Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Spletni Kung-Fu

Nekaj malega o varnosti in internetu...

... in kako pri tem ostati brez modrice na očesu...

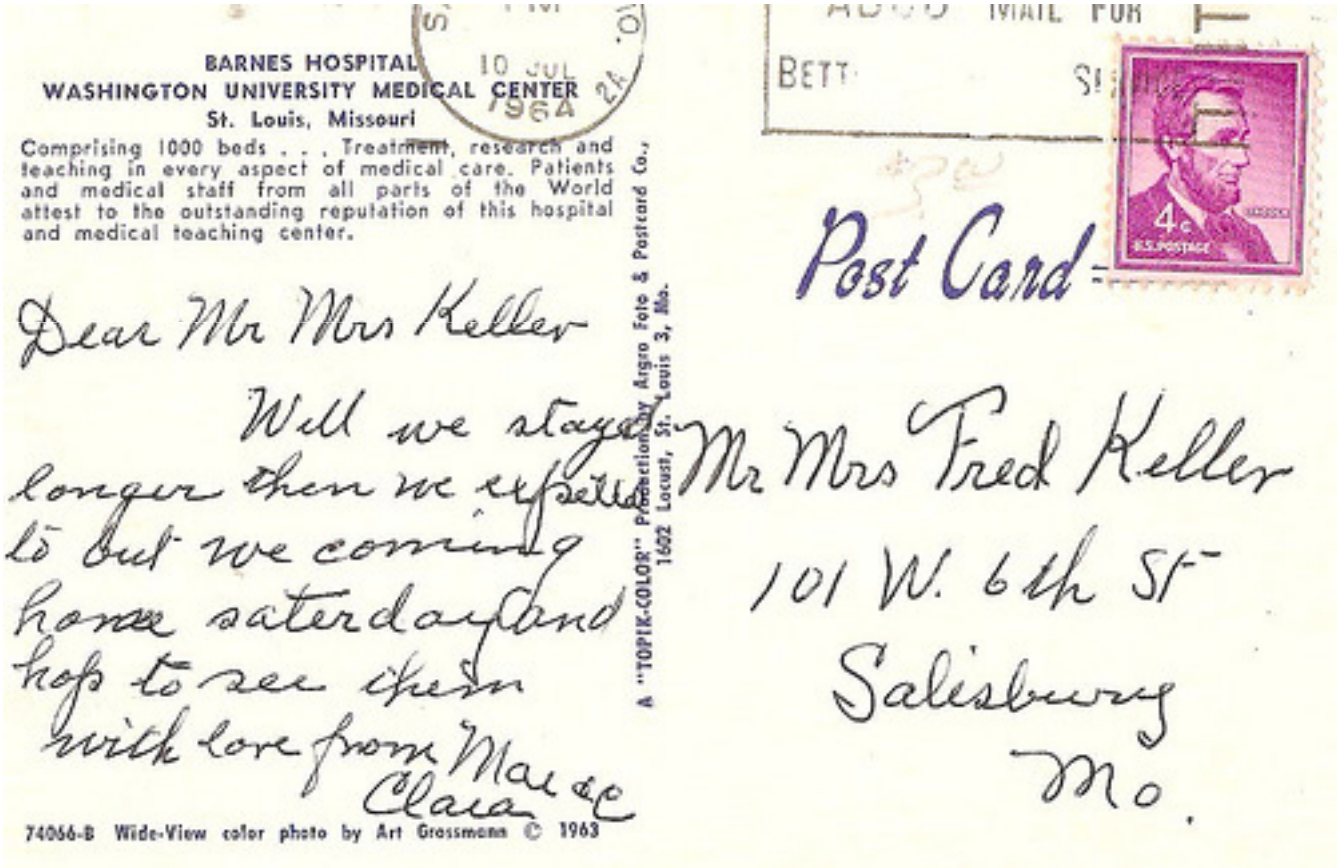
dr.Matjaž Pančur, LRK, FRI

http://movieoverdose.files.wordpress.com/2009/02/2008_kung_fu_panda_002.jpg

Uporabljate e-mail?

Elektronska pošta…?

....ali elektronska pošta?

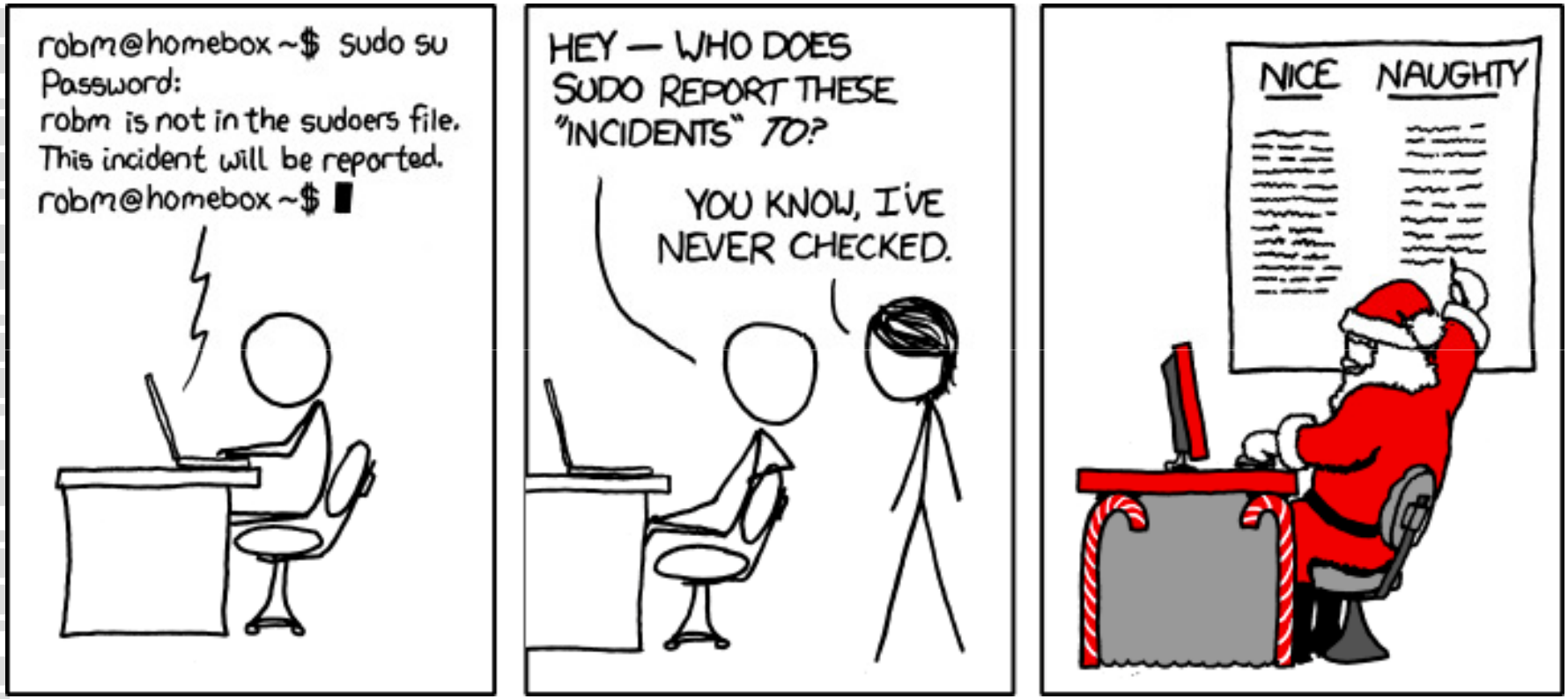


Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Demo

Lažna elektronska pošta

Huh…Dedek Mraz nas opazuje…?



http://xkcd.com/838/

Kaj pa Facebook?

Gmail?

Hotmail?
Live mail?
Twitter?

...

Ali mi lahko ukradejo moje geslo?

Kako pa sploh deluje internet?

http://www.icis.com/blogs/asian-chemical-connections/confused.jpg

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

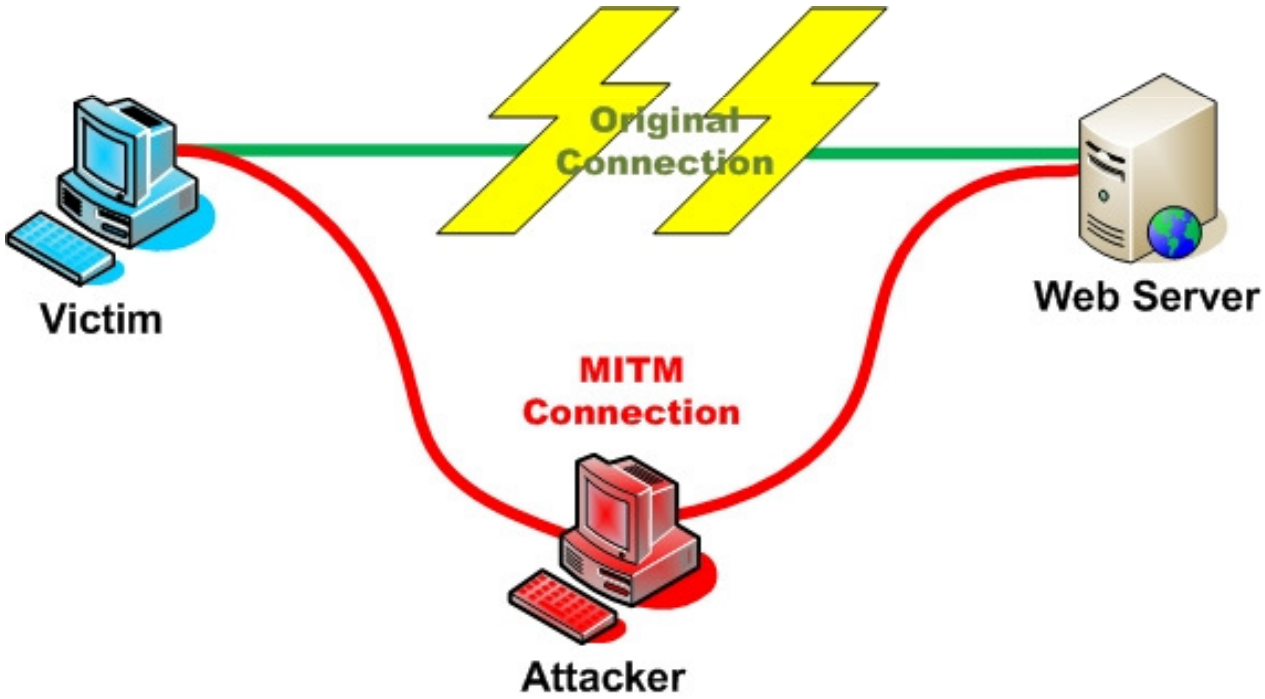
Film – Spletni bojevniki

… ogled žal brez kokic … :(

Warriors of the Net - www.warriorsofthe.net ali Youtube

Kako mi lahko ukradejo moje geslo?

Vrinjeni napadalec (MITM)



https://www.owasp.org/index.php/Man-in-the-middle_attack

Kako deluje protokol ARP

(huh…žal bo tole malo bolj tehnično… če zaspite, vas bom zbudil čez par minut, ko bo na vrsti demo)

ARP zastrupljanje

http://diazno.typepad.com/blog/2009/11/poisonous-apple-lol.html

Demo

Arp zastrupljanje + sslstrip + Facebook

Gesla so kot zobne ščetke!

Redno jih menjajte in nikoli ne posojajte.

10 najpogostejših gesel v VB

- 123
- password
- liverpool (nogomet!)
- letmein (sezam odpri se)
- 123456
- qwerty
- charlie
- monkey
- arsenal (spet nogomet)
- thomas (2. najpogostejse ime)

V neki aplikaciji s 100.000 uporabniki v Sloveniji…

- ljubezen
- krneki
- 123456
- slovenija
- SONCEK
- ljubljana
- pikica
- cokolada
- zvezdica
- pikapolonica

KAKŠNA SO VARNA SPLETNA GESLA?

Pri svojih spletnih aktivnostih (e-pošta, MSN, družabna omrežja, forumi, blogi ...) uporabljaj varna gesla, ki naj bodo skrivnost. Pogosto jih spreminjaj. Za gesla ne uporabljaj osebnih podatkov (svojega imena, rojstnega datuma, imena psa ...).

KAKO LAHKO SVOJE GESLO OHRANIŠ VARNO?

- Svoje geslo ohrani skrito in ga ne posreduj drugim osebam (tudi najboljšim prijateljem ne).
- Ob najmanjšem sumu, da je za tvoje geslo izvedel nekdo drug, ga nemudoma zamenjaj.
- Zlorabo svojega gesla oz. krajo identitete takoj prijavi skrbniku spletne strani, kjer se ti je to zgodilo!
- Nasvet, kako si lažje zapomniš svoje geslo, ki sicer izgleda nelogično: »Dbk3rp« - Danes bom kupil 3 rdeče paradižnike.
- Priporočamo ti, da svoj e-poštni naslov raje opišeš, namesto da ga v celoti objaviš na internetu. Tako si zagotoviš, da ga ne bodo prebrali in uporabili pošiljatelji spama oz. nezaželene pošte.

Primer: zvezda.danica@mojmail.com = zvezda pika danica at mojmail pika com

www.safe.si

Za dodatne informacije vam je na voljo **www.safe.si!**

Brezžična omrežja

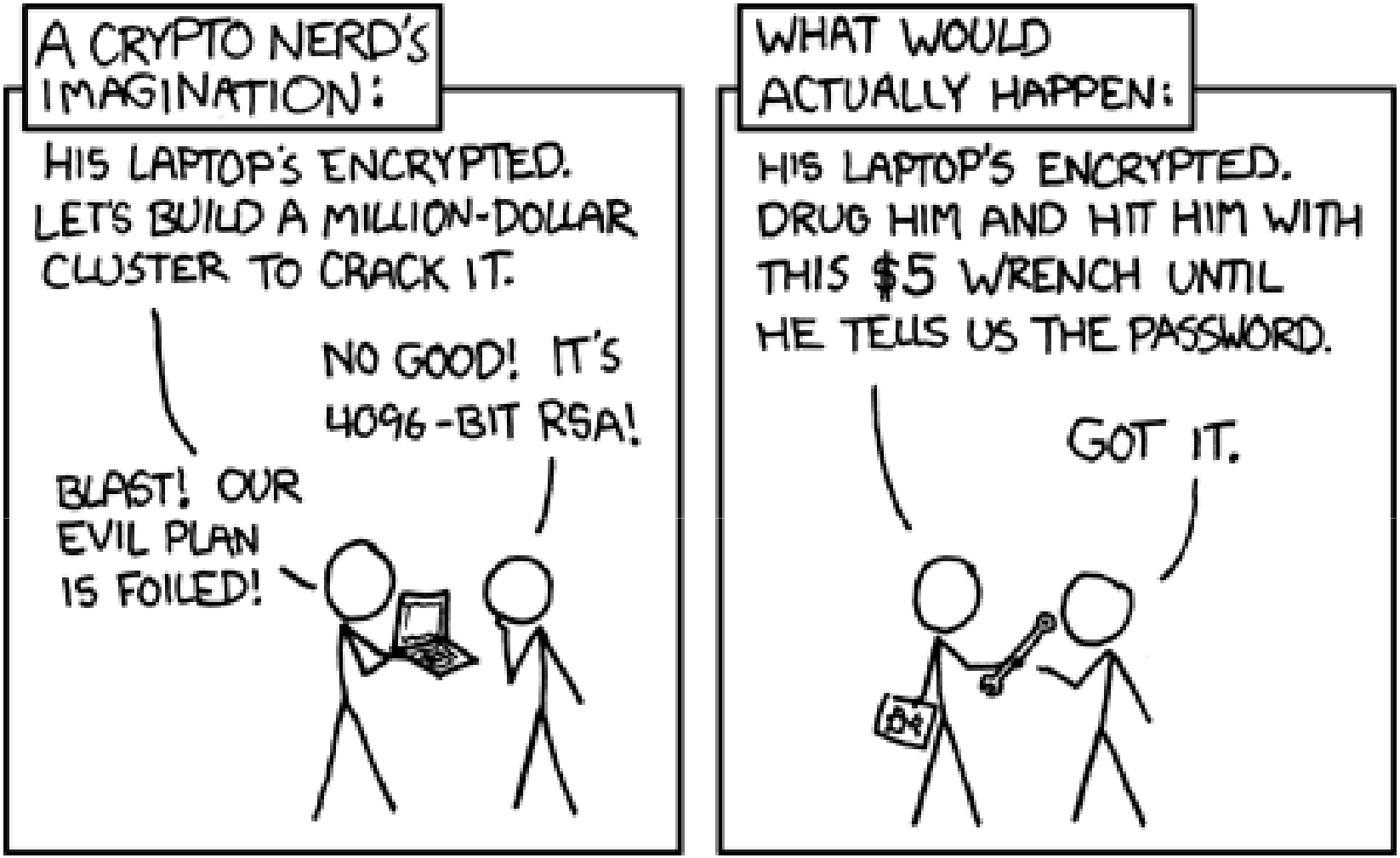
- Izbor gesla za vašo dostopno točko
- Če je geslo šibko, se ga lahko hitro ugane

Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Demo – slabo geslo za dostopno točko

Uganjevanje s pomočjo najpogostejših gesel

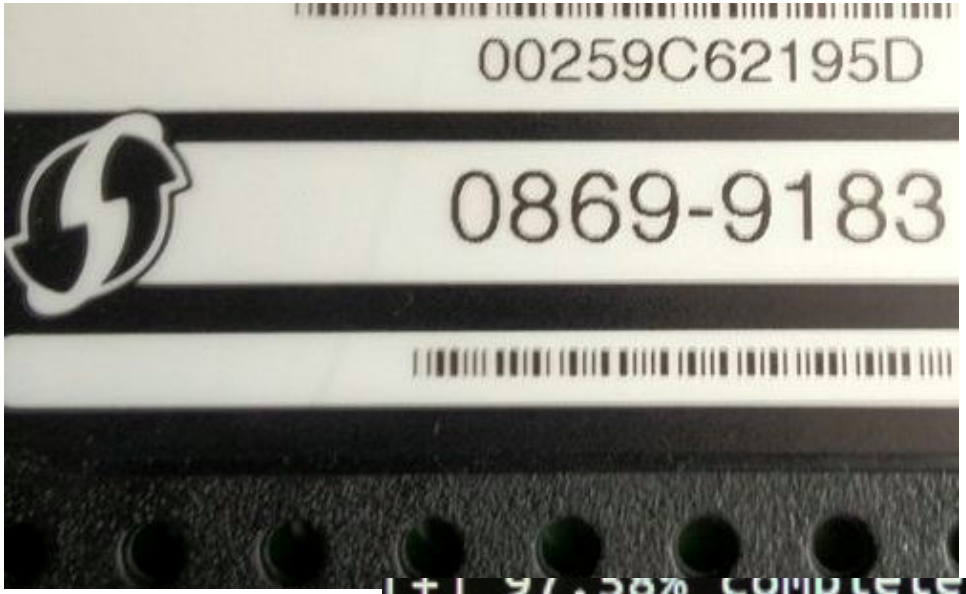
Torej nam bodo dobra gesla in šifriranje rešilo vse probleme?



http://xkcd.com/538/

Brezžična WiFi omrežja

- Reaver – najnovejši napad na WPS (WiFi Protected Setup), star manj kot mesec dni (zadnje dni leta 2011)
- WPS - enostavno nastavljanje WPA2 šifriranja s PIN številko
- Napaka v implementaciji PIN protokola – preizkusiti je potrebno samo 11 000 kombinacij –> napad s poskušanjem traja 4-6 ur
- V nekaterih WiFi dostopnih točkah **NE MORETE** izklopiti WPS funkcionalnosti…




```
[+] 97.63% complete @ 19 seconds/attempt
[+] 97.67% complete @ 19 seconds/attempt
[+] 97.72% complete @ 19 seconds/attempt
[+] 97.76% complete @ 19 seconds/attempt
[+] 97.81% complete @ 18 seconds/attempt
[+] 97.85% complete @ 18 seconds/attempt
[+] 97.90% complete @ 18 seconds/attempt
[+] WPS PIN: '08699183'
[+] WPA PSK: '[redacted]'
[+] AP SSID: 'gallaghernet'
sean@sean-Satellite-A135:~$
```

http://arstechnica.com/business/news/2012/01/hands-on-hacking-wifi-protected-setup-with-reaver.ars

...ampak na take poceni finte pa ja padejo samo neuki uporabniki...

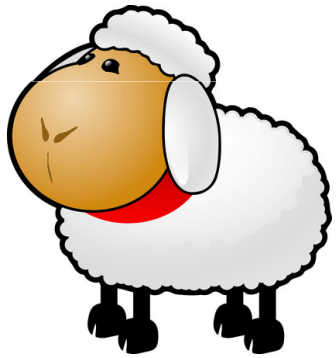
(...in potem svizec zavije čokolado...)

Zid ovc (Wall of sheep) – DEFCON konferenca


Wall
of
Sheep


WALL OF SHEEP
Cisco Network Engineer
I am now a sheep ! ! !
Announcements:
01.) Wall of Sheep 2008, this year we even have the best from Harvard ! ! !
02.) Roland is our new special friend and we do not fear Serle.
03.) Have any short funny mpeg movies? We want them!
04.) www.digitalwolves.net
05.) These sheep should have listened to the fans...
06.) Mr Jdog... not good enough for even the wall...
07.) Ok... ICQ is not secure.
08.) KT... your phone is not very badass.
09.) Does anyone have a passive captive ehly ethernet cable... see us.

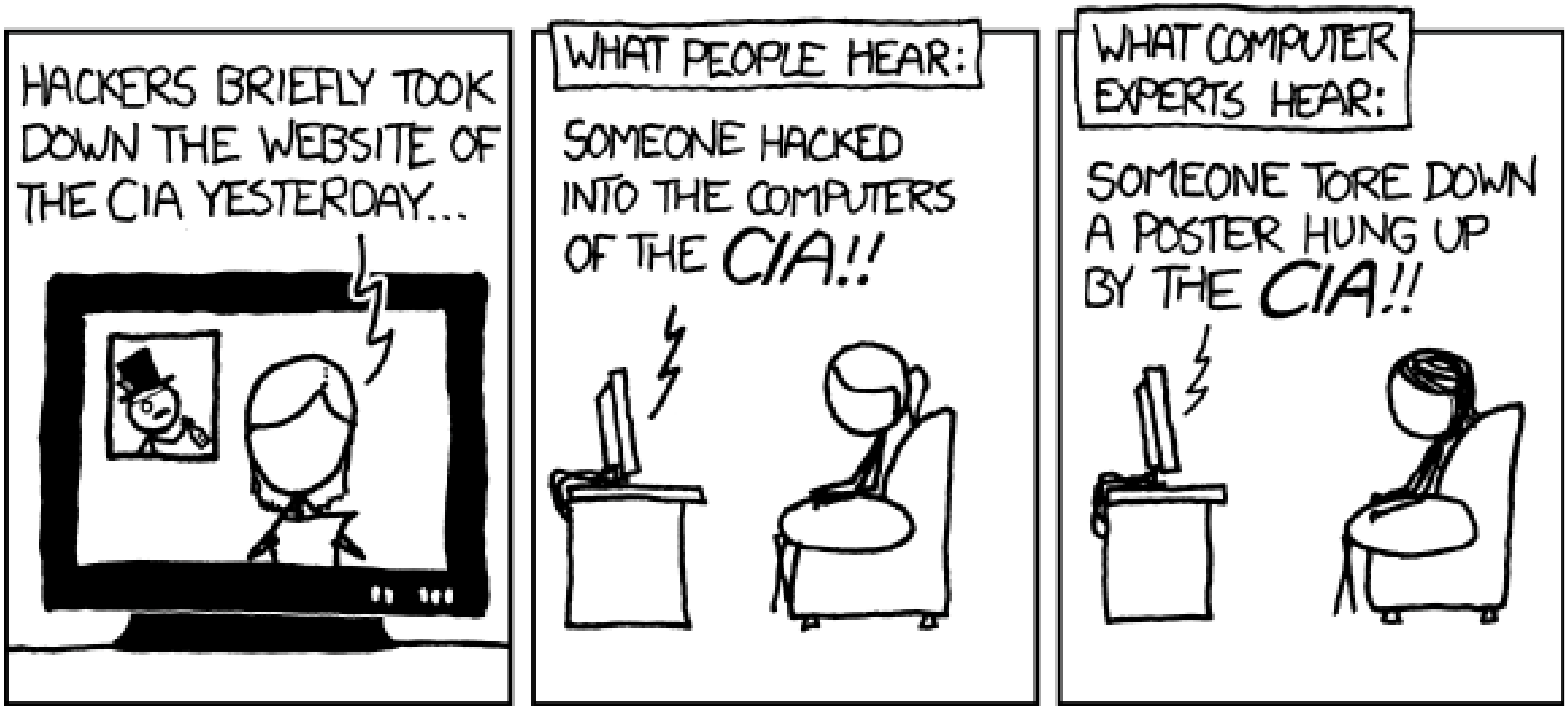
Ne bodite ovce… preberite si o varnem obnašanju na internetu… Toplo priporočamo, še posebej ob mrzlih zimskih večerih :)



- http://www.safe.si
- http://www.cert.si/
- http://www.varninainternetu.si/

Računalniško izobražene ovce gledamo na novice o “vdorih” malo drugače kot ostale ovce…

CIA



http://xkcd.com/932/

Vprašanja?