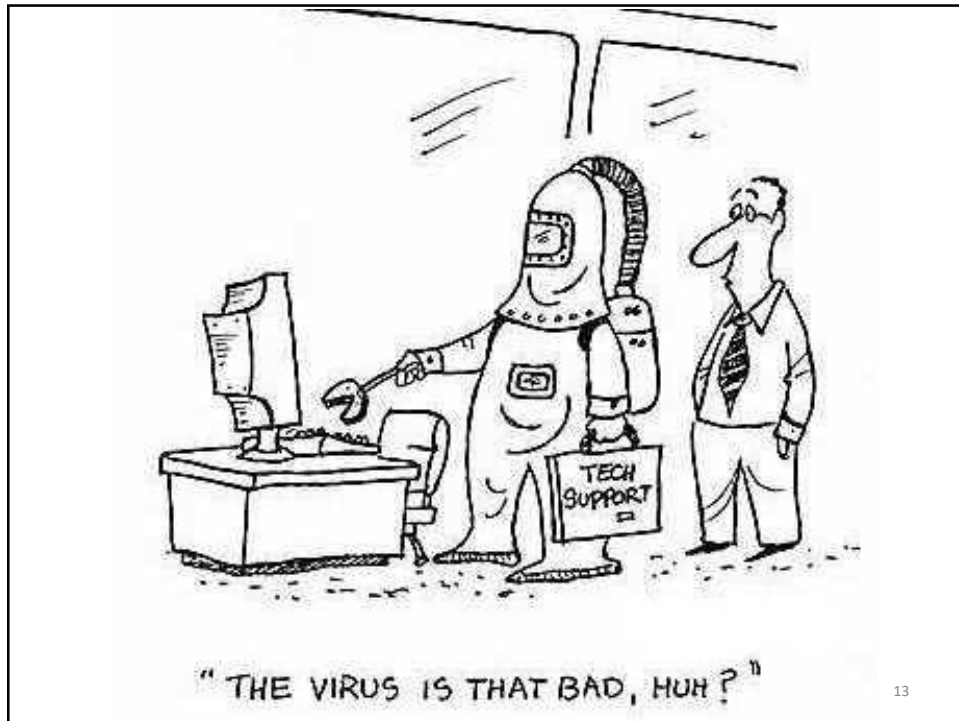


MALWARE

Don't open attachments or click links in emails from unknown or untrusted senders.

Never install dubious software and keep your malware prevention up to date.

12




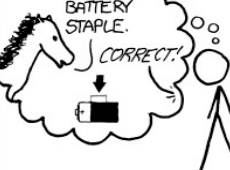
Passwords

15



16



<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STORED HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p>  <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p>  <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

19

Diceware

<http://world.std.com/~reinhold/diceware.html>





**Storing
data safely**

22

TRUST ME. OUR
SECURITY IS SO
GOOD EVEN YOU WON'T BE
ABLE TO ACCESS YOUR
OWN DATA!



23



Maybe it's time we introduced
a more formal backup strategy

24

Drive encryption

- **Bit Locker**
- **TrueCrypt**



25