Lecture -4 (BDU)

28/01/2019

- **Phishing**

It is a criminal fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. It is a type of deception designed to steal person's identity.
Email spamming is mostly used for it.

# Types of spam email -

- Unsolicited bulk email (UBE)
- Unsolicited commercial email (UCE)

CANSPAM 2003 - against spamming

# Target of phishers -

- Banking sector (recent attack on HSBC)
- Social media
- Online shopping / E-commerce (like Amazon)
- Online auction (like eBay)

Scanned with CamScanner

# To maximize their chances, phishers use following tactics

- Name of legitimate organization
- From a real employee.
- URL that looks right.
- Urgent message.

# Ways to minimize spam threat

- Share your email with only limited people.
- Never reply to a spam mail.
- Make a habit to preview an email before opening it.
- Use alternate mail addresses for different e-commerce sites.
- Never use email address as screen name in public chats.
- Never respond to a spam email asking to remove your email address from the mailing distribution list.
- Disguise the email address on public website or groups by spelling out the sign.

- **Spam bots** - Program which generates spam mail. Also called web crawler, as it gathers list of email addresses to spam.

Scanned with CamScanner

- Hoax mail - These are deliberate attempts to devise or trick a user into believing or accepting that something is real when the hoaxer knows it is fake.

  To verify hoax mails -

  www.breakthechain.org

  www.hoaxbusters.org

Scanned with CamScanner