Information Security

Creating Awareness, Educating Staff, and Protecting Information

Mustaqeem Bin Abdullah

Topic Covered

Data Privacy	Spyware & Adware	SPAM & SPIM	Phishing
Passwords	Social Engineering	Email & Chat Services	Securing Workstations
Data Backups	Equipment Disposal	Data Recovery Demo	Data Disposal
Access Rights	Physical Security	Emerging Threats	Incident Response
Creating Awareness	Questions	Useful Links	

Why Security?

- Liability
- Privacy Concerns
- Copyright Violations
- Identity Theft
- Resource Violations
- Reputation Protection
- Meet Expectations
- Laws & Regulations

Understanding Threats

What is valuable?

What is vulnerable?

What can we do to safeguard and mitigate threats?

What can we do to prepare ourselves?

Most believe they will win lottery before getting hit by malicious code

Who Want Our Information?

White Hat

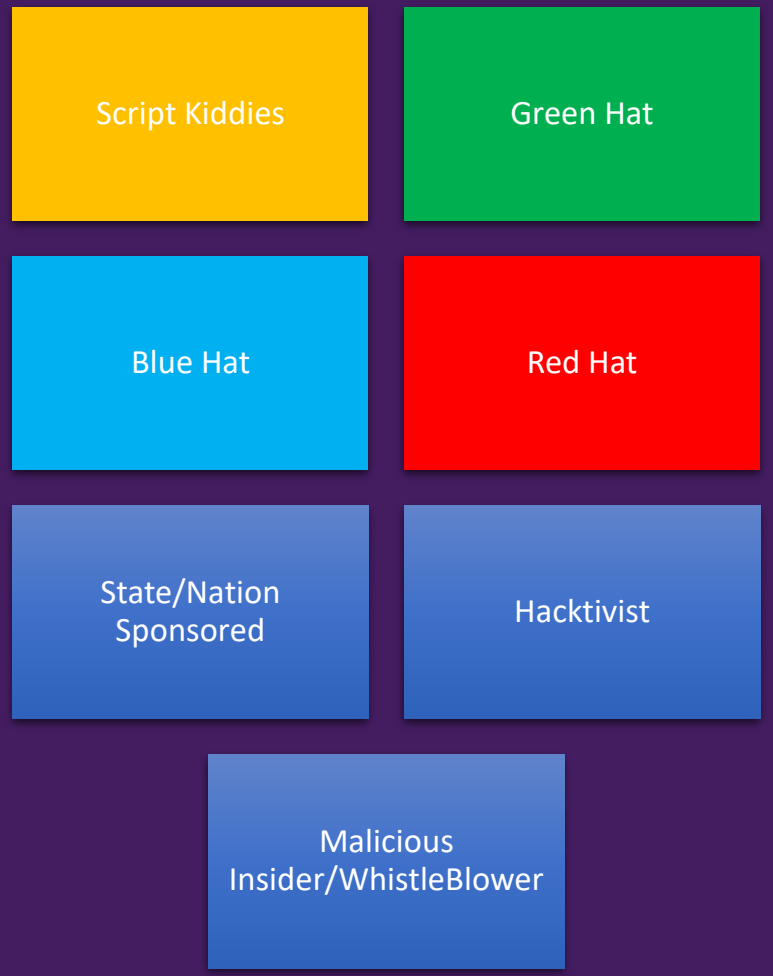
- Also known as Ethical Hackers
- Help Govt and organizations

Black Hat

- Hacking for personal gain
- Looking for vulnerabilities in organization systems

Gray Hat

- Unethical Hacker
- Skillful, but not for personal gain



Spyware & Adware

Adware

Trojan

Tracking Cookies

System Monitors

Don’t

Accepting a prompt or pop-up without reading

Downloading software from an unreliable source

Open emails from unknown senders

Pirating media such as movies, music, or games

A total of 978 million people in 20 countries were affected by cybercrime in 2017, resulting $172 billions lost according to Norton Cyber Security Insights Report Global Results

Spam/SPIM

Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc

Medium of Spam:

- E-mail
- Instant Messaging
- Chat
- Newsgroup/forum
- Mobile phone
- Online game
- Video sharing site

Phishing

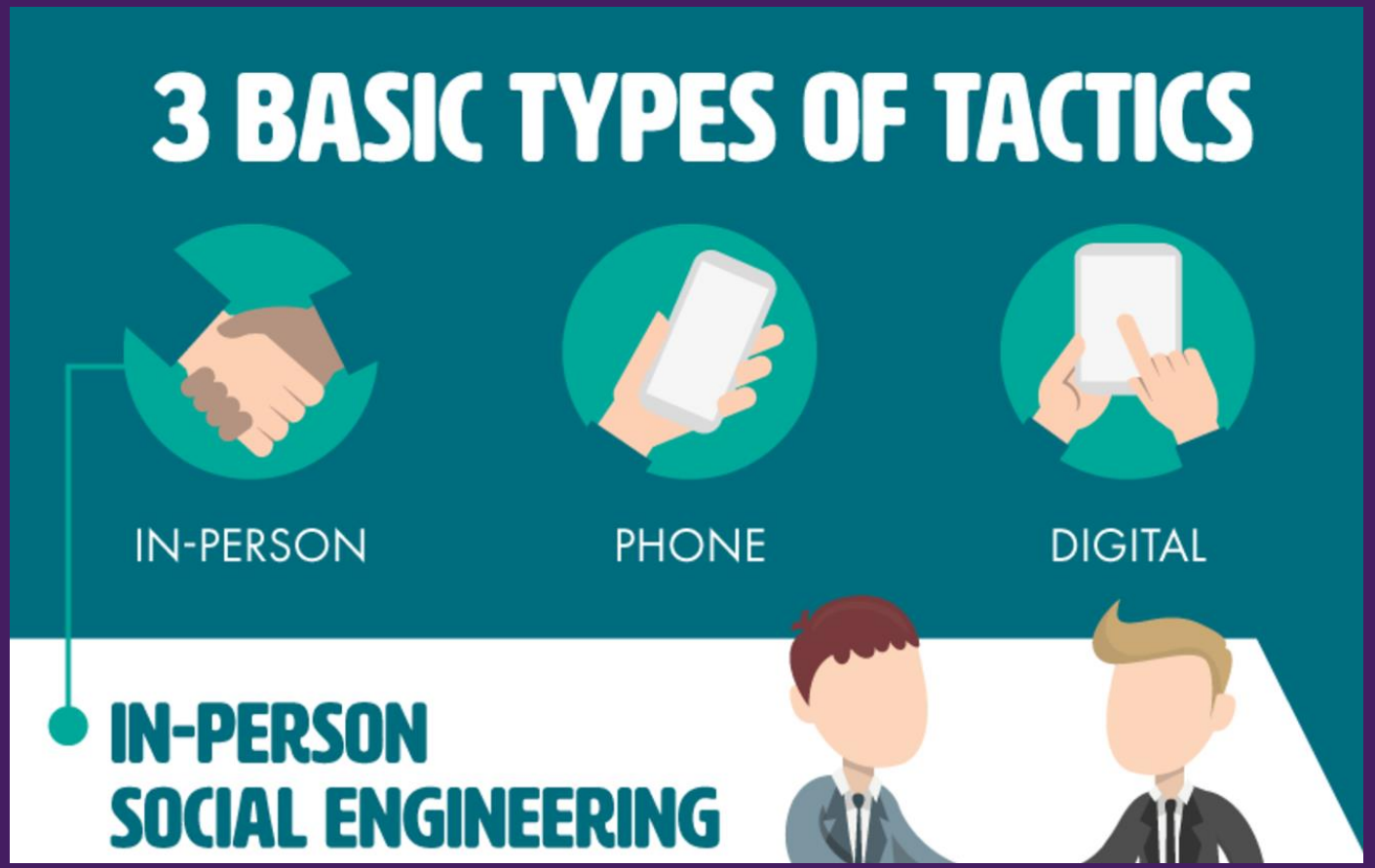
A computer scam that uses SPAM, SPIM & pop-up messages to trick us into disclosing private information (Social Security Number, Credit Cards, banking data, passwords, etc)

- Often sent from someone that we “trust” or are in some way associated with us
- Appears to be a legitimate website
- Embedded in links emails & pop-up message
- Phishing emails often contain spyware designed to give remote control to our computer or track our online activities

Social Engineering

Art of prying information out of someone else to obtain access or gain important details about a particular system through the use of deception

6 Types:
Baiting
Phishing
Email Hacking
Pretexting
Quid pro quo
Vishing



Email & Chat Services

- Email and chat are sent in clear text over the Internet
- Data can easily be captured and read by savvy computer users and systems administrators
- Safeguards should be put into place prior to using these programs for sending/receiving sensitive information like Social Security Numbers and ID/Password etc.

Enhanced Work Area Security

Secure workstations

- Lock our systems (Ctrl-Alt-Delete)
- Shut down
- Run up to date virus scanning software
- Password protect files
- Apply software patches
- Install cable locks
- Run a desktop firewall

Is Our Data Being Backed Up?

- Test backups
- Securely store backup media (offsite)
- Restrict access to who can perform restoration

- **140,000 hard drives fail in the United States each week**

(source: Small Business Trends)

- **On average, small companies lose over $100,000 per ransomware incident due to downtime.**

(source: CNN Money)

- **60% of companies who experience data loss shut down within six months.**

(Source: Boston Computing)

- **58% of businesses have no backup plan for data loss.**

(Source: Small Business Trends)

Equipment Disposal

- What happens to old computer when they are replaced?
- Do those systems contain sensitive information?
- Several programs to securely remove data from computer systems are commercially available

Dumpster Diving

- We never know who is looking in our trash
- Shred sensitive documents
- Secure shred barrels, and make sure that proper handling procedures are in place

Access Right

- Only allow access that is absolutely required
- Don’t grant accounts based on the fact that access “may” be required
- Use least privilege access policies that state access will only be granted if required, not by default
- Are accounts removed and passwords changed when someone changes jobs or is terminated?
- Perform audits

Be Aware!!

Do you know what to do and who to contact if a security breach occurs?

Be Aware!

- Report anything “strange”
- Don’t give private information out
- Properly dispose of sensitive information
- Run up to date virus protection & software
- Ask questions

USM Policies

- Dasar Teknologi Maklumat dan Komunikasi Universiti Sains Malaysia
- GARIS PANDUAN DAN PROSEDUR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

Thank You!