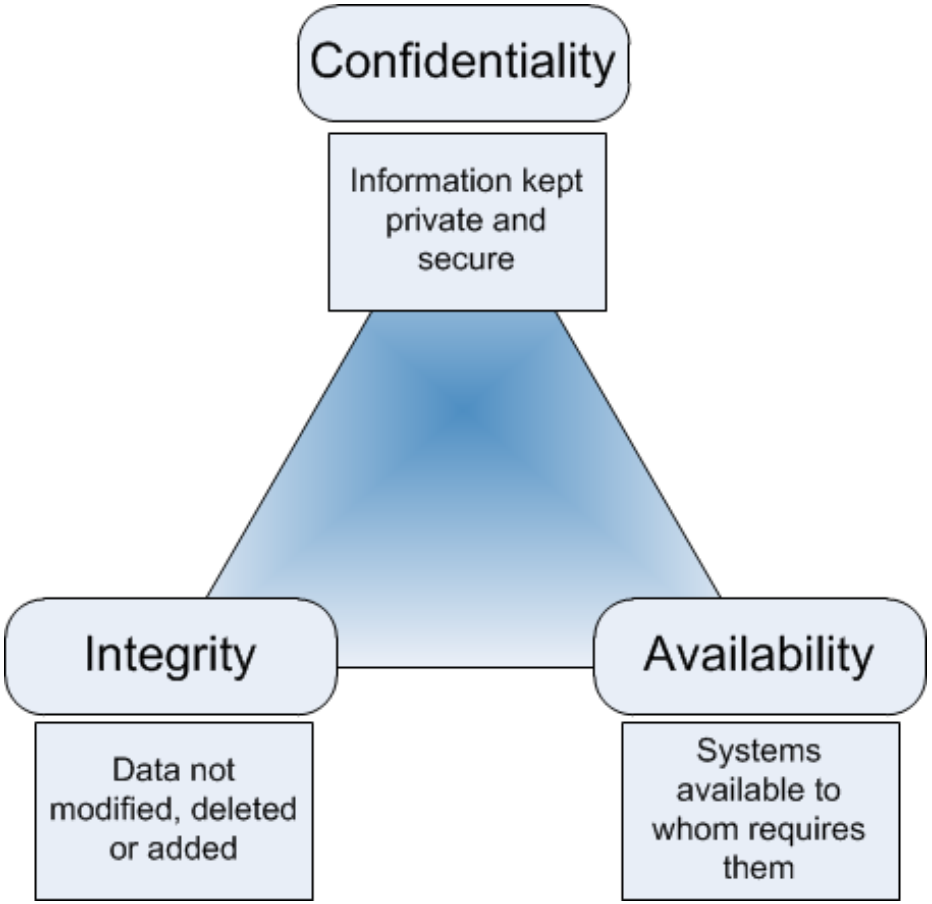
INFORMATION SECURITY AWARENESS SESSION

Agenda

- Information security goals
- Different types of malware
- Top security breaches of 2015
- Social engineering
  - Human based attacks
  - Computer based attacks
- Incident reporting
- Security tips & counter-measures
  - HTTPs – WOT
  - How to create a strong password
  - Clean desk & clear screen
  - Email security
  - Mobile threat & security
  - How to protect your PC
- Conclusion

Information security goals

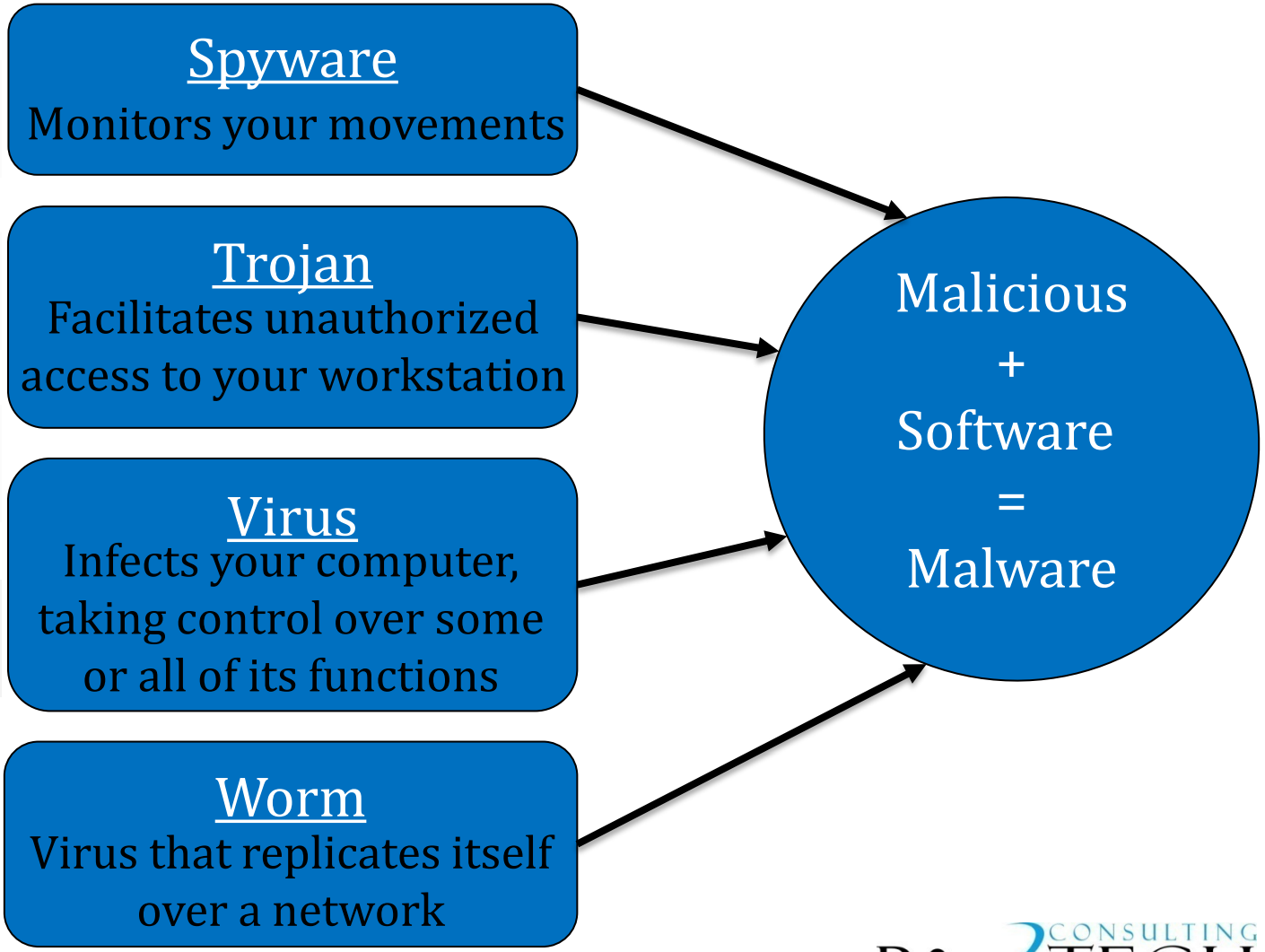


Information security goals

- Maintain an **appropriate level of awareness, knowledge and skills** amongst managers and employees.
- Ensure **business continuity** following information security incidents.

CONSULTING PETECH

Different types of malware



Top security breaches of 2015

ASHLEY MADISON

July 2015 -- Hacked By_The Impact Team

37,000,000

affected

When the online affair site was breached, hackers released millions of names and email addresses of Ashley Madison users — including multiple federal officials and Josh Duggar.

LASTPASS

June 2015 -- Hacked By_Unknown

7,000,000

affected

****

LastPass, a password manager program, was hacked,and the hackers gained access to email addresses, encrypted passwords, and password reminder phrases.

U.S. OFFICE OF PERSONNEL MANAGEMENT

June 2015 -- Hacked By_Unknown, Possibly China

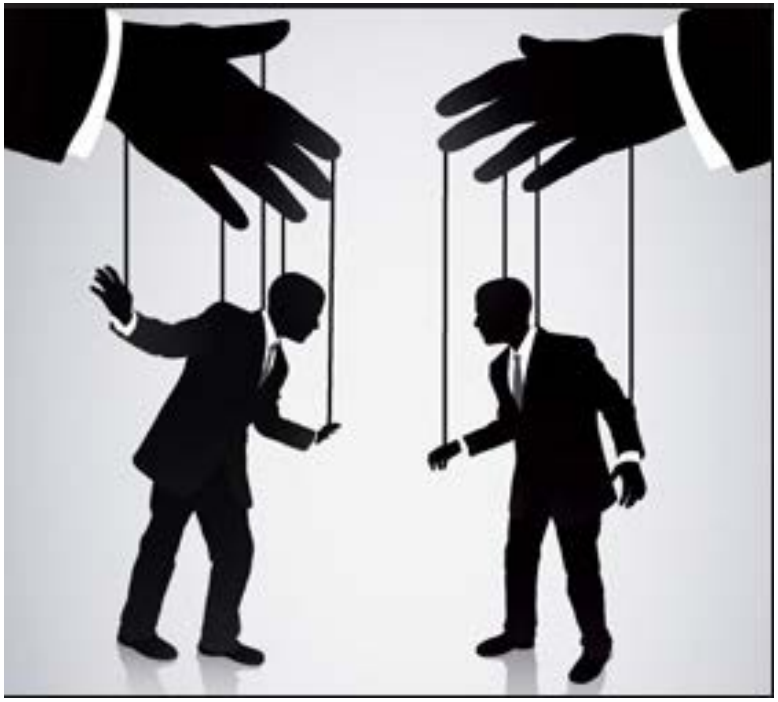
22,200,000

people affected

In an attack targeted at the Office of Personnel Management, hackers obtained massive amounts of information about former and current federal employees, including financial information, fingerprints, health records, and security clearance information over the course of two separate hackings.

Social engineering

THE ART OF HUMAN HACKING



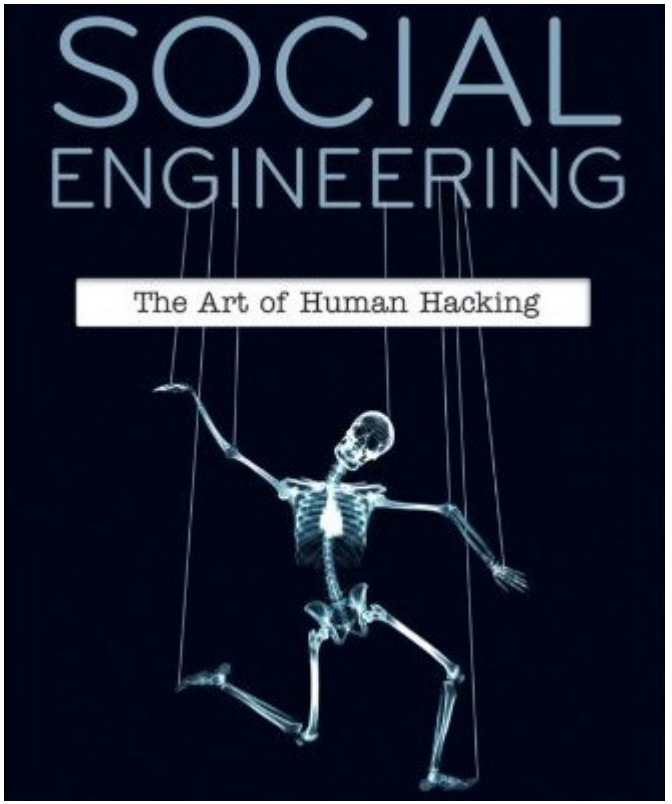
BECAUSE THERE IS NO PATCH FOR HUMAN ERRORS

CONSULTING PTECH

Why social engineering?

EVERY USER HAS INFORMATION AND EVERY INFORMATION IS GOOD TO TAKE

- One of the simplest attacks.
- Difficult to detect and track.
- Considered the most effective.



Type of social engineering attacks

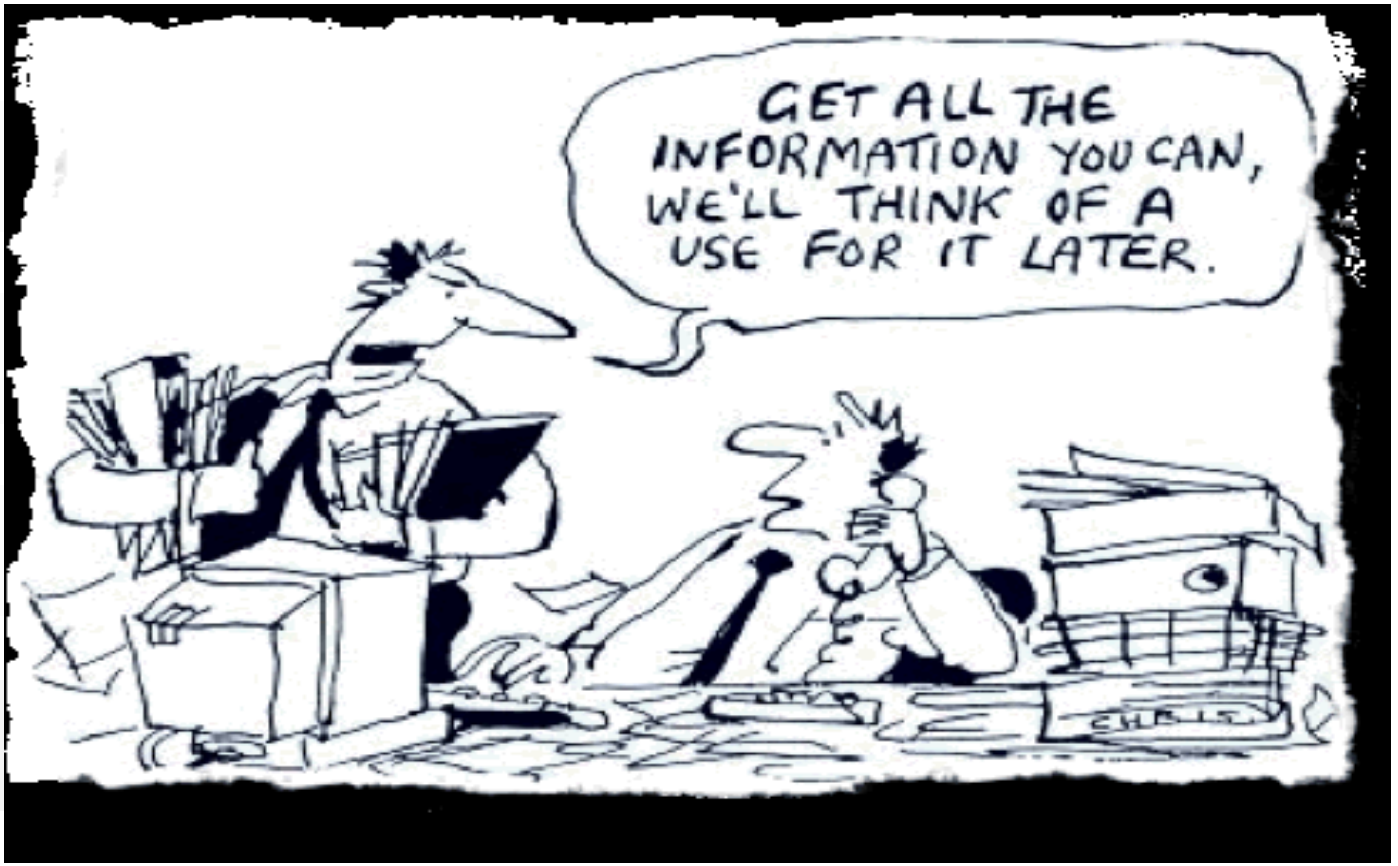
- Information gathering (Social media vectors)
- Shoulder surfing
- Dumpster diving
- Impersonation

Human based attacks

- Phishing
- Online Scams

Computer based attacks

Information gathering

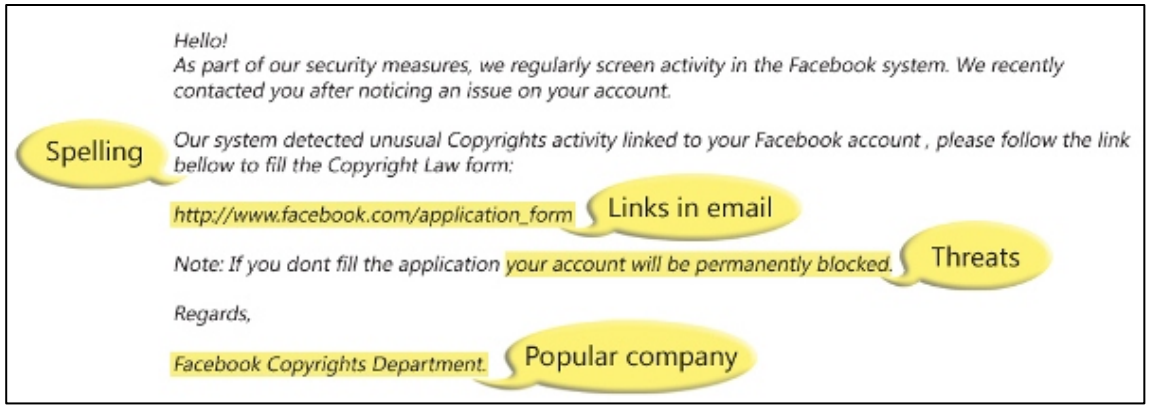


STAFF ARE THE FIRST LINE OF DEFENSE

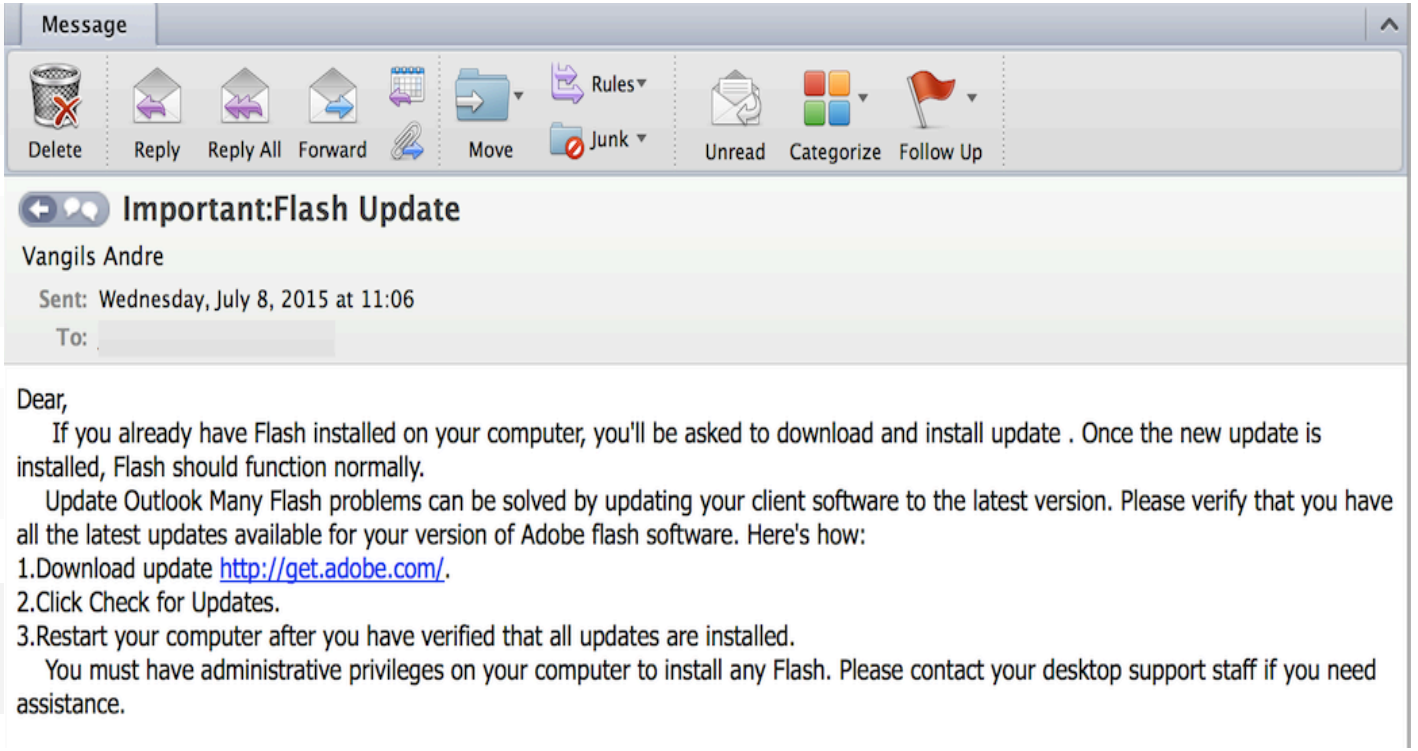
CONSULTING PC TECH

Phishing e-mails

- Phishing e-mails characteristics:
  - Deceptive subject line
  - Messages that sound attractive or threatening
  - Forged sender's address
  - Forged content (logos, fonts, images, etc.)
  - Forged hyperlinks
  - Submission forms



Phishing e-mails



Advanced Persistent Threat (APT)

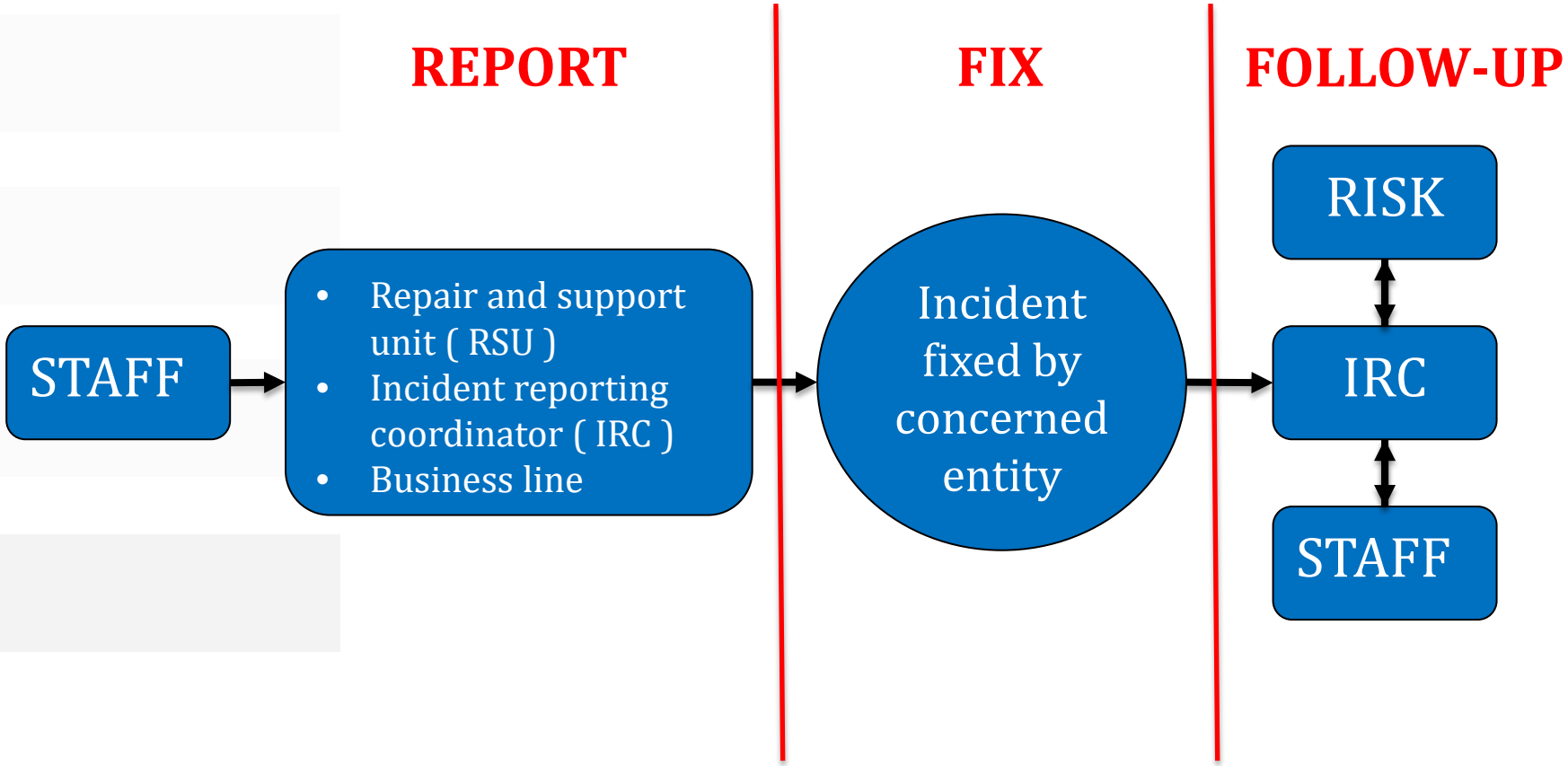
- **Definition:** An APT is an attack in which an unauthorized person gains access to the network and stays there undetected for a long period of time in order to steal data.

- An APT attacker often uses a type of **social engineering** to gain access to the network through legitimate means. Once access has been achieved, the attacker establishes a back door.

- **Countermeasures:**
  - Report odd user behavior, such as user activity after working hours or during weekends.
  - Keep aware of social engineering attempts; information/credentials disclosure could compromise the entire information system.

Online scams

Incident reporting



Real case incidents

Successful phishing attack ☹

I want to transfer 50000$

OK !!

Customer complains of unauthorized transfer

Bad image for bank and employee

Real case incidents

Phishing email detected ☺

I want to transfer 10000$

"Hey sir, do you confirm the unusual transfer?"

Security tips & counter measures

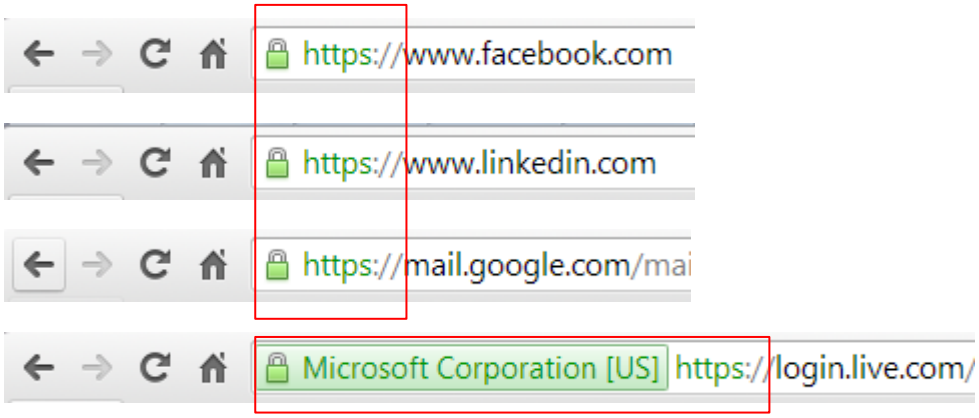
Digital Information is not only easy to store but also easy to leak.

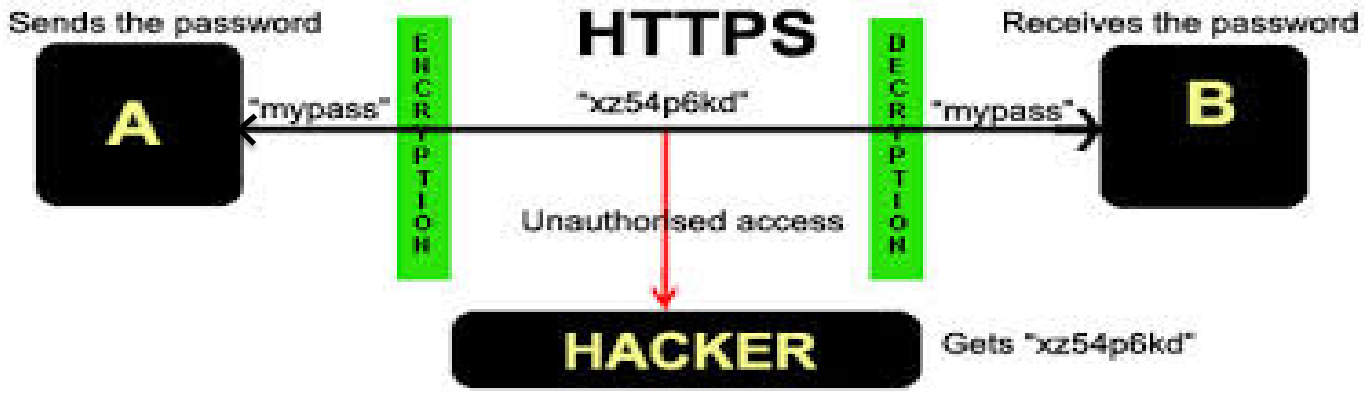
CONSULTING P TECH

Security tips & counter measures

- HTTPs
- WOT
- Social networking security
- Password security
- Physical security
- Email security
- Mobile security
- General security tips

HTTPs

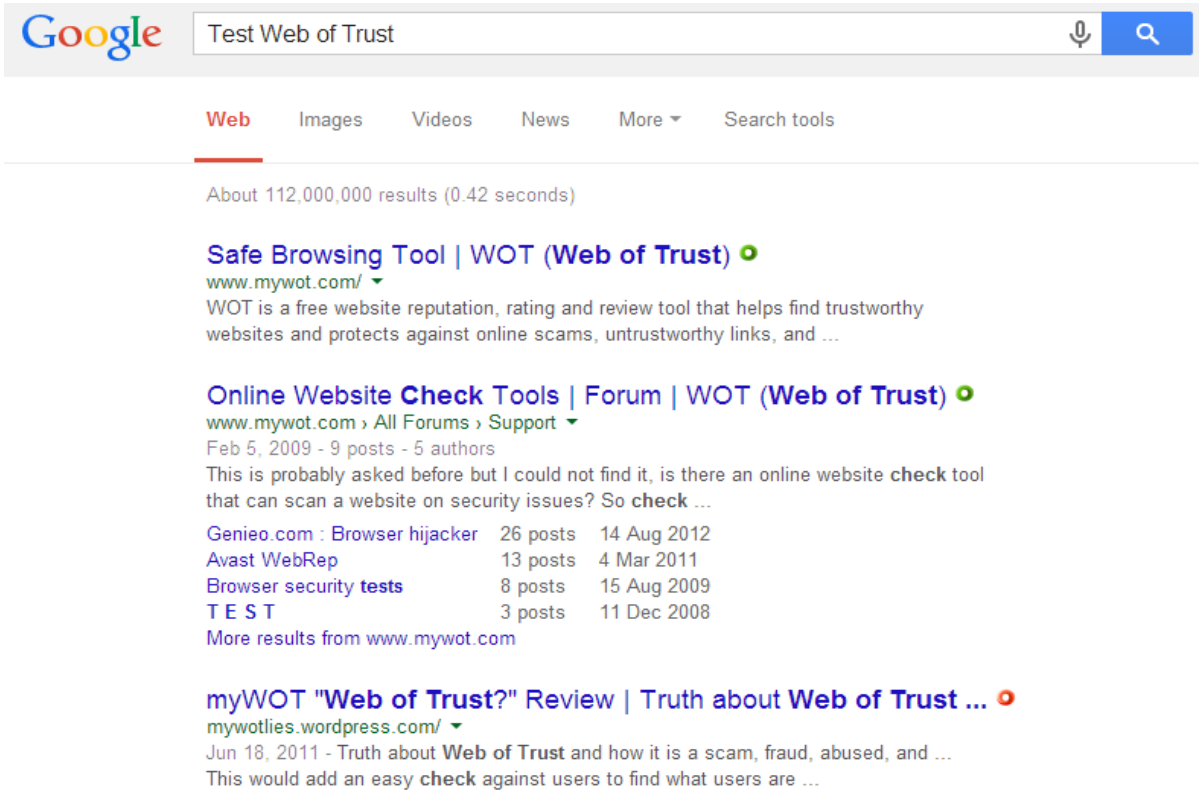




CONSULTING PC TECH

Web of Trust – WOT

WOT displays a colored traffic light next to website links to show you which sites people trust for safe searching, surfing and shopping online.



Web Security (POC)

- Website Verification
- Freeware
- Downloads

Social networking security

- Once you publish something you can't take it back
- Limit the amount of personal information you post
- Evaluate your security settings
- Be wary of third-party applications
- Use strong passwords
- Check privacy policies
- Don't believe anything you read online

CONSULTING PETECH

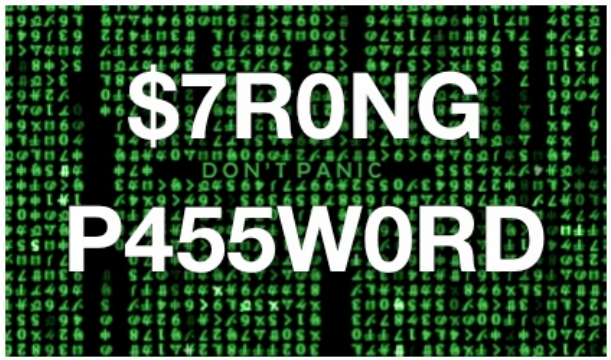
Social networking security (POC)

- Evaluate your security settings
- Third-party applications
- Use strong passwords
- Check privacy policies
- Scam Examples

Password security

- How to select a strong password:
  - At least 8 characters
  - Mix of upper and lowercase characters
  - Mix of alpha and numeric characters
  - Don't use dictionary words
- Change passwords frequently
- Don't share or reuse passwords
- Use different passwords for different accounts
- Don't write down passwords
- Use password phrases:

I was Born on May 9 nineteen90 # → IwBoM9n90#



Clear desk & clear screen

- Clear away paperwork
- Use **shredders** for sensitive documents disposal
- Lock desk and filing cabinets
- Lock away portable devices such as tablets
- Lock your workstation when you leave
- Make sure no documents are left in the printer
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

Email security

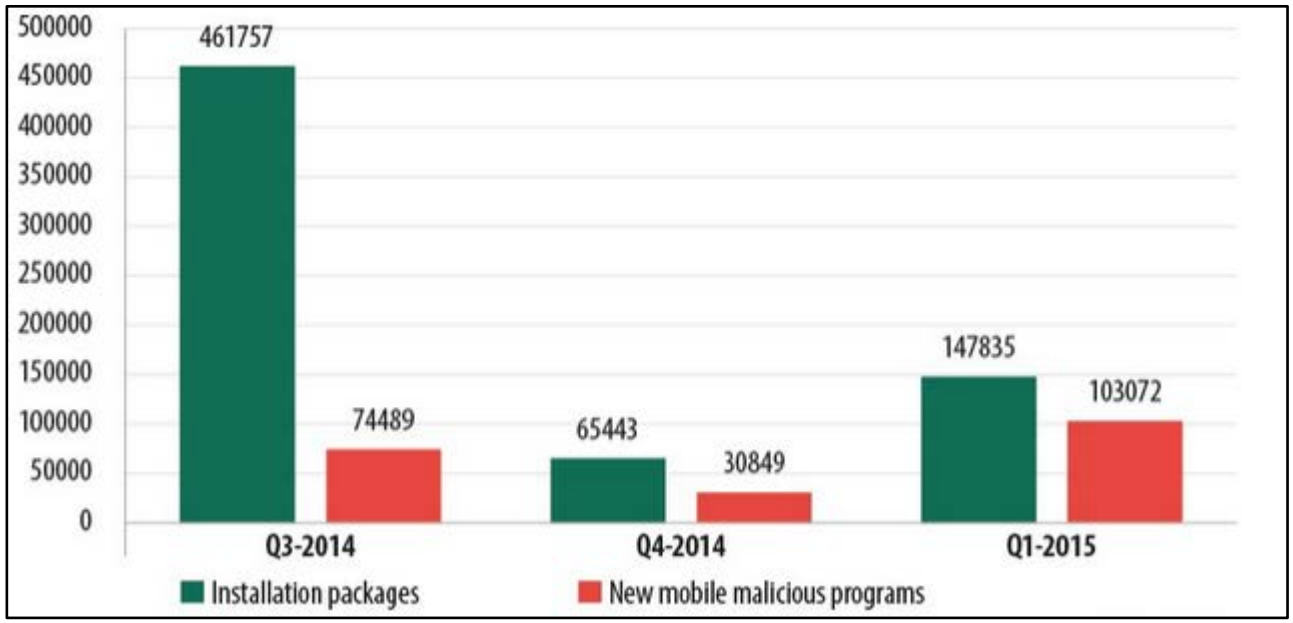
- Never open an attachment from an unknown sender
- Make sure the email references the attachment
- Do not hesitate to contact the sender of an email message that contains an attachment
- Never send anyone your personal data (name, address, phone number, password, account numbers)
- In case of suspicion, contact the IT department or the information security officer

"Trust your instincts - It may well be a virus"

CONSULTING PC TECH

Mobile threat

Number of malicious installation packages and new malicious programs detected (Q3 2014 – Q1 2015)



Mobile phones security

- Never plug in your phone to the PC
- Download applications only from trusted sources:

- Install antimalware controls
- Never store business related documents on your phone
- Always change the factory pin code (0000)
- Always use a screen lock

Mobile phones security (POC)

- Locking
- Trusted Source
- Secure Messaging Apps
- Mail

Mobile phones security

- Share with care. Once you post a text, photo, and/or video it's tough to take back, can be copied and pasted elsewhere. Think about the people in them (including you!). Privacy is at stake.
- Pay attention to any permissions applications request as you install them.
- Use a "find your phone tool." Certain software and applications make it easy to find your phone if you lose it.
- Keep your operating system and applications updated as they contain security patches.
- Disable services like GPS or Bluetooth if not needed.

How to protect your PC

- Always backup sensitive data
- Always lock your workstation when away from your desk (Windows: Windows key + L)
- Ensure that antivirus definitions are updated regularly
- Reboot your system after applying new updates
- Use a strong password and try not to be confused with the passwords used in personal accounts
- Never charge smartphones from the PC
- Never insert a USB or any storage device into your PC

Conclusion

Security

20% Technical

80% Behavior