

Social Engineering and Phishing Attacks

A large, semi-transparent watermark of the NPTEL logo is centered in the background. It features a circular emblem with a stylized flower or star in the center, surrounded by a ring of text, and the word 'NPTEL' in large, bold, sans-serif letters below it.

DR. NEMINATH HUBBALLI

Outline

- ❑ Social Engineering Attacks
- ❑ Forms and means of Phishing Attacks
- ❑ Phishing today
- ❑ Staying safe
 - ❑ Personal level defense
 - ❑ Enterprise level defense
 - ❑ Role of banks and financial institutions



Case Study: Phone Phishing Experiment

50 users were contacted

Managed to get e-banking passwords

Response to Phone Phishing Experiment	Number of Employees
Giving away their full e-banking credentials(user name & password)	16
Giving away only their e-banking user name without password	8
Refused to reveal their credentials or any kind of information	26
Total	50

Source: Experimental Case Studies for
Investigating E-Banking Phishing
Intelligent Techniques and Attack Strategies

Social Engineering

❑ Is a method to stage a cyber attack through human interaction and errors.

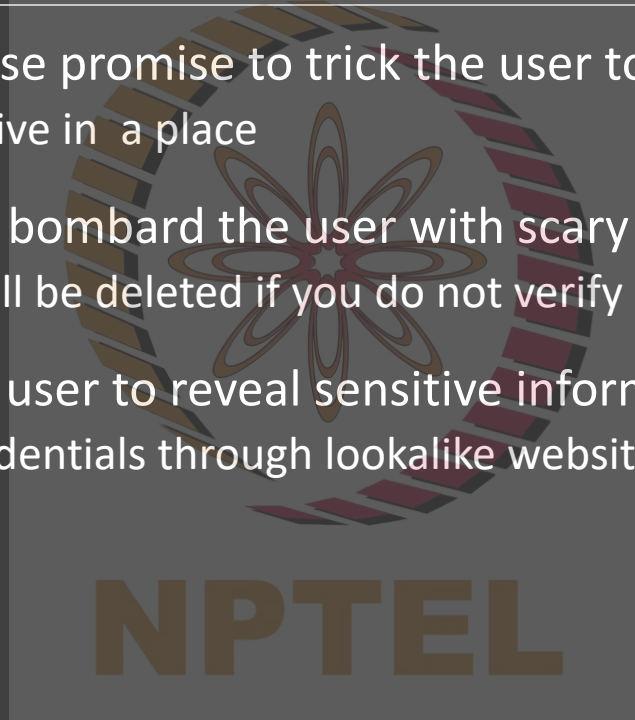
❑ Stages

1. Investigation: Preparing ground
2. Hook: Gain foothold
3. Play: Expand the foothold
4. Exit: Erase all traces



Social Engineering: Types

- ❑ Baiting: Make a false promise to trick the user to do something.
 - ❑ Ex: Leave a flash drive in a place
- ❑ Scareware: Falsely bombard the user with scary messages
 - ❑ Ex: Your account will be deleted if you do not verify
- ❑ Phishing: Trick the user to reveal sensitive information.
 - ❑ Ex: Collect user credentials through lookalike websites



Phishing Attacks in India and Globally

India lost around \$53 million (about Rs 328 crore) due to phishing scams with the country facing over 3,750 attacks in July-September 2017

4th Largest target of phishing attacks in the world

7% of global phishing attacks are targeted in India

US tops the rank with 27% of phishing attacks

Courtesy: The Hindu Business <http://www.thehindubusinessline.com/industry-and-economy/info-tech/india-lost-53-m-to-phishing-attacks-in-q3/article5414170.ece>

Phishing Attack

It is made-up of

- Phreaking + Fishing = Phishing
- Phreaking = making phone calls for free back in 70's
- Fishing = Attract the fish to bite



There are lot of fishes in pond
Lure them to come and bite
Those who bite become victims

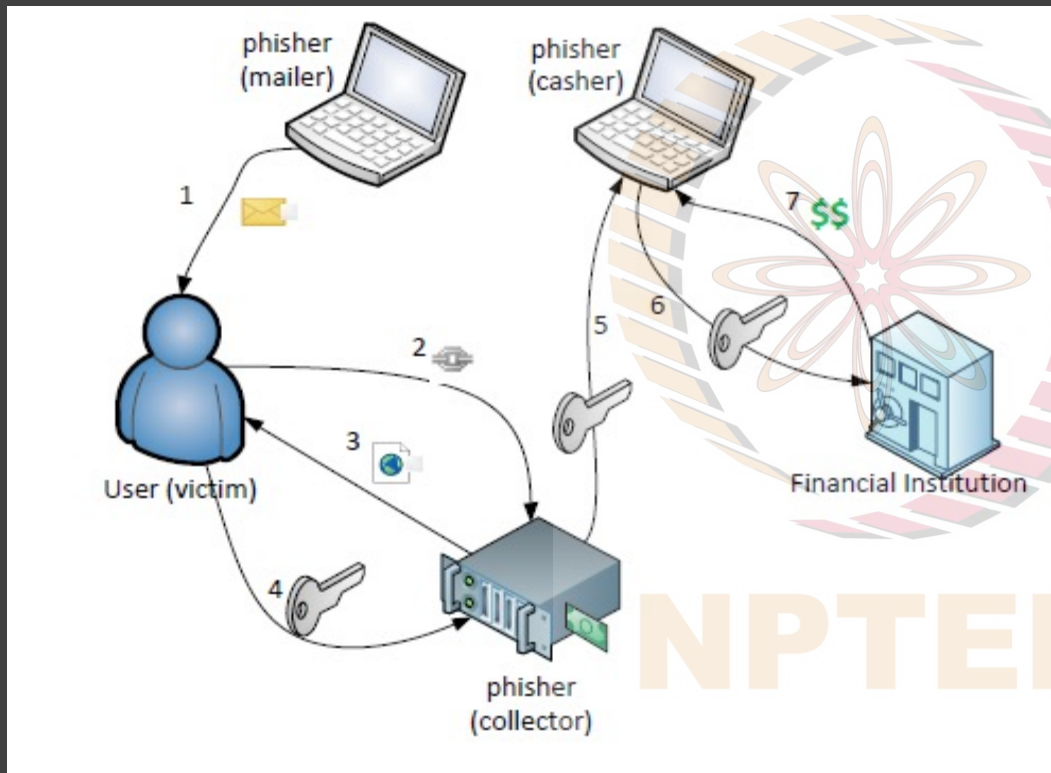
Courtesy: Google Images

Phishing Attack

- ❑ Phishing is a form of social engineering attack
 - ❑ Not all social engineering attacks are phishing attacks !
- ❑ Mimic the communication and appearance of another legitimate communication and companies
- ❑ The first fishing incident appeared in 1995
- ❑ Attractive targets include
 - ❑ Financial institutions
 - ❑ Gaming industry
 - ❑ Social media
 - ❑ Security companies



Phishing Information Flow



Three components

- Mail sender: sends large volume of fraudulent emails
- Collector: collect sensitive information from users
- Cashier: use the collected sensitive information to en-cash

Courtesy: Junxiao Shi and Sara Saleem

Phishing Forms

❑ Misspelled URLs

- ❑ www.sbibank.statebank.com

- ❑ www.microsoft.com

- ❑ www.mircosoft.com

❑ Creating anchor text

- ❑ `<a href = "anchor text" > Link Text </a>`

- ❑ Link Text

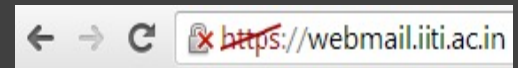
❑ Fake SSL lock

- ❑ Simply show it so that users feel secure

❑ Getting valid certificates to illegal sites

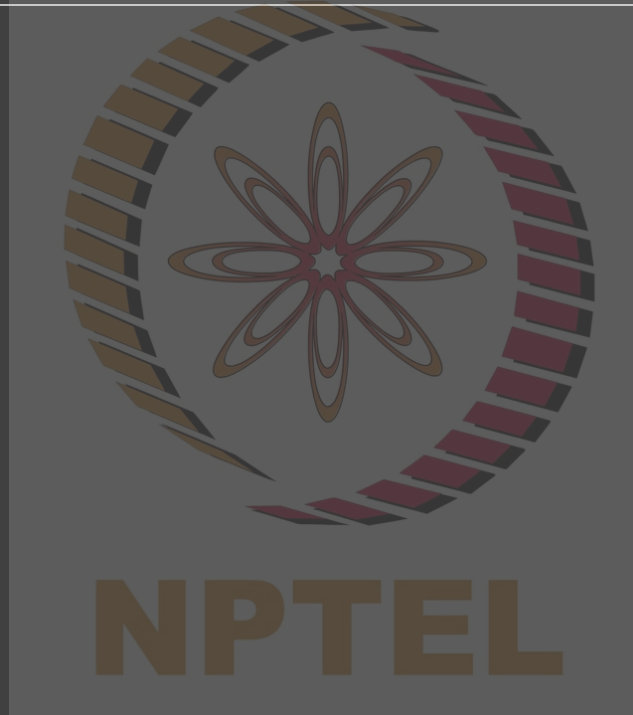
- ❑ Certifying agency not being alert

❑ Sometimes users overlook security certificate warnings



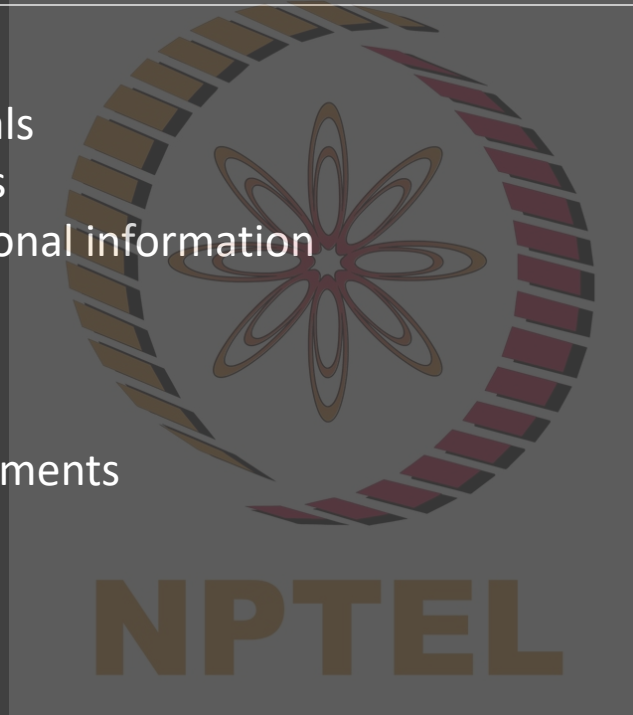
Phishing Payload

- ☐ Keyloggers
- ☐ Spyware
- ☐ Screen Grabber
- ☐ Bot



Phishing Purpose

- ☐ Login credentials
- ☐ Banking credentials
- ☐ Credit card details
- ☐ Address and personal information
- ☐ Trade secrets
- ☐ DDoS agent
- ☐ Botnet growth
- ☐ Confidential documents



Types of Phishing

❑ Clone Phishing:

- ❑ Phisher creates a clone email
- ❑ By getting contents and addresses of recipients and sender

❑ Spear Phishing:

- ❑ Targeting a specific group of users
- ❑ All users of that group have something in common
 - ❑ Targeting all faculty members of IIT

❑ Phone Phishing:

- ❑ Call someone and say you are from bank
- ❑ Ask for password saying you need to do maintenance



Email Spoofing for Phishing

An email concealing its true source

Ex. customer care@sbi.com when it is actually coming from somewhere else

Send an email saying your bank account needs to be verified urgently

When the user believes

- Sends her credit card
- Gives her password

Sending spoofed email is very easy

- There are so many spoof mail generators

Sample Email

Subject: Westpac official notice

Westpac
Australia's First Bank

Dear client of the Westpac Bank,

The recent cases of fraudulent use of clients accounts forced the Technical services of the bank to update the software. We regret to acknowledge, that some data on users accounts could be lost. The administration kindly asks you to follow the reference given below and to sign in to your online banking account:

<https://oib.westpac.com.au/ib/default.asp>

We are grateful for your cooperation.

Please do not answer this message and follow the above mentioned instructions.

Copyright © 2004 - Westpac Banking Corporation ABN 33 007 457 141.

Phishing Today

- ❑ Use bots to perform large scale activity
 - ❑ Relays for sending spam and phishing emails
- ❑ Phishing Kits
 - ❑ Ready to use
 - ❑ Contain clones of many banks and other websites



Phishing Today

Uncommon encoding mechanisms

Hexadecimal	%68%74%74%70%3a%2f%2f%77%77%77%2e%65%78%61%6d%70%6c%65%2e%63%6f%6d
ASCII Text	http://www.example.com

Fake banner advertisements



NPTEL

❑ Phishing Today

❑ Dynamic code

- ❑ Phishing emails contain links to sites whose contents change
- ❑ When email came in midnight it was ok but next day when you clicked it is spreading malware

❑ Numbers (IP address) in urls 20.100.23.45

❑ Use of targeted email

- ❑ Gather enough information about user from social networking sites
- ❑ Send a targeted email using the knowledge of previous step
- ❑ Unsuspecting user clicks on link
- ❑ Attacker takes control of recipient machine (backdoor, trojan)
- ❑ Steal / harvest credentials

Personal Level Protection

❑ Email Protection

- ❑ Blocking dangerous email attachments
- ❑ Disable HTML capability in all emails

❑ Awareness and education

❑ Web browser toolbars

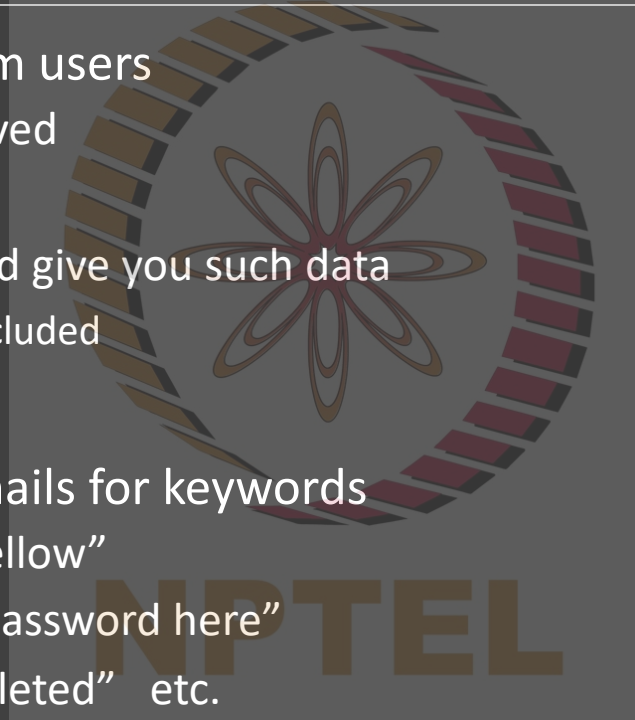
- ❑ Connect to a database of FQDN IP address mapping of Phishing sites



❑ Multifactor authentication

Enterprise Level Protection

- ❑ Collecting data from users
 - ❑ About emails received
 - ❑ Websites links
 - ❑ Why any one should give you such data
 - ❑ Her interest also included
 - ❑ Incentives
- ❑ Analyzing spam emails for keywords
 - ❑ “click on the link bellow”
 - ❑ “enter user name password here”
 - ❑ “account will be deleted” etc.
- ❑ Personalization of emails
 - ❑ Every email should quote some secrete that proves the identity
 - ❑ Ex: Phrase as Dear Dr. Neminath Instead of Dear Customer
 - ❑ Referring to timing of previous email



What Banks are Doing to Protect from Phishing

- ❑ Banks and their customers lose crores of rupees every year
- ❑ They hire professional security agencies who constantly monitor the web for phishing sites
- ❑ Regularly alert the users “to be alert” and not to fall prey
- ❑ Use best state of the art security software and hardware
- ❑ White list and blacklist of phishing sites

