Cyber Crime
What, Where and How

Prof. Zaheed Shaikh

Agenda

- Current Scenario

- What is Cyber Crime

- Types of Cyber Crime

Cyber Crime-Scenario

- International
  - Attacks on Power Sector in US
  - Attacks on ICT infrastructure of Estonia

- India
  - National
    - Terrorist infiltration in Technical Industry
    - Attacks on Institutions of Excellence
    - Terrorist funding of Capital Markets in India
  - Personal
    - Facebook alterations
    - Email hacking

Power Sector Attacks-SCADA

- "In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."
  - CIA senior analyst Tom Donahue quoted in Information week Jan 18, 2008

- Supervisory Control and Data Acquisition (SCADA) use in India not a distant dream
  - Electricity Act 2003 allows third party sales. The act also provides open access to transmission as well as distribution of electricity

Estonia

- Most electronically networked country
- Attacks left entire country paralysed- April- May 2007

Cyber Crime-Definition

- Crimes committed via the Internet and other computer networks, dealing particularly with
  - Infringements of copyright
  - Computer-related fraud,
  - Child pornography and
  - violations of network security
    - Convention on Cyber Crime, July 2004- Strasbourg- active participation of US, Canada and Japan
- Additional Protocol- Feb 2006
  - To criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults

Types of Cyber Crime

- Finjan Survey July 2008- 91% Percieve Cyber Crime major threat
  - 73% of the all responding CIOs and CSOs were more concerned about data theft (crimeware stealing their business data) than about downtime and loss of productivity due to virus infections
  - The majority of the respondents (68%) indicated that their corporate intellectual property and sensitive information is at risk of data-theft
  - More than half of the respondents (54%) worry about their corporate employee information being stolen

Types of Cyber Crime

- Survey 2008
  - 47% of all respondents listed theft of their corporate customer information as a major business concern
  - In the banking and financial sector, 95% of the respondents perceived cybercrime as a major business risk to their organization
  - Of the responding healthcare providers, 73% listed their patients' medical records as the main potential cybercrime target
  - 25% of the respondents reported that their data had been breached, with an overwhelming
  - 67% of respondents knowledgeable about web security listed real-time content inspection technology as the preferred web security solution

Types of Cyber Crime

- Hacking
- Phishing
  - Identity Theft
- Denial of Service
- Virus
- Trojans

Methods-Advance Fee Fraud

- Advance fee fraud is a confidence trick in which the target is persuaded to advance sums of money in the hope of realizing a very much larger gain
  - 419 is the article in Chapter 38 of "Obtaining Property by false pretences; Cheating

Extortion Virus-Ransomware

- Lock the files of targeted computer
- Demand Ransom for unlocking the files
- Wannacry Ransomware Attack

Virtual Theft

- A Dutch teenager arrested for allegedly stealing virtual furniture from "rooms" in Habbo Hotel, a 3D social networking website- Nov 2007

- Stealing $5800 worth of *virtual* furniture from *virtual*

- Done by luring victims to disclose passwords through fake habbo sites

- Habbo users can create their own characters, decorate their own rooms and play a number of games, paying with Habbo Credits, which they have to buy with real cash

International Espionage

- Cuckoo's Egg- Clifford Stoll
  - Discovered through investigation of USD 0.75 accounting error in the computer usage accounts
  - Intrusion from West Germany using Tymnet
  - The hacker's name was Markus Hess and he had been engaged for some years in selling the results of his hacking to the Soviet Union KGB (Committee for State Security).

Major Concerns

- UN E Government Survey 2008

    - E Government readiness-India slipped to 113 in 2008 as compared to 87 in 2005- Maldives and Sri Lanka ahead of India

- Lack of critical infrastructure protection standards
- Lack of established programs to identify risks and vulnerabilities in Infrastructure and efforts to plug them

What Is Cyber Crime?

When an offence is committed, in full or in part, via a computer, network or other computer enabled device.
-Warwickshire Police

Types of Cyber Crime

Fraud

Identity Theft

Phishing Scams

Viruses

child pornography

Online Hate Crime

Grooming

Stalking

Holiday Fraud

Dating Fraud

Bullying

Pension Fraud

Hacking

Online Extremism

Online child abuse

…and this is just the tip of the iceberg

Stats

As age increases, knowledge of online risks reduces slightly while the feeling of being at risk increases significantly

56.4% of those surveyed had received a phishing email

1 in 10 fell victim to the phishing scam

Under 18s are the age group most targeted for online harassment or bullying with females targeted twice as much as males

Nearly one third of parents have neither applied online restrictions nor spoken to their children about internet safety

Real Or No Real: Emails

Von: Sherman Shaw <Shaw1944@icba.org>   Gesendet: Mi 09.11.2011 12:06
An: @emsisoft.com
Cc:
Betreff: Funds Transfer was hold by our bank

Dear bank account owner,

I regret to inform you ... behalf was hold by our ban...

Transaction ...
Current status ...

Please review tra...

T. K. Shaw
Treasury Manager

Real Or No Real: Emails

Phishing- The Warning Signs

The offer seems too good to be true

Links do not go to the place you would expect them to

Spelling mistakes throughout the email or in the subject line

The sender's address is not a genuine email (e.g. instead of halifax.co.uk, it is halifab.co.uk, or even fiodnusgbi.hfx

There is a sense of urgency to respond to the email's request

Be aware for calls & texts too!

Cryptolocker 2.0

Your personal files are encrypted

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files   << Back   Proceed to payment >>

Viruses

- 1.4 million cases of computer viruses in the UK (ONS 2016 Crime Data)

- Malware can have harmful effects such as:
    - displaying irritating messages
    - stealing data
    - giving hackers control over your computer
    - certain malware can lock your computer until you pay a 'ransom fee'

Passwords

- Pitfall for a great amount of cyber security

- Most common passwords globally:
  1. 123456
  2. password
  3. 12345678
  4. qwerty
  5. 12345
  6. 123456789
  7. football
  8. 1234
  9. 1234567
  10. baseball
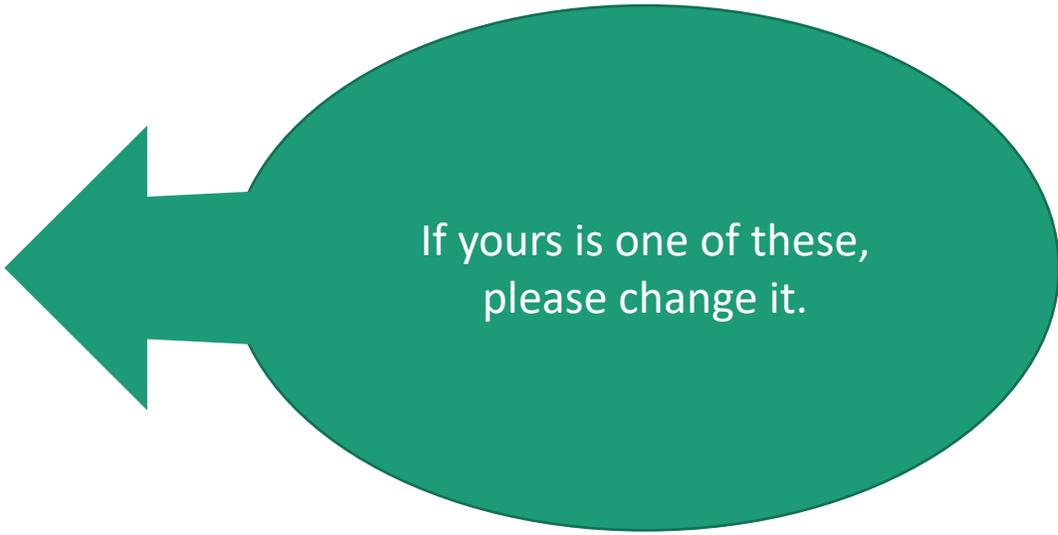
If yours is one of these, please change it.

Passwords

- Need a new password?
  - think of your favourite book/film/song/poem

  - choose a line from it

  - take the first letters of each word

  - change some of the letters for CAPITALS, numb3r5 and punctuat!on

Top Tips For Online Safety

- Be careful of links and attachments in e-mails.

- Use different passwords for online accounts.

- Check websites security.
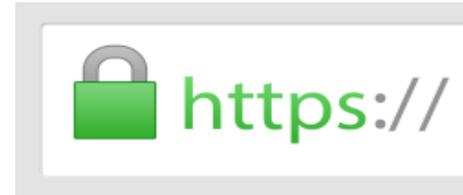
- If you are ever unsure about something online, do your research.

- Anti-virus software.

Top Tips For Online Safety

- Keep computer software updated.

- Keep all devices safe.

- Limit use of public Wi-Fi for work.

- Update social media privacy settings.

- Report it

- As with any crime, it is also important that victims are signposted to Victim Support fro any psychological/emotional impact they may have experienced