Internet/Mobile Banking Security tips

Protecting your information

Phishing

What is Phishing?

Phishing is a global problem faced by Banks worldwide. It is an attempt to 'fish' for your banking details. Phishing could be an e-mail that appears to be from a known institution like banks / a popular website.

Please note that Banks will never ask for confidential data like login and transaction password, One Time Password (OTP), Unique Reference No. (URN), etc.

How does phishing happen?

- Phishers sets up a replica page of a known financial institution or a popular shopping website
- Bulk e-mails are sent to users asking for their personal data like account details, passwords etc
- When the user clicks on the link, the replica of the website will open. Or while the user is online, a form will populate through an "in-session pop-up"

How to identify a Phishing attempt?

- Unsolicited emails, calls from strangers or websites asking for confidential banking details
- Messages asking for urgent action due to security reasons
- Links received in emails to access known websites
- To check the actual website, roll the cursor over the link or check for https:// where "s" stands for 'secure site'
- The fraudster may use well known bank's email address, domain name, logo, etc to give an authentic look to the fake email
- Such fake emails will always address you by a generic salutation or address you by "Dear Net Banking Customer" or "Dear Bank Customer". Bank's authentic emails will always address you personally by your name e.g. "Dear Mr. Suresh Kumar"
- Very often, such fake emails are poorly drafted and may have spelling or grammatical mistakes
- Such fake emails will always encourage you to click on to a link to verify or update your confidential account information
- The links embedded in such fake emails may sometimes look authentic but when you move the cursor/pointer over the link, there may be an underlying link/url to a fake website

How to avoid Phishing?

- Do not open spam mails. Be especially cautious of e-mails that:
- Come from unrecognized senders.
- Ask you to confirm personal or financial information over the Internet and/or make urgent requests for this information.
- Are not personalized.
- Try to upset you into acting quickly by threatening you with frightening information.
- Do not click on links, download files or open attachments in e-mails from unknown senders. Be cautious even if the e-mail appears to come from an enterprise you do business with. It is a good practice to call up the concerned to confirm in case the e-mail is unexpected.
- Communicate personal information only via secure web sites. In fact:
- When conducting online transactions, look for a sign that the site is secure such as a lock icon on the browser's status bar or a "https:" URL whereby the "s" stands for "secure" rather than a "http:".
- Also, check if the website address is correct before conducting online transactions.

- Protect your computer by installing effective anti-virus / anti-spyware / personal firewall on your computer / mobile phone and update it regularly.
- Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.
- Do not disclose details like passwords, debit card grid values, etc. to anyone, even if they claim to be bank employees or on e-mails/links from government bodies like RBI, I.T. Dept., etc
- Type the web address in the browser. Do not use links received in e-mails.
- In case you have used a cyber cafe / shared computer, change your passwords from your own computer.
- Register for e-mail and mobile alerts to check your account regularly.
- Report any fraudulent incident to the Bank / institution on the number mentioned on the Debit / Credit card, bank / credit card statement or official website.
- Do not rely on the name and source in the "From" field of the email address as it may be easily manipulated by the fraudster to a valid email account of bank
- Always access your bank website by typing the URL in the address bar of your browser only
- Always check the authenticity of the software before downloading
- If you get an email asking for personal or credit/debit card information, please do not provide this information no matter how 'genuine' the page appears to be. Such pop-ups are most likely the result of malware infecting your computer. Please take immediate steps to disinfect your device
- Any bank or their representative will never send you emails to get your personal information, password or one-time SMS (high security) password. Such e-mails are an attempt to fraudulently withdraw money from your account through Internet Banking

Report phishing emails and texts.

- Forward phishing emails to spam@uce.gov – and to the organization impersonated in the email. Your report is most effective when you include the full email header, but most email programs hide this information. To ensure the header is included, search the name of your email service with “full email header” into your favorite search engine.
- File a report with the Federal Trade Commission at FTC.gov/complaint.
- Visit Identitytheft.gov. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.
- You can also report phishing email to reportphishing@apwg.org. The Anti-Phishing Working Group – which includes ISPs, security vendors, financial institutions and law enforcement agencies – uses these reports to fight phishing.

(Federal Trade Commission, Consumer Information , 2017)