Don't Fall for Scams, Protecting your Online Reputation

CHETAN SONI, C-DAC Mohali

Safety is not a slogan, it’s a way of life.

Objective

The objective of this presentation is to educate and create awareness amongst the community on use of Technology, Internet Media and its implications on possible cyber crimes.

What it covers ?

- Intro to Scam and its types
- Pillars of Cyber Security
- Cyber Crime and their History
- Unicode Phishing
- Learn to spot Fake Websites
- Indications of Virus Attack
- Safe Social Networking & FB Security
- Security Tips for Online Shopping
- How to File a Cyber Complaint?

What is SCAM ?

- A scam is a term used to define a fraudulent business which takes money or other expensive good from an unsuspecting person.
- As everything s getting connected to the internet, online scam is increasing rapidly.
- Many successful internet scams have similar endings: Victims either lose their own money or fail to receive funds the fraudster promised.
- The common type of online scams are:
  - phishing, auction fraud, donation scam, catfish, cold call scam, 419 scam, online survey scam and much more.

11 Famous Internet Scams

1. Romance scam
2. The overpayment scam
3. Quick-money promise
4. Facebook impersonation scam
5. Fake shopping websites
6. Phishing scams
7. Unexpected prize scam
8. The Nigerian letter scam
9. Exortion or threat or “*hitman*” scam
10. Malware and ransomware scams
11. The tech support online scam

3 Pillars of Cyber Security

- **Communication Security -** protecting organization communication media , technology , and content.

- **Network Security -** is the protection of networking components, connection and content.

- **Information Security -** protection of information and its critical elements , including the systems and hardware that use , store or transmit that information.

Cyber Crimes and their History

- INDIA is the third-most targeted country for Phishing attacks after the US and the UK,
- Social networks as well as ecommerce sites are major targets,
- 6.9 million Bot-infected systems in 2010,
- 14,348 website defacements in 2010,
- 6,850 .in and 4,150 .com domains were defaced during 2011,
- India is the number 1 country in the world for generating spam.
- ‘The ‘dislike’ button’ Spam,
- ‘Make thousands working from home!’,
- Twitter direct messages with bad links,
- ‘Justin Bieber stabbed!’,
- ‘Facebook will start charging members!’, and the list can go on and on.

FIND the Difference ?

https://www.apple.com/

https://www.apple.com/

https://www.epic.com/

https://www.epic.com/

Learn to Spot Fake Websites

- The website has a strange URL. Instead of seeing something like “ebay.com,” you get “shop-at-ebay.com” or “bestonline-shoppingstore.com.”
- There is no green padlock icon before the URL bar, meaning the website doesn’t use SSL encryption.
- The website’s URL address starts with “http” instead of “https.”
- There are extremely low prices, like seeing an iPhone X for sale for only $100-$200, when it normally costs around $1,000.
- The contact details are very sketchy. For instance, instead of seeing “support@ebay.com,” you’ll see “supportebay@yahoo.com.”
- The website has a confusing mix of products. For example, the site claims to only sell clothing, but you notice weird extra items like car parts.
- The website has a horrible design and layout.

Indications of Virus Attack

1. Processes take more resources and time.
2. Computer beeps with no display.
3. Drive label changes.
4. Unable to load OS.
5. Computer slows down when program starts.
6. Anti-virus alerts.
7. Computer freezes frequently or encounters error.
8. Files & Folders are missing.
9. Hard Drive is not accessible.
10. Browser window freezes.

Top 10 Popular Viruses/Worms

• **ILOVEYOU**	– Mailing System	(Loss $10 billion)
• **CodeRed**	– Microsoft IIS Server	(Loss $2 billion)
• **Melissa**	– MS WORD	(Loss $80 million)
• **Sasser**	– Buffer overflow	(Loss $18 billion)
• **Zeus**	– Key logger/Botnet	(Loss $70 million)
• **Conficker**	– Botnet/Win32	(Loss $9 billion)
• **Stuxnet**	– Nuclear Worm	(Loss $90 million)
• **Mydoom**	– Email Malware	(Loss $38 billion)
• **CryptoLocker**	– Ransom ware	(Loss in billions)
• **Flashback**	– JS Malware for MAC	(Loss in millions)

Safe Social Networking

Today's world is a global village. Everyone is connected to one another in this vast network generated by network.

As of 2015, the world's largest social networking company, Facebook has 1.49 billion active users, and the no. of users are increasing every year.

- 72% - High School Students
- 78% - College Students

Facebook Security

- Koobface (2009) – A Must see viral video
- Zeus – Botnet
- LikeJacking – Fake Likes
- Facebook Black – JS Malware
- Who Viewed Your profile? – Browser Hijacking

Security –

1) For Account Recovering - http://facebook.com/hacked
2) To Report anything - https://www.facebook.com/help/contact/274459462613911
3) About Safety Check - https://www.facebook.com/about/safetycheck/

How to Bank Safely Online

1) Never login to your bank website through a link in an email, even if the email appears to have come from your bank. Type the web address in yourself.
2) The login pages of bank websites are secured through an encryption process, so a locked padlock or unbroken key symbol should appear in your browser window when accessing your bank site.
3) The beginning of your bank's internet address will change from 'http' to 'https' when a secure connection is made.
4) Be wary of any unexpected or suspicious looking pop-ups that appear during your online banking session
5) Check the online banking security options your bank provides; some offer free anti-virus and browser security software

How to Bank Safely Online

6) Check your bank statement regularly and contact your bank immediately if you spot any transactions that you didn't authorize
7) When sending money via your online bank account, always double check the amount you are sending as well as the account number and sort code you are sending it to
8) Fraudsters sometimes try to trick people into making a real payment by claiming "it's just a test"
9) Make sure that your bank has your up-to-date contact details
10) Never give anyone your login details in full either by email or over the phone – your bank will never request these in this way

How to File a Complaint ?

1. FBI's Internet Crime Complaint Center	https://www.ic3.gov/Home/ComplaintChoice
2. National Cyber Crime Reporting Portal	https://cybercrime.gov.in/
3. Cyber Crime Unit (Delhi Police)	http://www.cybercelldelhi.in/Report.html
4. Digital Police	https://digitalpolice.gov.in/
5. Indore Police	http://www.indorepolice.org/
6. Federal Trade Commission	https://identitytheft.gov/ and https://reportfraud.ftc.gov/
7. Cyber Tipline	https://www.missingkids.org/gethelpnow/cybertipline
8. Identity Theft Resource Center	https://www.idtheftcenter.org/
9. Office of the Inspector General	https://oig.ssa.gov/report-fraud-waste-or-abuse
10. CERT-in (INDIA)	https://www.cert-in.org.in/

THANK YOU

The only system which is truly secure is one which is switched off and unplugged, so the only way to be safe is **Pay attention** and **Act smart**.

{ Any Enquiry }

chetansoni@cdac.in
http://www.infosecawareness.in & http://isea-pmu.in/

CDAC-Mohali
Centre for Development of Advanced Computing, MeitY, Govt. of India.