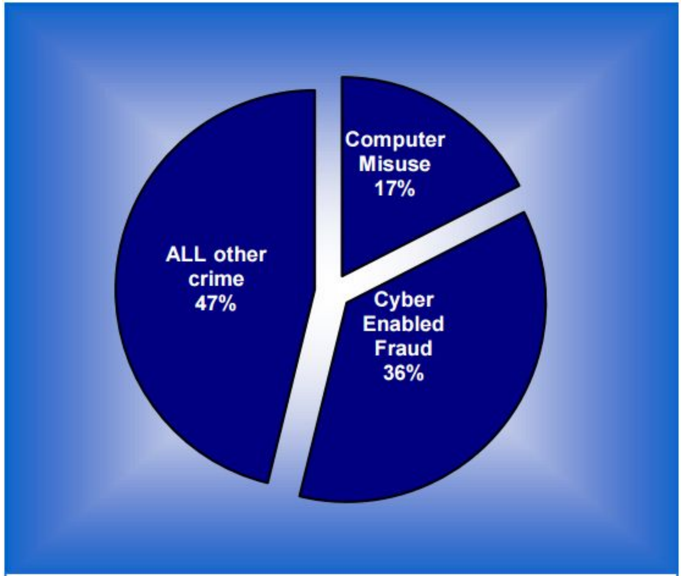
Security Trends of 2016

By Maydha M., Neha M. and Krishna P.

Security Trends of 2016

- The 2016 Internet Organised Crime Threat Assessment **(IOCTA)** reported a continuing and increasing acceleration of the security trends observed in previous assessments

- In some countries cybercrime has surpassed traditional crime in terms of reporting



Cyber Crime as a proportion of total UK crime in 2015 (Source: ONS)

Some of the biggest trends in cybercrime during 2016 were:

- Child exploitation
- Mobile device threats
- Social engineering

Child exploitation

What:

The use of the internet as a platform for predators to communicate, store/share child sexual exploitation material **(CSEM)** and to hunt for new victims

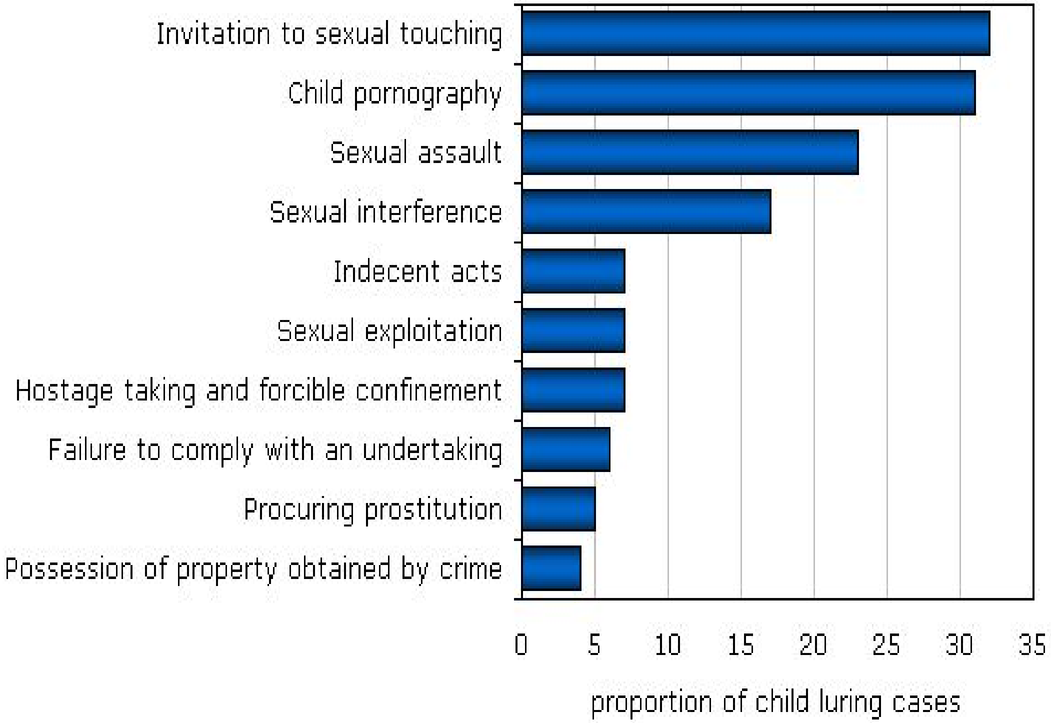
Why:

Sexual purposes and/or financial motives

Child exploitation

How - Using manipulative tactics over different online platforms and making use of the following over the internet:

- Social networks
- Online games and forums
- The liberty of being anonymous
- P2P networks
- Darknet
- Live Streaming



2016 case - Ontario man accused of cyber sex abuse

- Ontario medical student, Marco Viscomi, was alleged to have forced two American teenage sisters to engage in sexual and violent acts while he watched via Skype

- Used live streaming which is facilitated by end-to-end encrypted platforms **(E2EE)**

- Not even the service providers can access what is being shared amongst their users

New figures obtained by the NSPCC reveal that the internet was used to commit an average of eight sexual crimes against children each day in the past year, including rapes, grooming and live streaming of abuse

Child exploitation

SOLUTION?...

- Strengthen the current cyber security measures
- Early detection, blocking and removal of CSEM online

….However, this is a problem that cannot be combatted with cyber safety measures alone

- The development of preventive campaigns to raise awareness and providing children with tools to protect themselves are essential

Mobile device threat

What: Physical and software based threats that can compromise the data on smart phones, tablets and similar mobile devices

Why:

People often carry sensitive information on their cell phones including banking apps, payment informations, personal pictures, etc. This becomes a motive for hackers to do mobile attacks

TOP THREATS TARGETING MOBILE DEVICES

DATA INTEGRITY THREATS

- Attempts to corrupt or modify data
- Purpose is to disrupt operations of an enterpris or for financial gain
- Can also occur unin-tentionally

Courtesy: Syma

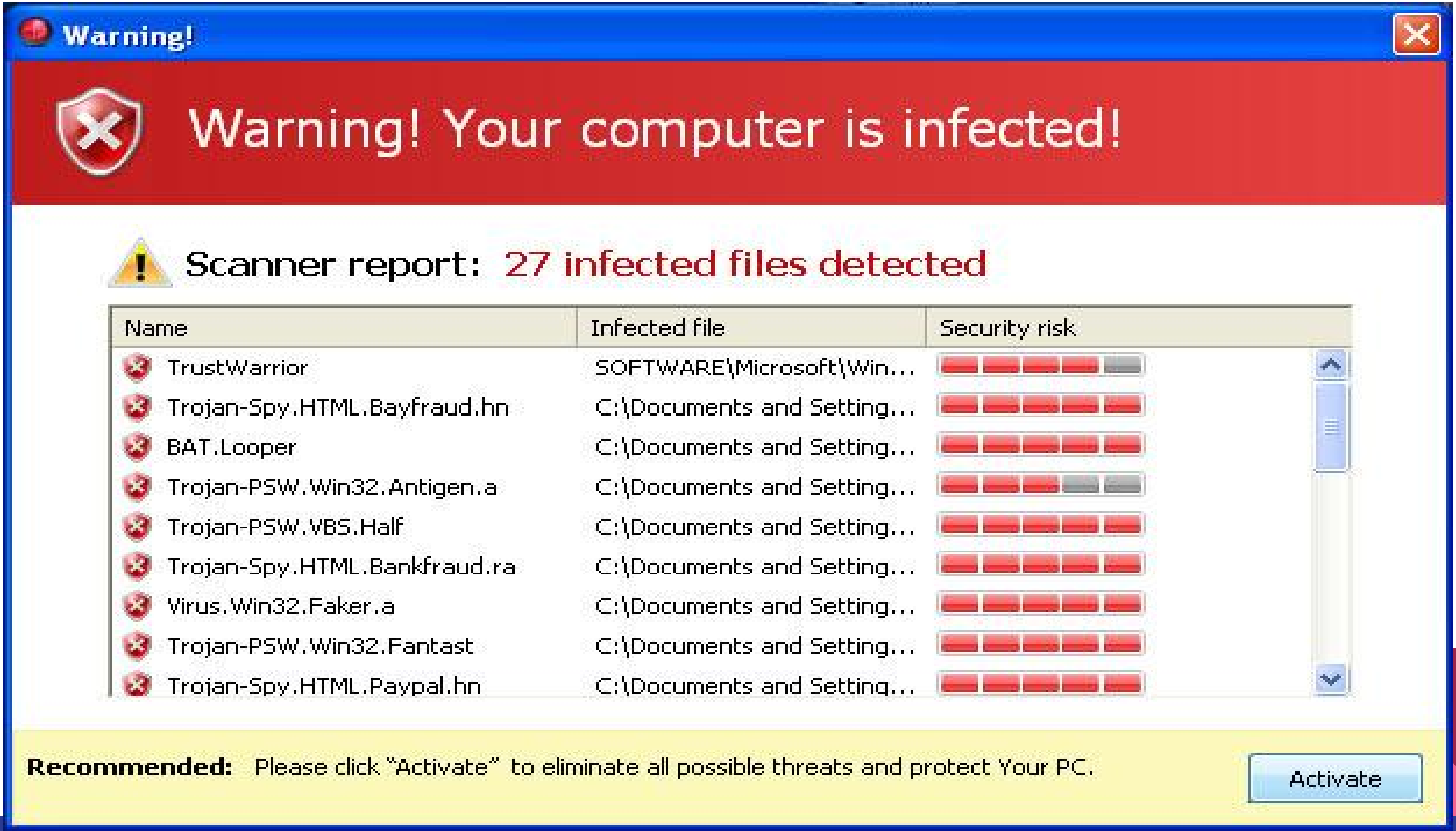
Mobile devices threats

How:

- Malware injection - the act of inserting malicious code into a vulnerable web server page with poor application input filtering
- Mobile phishing and ransomware - using mobile apps and SMS text messages to take advantage of human behavior and trust to gain access to data or infiltrate businesses
- Cryptocurrency mining attacks - the malware infiltrates mobile devices in search of digital currencies, like Bitcoin, Litecoin and Dogecoin

2016 case - Shedun

- In mid 2016, arstechnica reported that approximately 10,000,000 devices would be infected by this malware
- Classified as "**aggressive adware**" for installing potentially unwanted program applications and serving ads
- Once downloaded, the application generates revenue by serving ads
- Auto-roots the android using well-known exploits like ExynosAbuse, Memexploit and Framaroot
- Not even a factory can remove the malware from infected devices

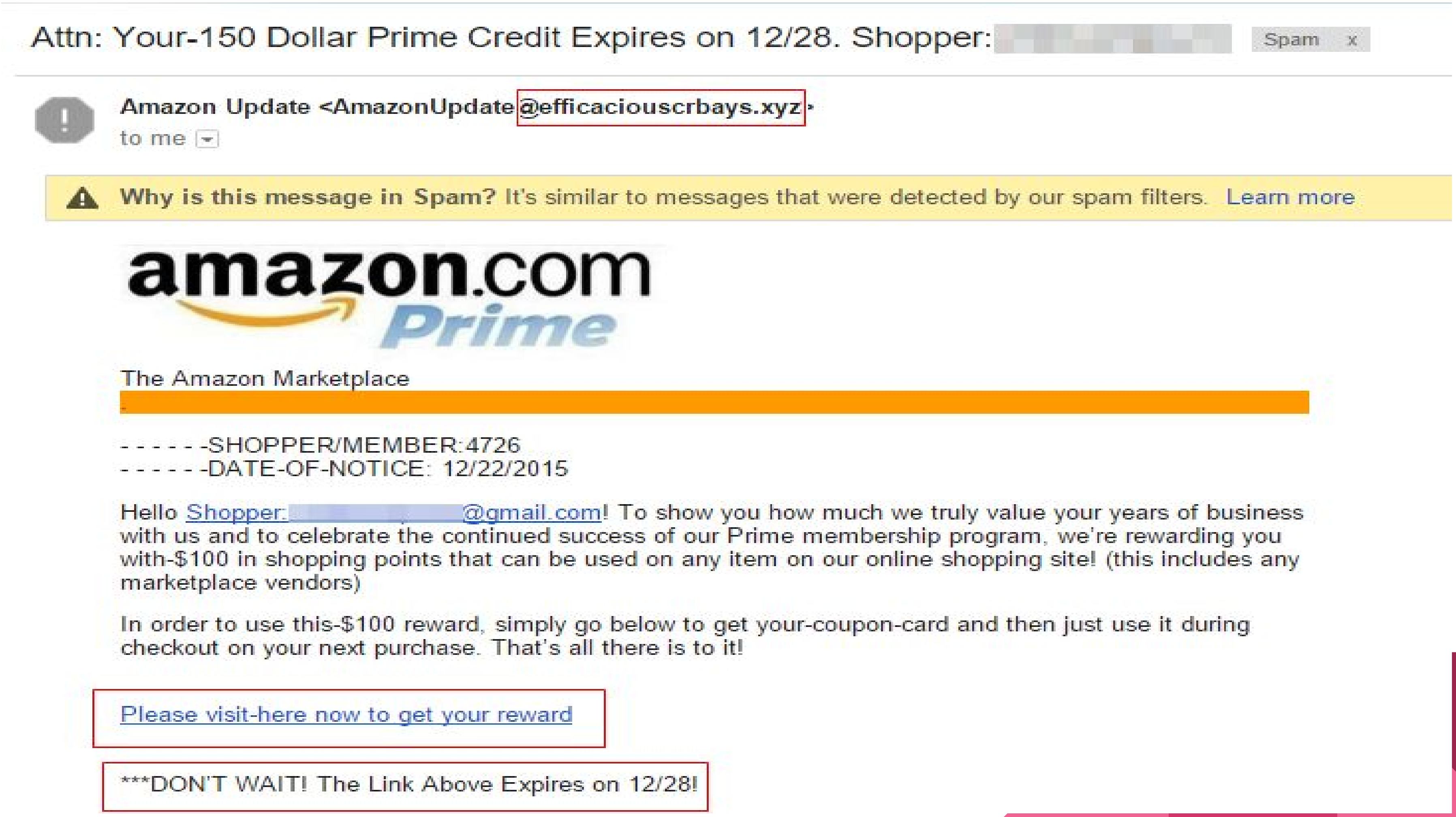


Warning! Your computer is infected!

Scanner report: 27 infected files detected

Name	Infected file	Security risk
TrustWarrior	SOFTWARE\Microsoft\Win...	🟥🟥🟥🟥⬜
Trojan-Spy.HTML.Bayfraud.hn	C:\Documents and Setting...	🟥🟥🟥🟥🟥
BAT.Looper	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-PSW.Win32.Antigen.a	C:\Documents and Setting...	🟥🟥🟥⬜⬜
Trojan-PSW.VBS.Half	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-Spy.HTML.Bankfraud.ra	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Virus.Win32.Faker.a	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-PSW.Win32.Fantast	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-Spy.HTML.Paypal.hn	C:\Documents and Setting...	🟥🟥🟥🟥🟥

Recommended: Please click "Activate" to eliminate all possible threats and protect Your PC.



Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper:[redacted]

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>

to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

The Amazon Marketplace

- - - - - -SHOPPER/MEMBER:4726
- - - - - -DATE-OF-NOTICE: 12/22/2015

Hello Shopper:[redacted]@gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

Please visit-here now to get your reward

***DON'T WAIT! The Link Above Expires on 12/28!

Social engineering

What:

An attack vector that relies heavily on human interaction and often involves tricking people into sharing personal information or transferring money

Why:

Influencing people into acting against their own interest is often a simpler than resorting to malware or hacking for financial gains

Social engineering

How: A social engineer runs what used to be called a "con game." Techniques such as *appeal to vanity*, *appeal to authority* and *appeal to greed* are often used in social engineering attacks

- Baiting
- Phishing
- Spear phishing
- Pretexting
- Scareware

2016 case - Hacker used social engineering to access critical information from the Department of Justice (DoJ), FBI and DHS

The hacker retrieved personal information of about 9,355 DoJ employees, 20,000 FBI employees, and over 9,000 Department of Homeland Security (DHS) employees

How he did it?

Step 1: Gaining credentials of a DoJ employee via spear phishing online
Step 2: Using the same credentials to log into the DoJ portal, but without success
Step 3: Calling the dept. and tricking them to believe he was a DoJ employee with the credentials he had gathered; once they believed him they gave him access to the portal

Social engineering

SOLUTION?..

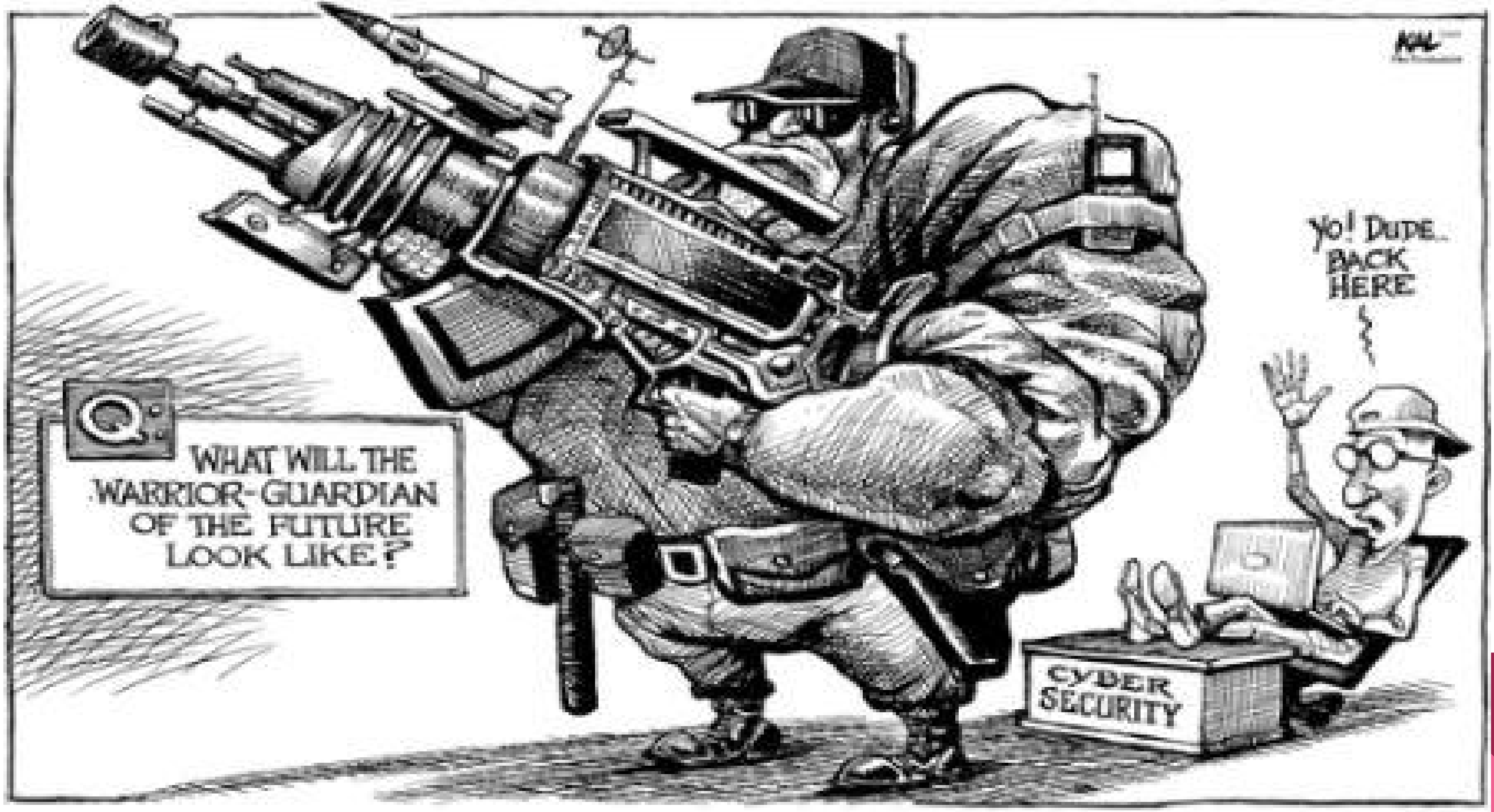
Penetration tests/white hat attacks using social engineering techniques

Mandatory security awareness training

Conclusion

Such cyber crimes became a trend in 2016 since many of them were carried over from previous years, and because these crimes are so easy to carry out, but difficult to prevent

Just the fact that these attacks are often so easy to perform becomes the motivation for criminals to learn how to use these tools. However, it is not as easy to come up with effective solutions for all the cyber threats


Q: WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE.. BACK HERE
CYBER SECURITY
KAL

Question 1:

What is E2EE and why can it be an advantage for cyber criminals?

Answer:

E2EE stands for *“end-to-end encryption”* and it can be an advantage for criminals since it disables any sort of tracking over conversations or data being shared, so even the service providers from accessing what is being shared amongst their users.

Question 2:

What is Social Engineering? Name 3 types of social engineering attack methods.

Answer:

Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into giving valuable information of money. Ex: Phishing, pretexting, scareware, etc.

Question 3:

What are white hat attacks?

Answer:

White hat attacks are also known as penetration testing where a company or organization tries to break into its own system using various social engineering hacks with the motive to figure out all the weaknesses in the system so that they can be fixed.

Thank you! :)

References

https://krebsonsecurity.com/2016/07/cybercrime-overtakes-traditional-crime-in-uk/

http://www.stcatharinesstandard.ca/2016/08/10/six-children-saved-six-adults-charged-in-online-sex-crime-case-dubbed-project-iceberg

http://www.570news.com/2016/10/26/ontario-man-accused-cyber-sex-abuse-case-ordered-extradited-plans-appeal/

https://www.thestar.com/news/canada/2016/10/26/ontario-med-student-ordered-extradited-to-us-on-cyber-sex-abuse-charges.html

https://en.wikipedia.org/wiki/Shedun

http://searchsecurity.techtarget.com/definition/social-engineering

http://www.statcan.gc.ca/pub/85-002-x/2009001/article/10783-eng.htm

http://siliconangle.com/blog/2016/02/08/hacker-users-social-engineering-hack-to-access-doj-releases-employee-files-from-dhs-fbi/

http://resources.infosecinstitute.com/the-ferizi-case-the-first-man-charged-with-cyber-terrorism/

http://www.welivesecurity.com/wp-content/uploads/2016/01/eset-trends-2016-insecurityeverywhere.pdf

https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf

https://www.proofpoint.com/sites/default/files/human-factor-report-2016.pdf