Phishing Attacks

Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, PIN, bank account, credit card details by masquerading as a trustworthy entity details through electronic communication means like e-mail.

Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users.

How does a phishing email message look like? In detail ….

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling — *Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:*

http://www.facebook.com/application_form — Links in email

Note: If you dont fill the application your account will be permanently blocked. — Threats

Regards,

Facebook Copyrights Department. — Popular company

- Spelling and bad grammar.
- Links might also lead you to .exe files. These kinds of file are known to spread malicious software.
- Threats

  Sometimes you may receive a threat mail saying that your webmail account would be closed if you do not respond to an e-mail message. The e-mail message shown above is an example of the same trick. Cybercriminals often use techniques to make one belive that security has been compromised.
- Spoofing popular websites or companies.

  Scam artists use graphics in email that look identical to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.
- Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.
- Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license.

steps to remember

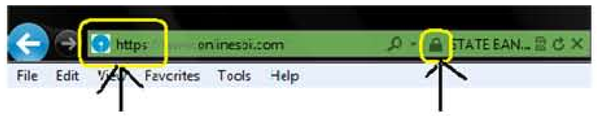
***Step1:* Cross check the URL in the browser**

Don't enter your information in the websites that start with numbers

***Step2:* Always check for the misspelled URL**

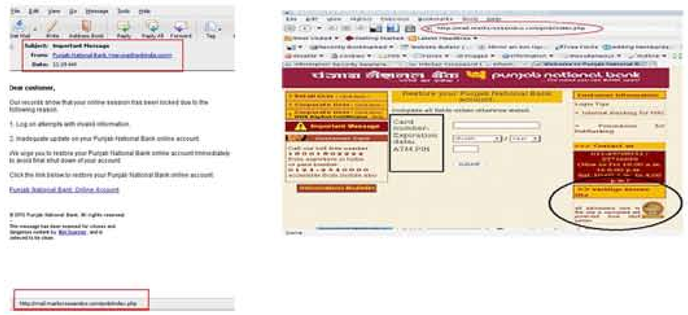
So Always key in the URL in the address bar yourself don't copy and paste

***Step3:* Always perform online banking in secure channel i.e check for the Padlock and secure channel for secure banking**



Always check for the trusted website which has https and padlock

***Step 4:* Always view any email request for financial or other personal information with suspicion, particularly any "urgent" requests. When in doubt, do not respond to questionable email or enter information on questionable websites. You may also contact the alleged sender to confirm the legitimacy of communications you've received.**



An Example of Phishing site, the look and feel of the Punjab national bank is same.

Step 5: ***Never respond to the emails that ask for your personal information like credit card /debit card/bank information.***

Do's

- Be cautious about opening any attachments or downloading files you receive regardless of who sent them.

- Look for the sender email ID before you enter/give away any personal information.
- Use antivirus, antispyware and firewall software (update them regularly too).
- Always update your web browser and enable phishing filter.
- If you receive any suspicious e-mail do call a company to confirm if it is legitimate or not.
- Do use a separate email accounts for things like shopping online, personal etc.

Don'ts

- Don't reply to an e-mail or pop-up message that asks for personal or financial information.
- Don't e-mail personal or financial information i.e credit card or other sensitive information via e-mail.
- Don't click on any email or social media messages you don't expect or need.
- Don't open e-mail that you have any suspicion may not be legitimate. If it is legitimate and the individual trying to contact you really needs to, they will try another means.
- Don't open attachments that you were not expecting, especially ZIP files and NEVER run .exe files.
- Don't use your company e-mail address for personal things.
- Don't open any spam e-mail.
- Don't open suspicious videos or images in social networking sites since social networking are prime target of phishing.
- Never respond to phone calls asking for bank details. It might be vishing (voice phishing).
- Beware of phishing phone calls.
- Don't respond if you receive any message(sms) asking you to confirm account information that has been "stolen" or "lost" or encouraging you to reveal personal information in order to receive a prize, it's most likely a form of phishing.

Here are the few Phishing techniques….

- Social networking sites are now a prime target of phishing, since the personal details in such sites can be used in identity theft.
- One of the latest phishing techniques is tabnabbing. It takes advantage of the multiple tabs that users use and silently redirects a user to the affected site.
- **Filter Evasion** - Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.
- **Phone Phishing** - Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Visher sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.
- Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information.

How I can recognize a message of phishing?

- Normally phishing e-mails display grammatical errors or overlapped text.
- Test using false data before putting in actual information.

What should I do if I think I've responded to a phishing scam?

Take these steps to minimize any damage if you suspect that you've responded to a phishing scam with personal or financial information or entered this information into a fake website.

- Change the passwords or PINs of all your online accounts that you think could be compromised.
- Place a fraud alert on your credit reports. Check with your bank or financial advisor if you're not sure how to do this.
- Contact the bank or the online merchant directly. Do not follow the link in the fraudulent e-mail.
- Routinely review your bank and credit card statements for unexplained charges or inquiries that you didn't initiate .