IT Security

Awareness Training

What is IT Security.

IT Security, or Information Security (InfoSec), is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.

How do we protect our precious data

Firewalls	VPN
Proxies	Ant-virus
Web Filters	Anti-spyware
Spam Filters	Passwords

IT Nerds	Blah Blah Blah Boring

What is IT Security….

and what does it mean for me

Technology - There is no denying that technology is vital to organisations operations and it is expanding at a rapid rate. It is no longer up to hardware and IT systems to keep our information safe. End users are now just important to keep information secure.

What we are trying to achieve here:

- Delivering a consistant message about the importance of information security
- Suggesting users to develop and maintain safe technology usage habits
- Motivating users to take a personal interest in information security
- Awareness that IT security is not only for employees but should be considered by everyone.

User Awareness

What user need to know:

Users need to know information about security issues that can affect their work, their home, themselves, and their families. They need to understand the threats and risks as well as the methods they can personally use to defend against those threats.

Types of security threats:

Malware

Spyware

Viruses

Spam

Phishing Scams

RootKits

MANY MANY MORE

What do they do / mean:

These are all basically small pieces of software/code that infect computers with the intentions to corrupt, steal, or delete your data.

They can do anything from record your passwords by logging keystrokes to hijacking your webcam to watch and record your every move.

Our Focus

The focus of this presentation will try to explain and educate by providing examples of common threats that target end users to gain access to systems.

Traditional Hacking Methods.

Traditional hacking is the method of trying to compromise systems or software to get sensitive data.

Social Engineering Methods.

Social engineering is the manipulation of humans to get sensitive information or compromise systems

Social engineering is a method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter.

Hacking in action

Example 1 – Website Vulnerabilities

Ill how a simple vulnerability can compromise a system. And your personal Information.

Example 2 – Passwords.

Passwords are like underwear:
You shouldn't leave them out for people to see.
You shouldn't loan them to a friend or colleague.
You should change them regularly.
And if they're too short they're not going to protect much.

Social Engineering

“You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned manipulation.”

- Kevin Mitnick

Social Engineering

There are 2 types of social engineering, technical and non-technical.

Technical Examples:

Phishing
Pop ups
Spam emails
Clicker bait

Non-Technical (Peer-to-Peer)

Dumpster Diving
Support Staff
Hoaxing
Authoritative Voice

Social Engineering

The Manipulation of the human Behaviour.
Hackers will exploit certain human traits to get information.

Curiosity

Clicker bait - “you would not believe this”
spam links, pop ups - “You are the 1000 visitor and have won an IPAD”

Fear

“your account has been hacked. Please log in to verify your identity”

Thoughtlessness

“Leaving passwords on your monitor.”
Or
Picking up a free usb from the car park

Back to the books

My aim is not to confuse but hopeful get you understand the fundamentals of how computers talk

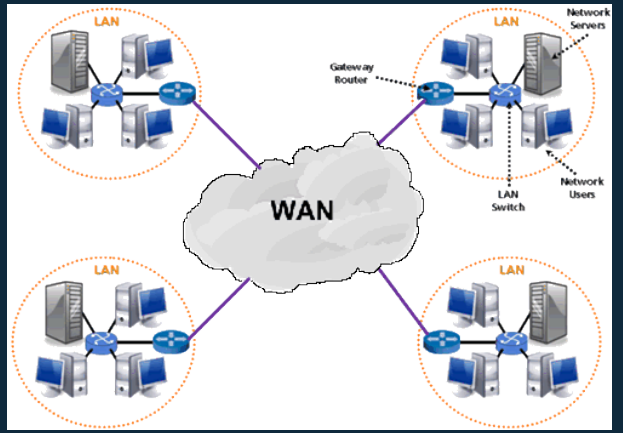
What is an IP address

IP is the number associated to a computer/server/phone wanting to talk on a network.

Duplicates are not allowed. Just like not 2 people can have the same phone number

There are 2 types of IP's, Local (LAN), External (WAN)

LAN Address	WAN Address
192.168.0.0	Anything else
10.0.0.0	101.178.170.1 – 101.178.170.15
172.16.0.0	



Back to the books

My aim is not to confuse but hopeful get you understand the fundamentals of how computers talk

What is a DNS

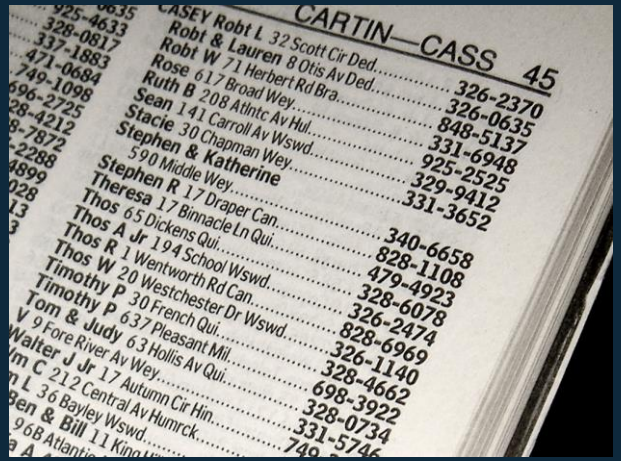
A DNS is what converts IP to human readable network names.

If IP's were phone numbers a DNS server would be like a phonebook

Example:

What is: 203.52.0.221

Internal or External?



Social Engineering in action

Example 1 – Website cloning

What you see is definitely not what you get. Be sure everything looks the part.. And more

Example 2 – Payloads/Backdoor

Scary stuff.

Social Engineering How To:
Step 1. Put on Ninja suit.
Step 2. Social away.

Mitigating the risk

So what now….
Continue as normal, No need to unplug your computers and give up.

We still have system in place to help protect against these threats.

Hopefully you are now more aware of different types of threats to IT Security how you can do your part in protecting information from the ninjas behind the computer screens.

Etc..

Thanks!

Any questions?

You can find me at:

- My Desk
- The Tea Room
- The Bathroom
- The Hallway