ONLINE banking has drastically changed the entire scenario of the banking industry. As one of the most rapidly developing countries in the world, India has seen an enormous increase in online banking users in recent years. But along with that has come a sharp spurt in e-crime related to online banking.

There are several types of e-crime that exist in the banking sector today, of which one is phishing. The word "phishing" originally comes from the analogy that early Internet criminals used email lures to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" in the terminology is most likely linked to popular hacker naming conventions, such as 'Phreaks' which refers back to early hackers who were involved in 'phreaking' – the hacking of telephone systems. The term was coined in 1996 by hackers who were stealing America Online accounts by scamming passwords from unsuspecting AOL users.

Phishing, and consequent identity theft is proving to be one of the biggest threats plaguing the banking sector today. While online banking and, more recently, mobile banking may be a convenient alternative to long cumbersome queues, it is an unsafe option for customers who are unaware of the associated threats. India has the second-largest online banking market in the world, behind the US. The number of phishing websites targeting Indian banks increased by 35% in 2009. As per CERT-In (Computer Emergency Response Team), which controls and deals with computer security incidents in India, the number of internet security incidents reported to CERT-In by banks has gone up 32% since 2008.

The number of phishing websites瞄准ing credit card and online banking information has increased over 1,000 since 2008. In 2009, over a thousand websites were identified as phishing sites.

Beware of Online Identity Thefts

The transformation from traditional banking to e-banking has been a great leap. But increasing instances of phishing attacks and several other types of scams related to online banking have snared several victims. However, with a little awareness and vigilance you can prevent yourself from falling into the clutches of the scammers.
Phishing attacks

Phishing targets many kinds of confidential information, e.g. user names and passwords, access numbers, account numbers, bank account numbers, credit card numbers, social security numbers, bank account numbers, and personal information such as birthdates and mothers' maiden names. Phishing includes many different types of attacks, including:

- **Deceptive attacks**, in which users are tricked by fraudulent messages into giving out information. The most common vector for deceptive phishing today is email. In a typical scenario, a phisher sends deceptive email, in bulk, with a "call to action" that demands the recipient click on a link.

- **Malware attacks**, in which malicious software causes data compromises. Malware-based phishing refers generally to any type of phishing that involves running malicious software on the user's machine.

- **DNS-based attacks ("pharming")**, in which the lookup of host names is altered to send users to a fraudulent server. DNS-based phishing involves polluting the user's Domain Name System cache with incorrect information that will be used to direct the user to an incorrect location. A fake mail sent by the hackers tries to redirect the users to the wrong domain which seems to be the original one.

Phishing Attacks on Indian Banks

There have been reports of phishing incidents in India's large state-owned banks such as the Punjab National Bank, Bank of India, Union Bank of India, and large private sector banks like ICICI Bank, HDFC, Axis Bank, and Citibank India in the recent past. Phishers have not spared even the Reserve Bank of India (RBI) and the Indian Bank Association (IBA).

**Reserve Bank of India (RBI):**

In March 2010, the number of phishing websites on Indian government bank brands increased by 35%. Six banks were the primary targets, including the Reserve Bank of India (RBI). The attack on RBI continued in April, with two phishing websites being hosted on servers based in the USA. The phishing websites were hosted using a single server template, allowing the phisher to easily create phishing websites that would otherwise vary using the same template and could exist on the server of that bank.

In June 2010, the Reserve Bank of India (RBI) issued a warning about the new lottery scam in which a victim gets a call congratulating them on winning a lottery prize. Further, to convince the user, phishers use forged RBI certificates containing the name, official position, and signature of some officials to increase the fraud.

**Punjab National Bank:**

In January 2010, a malware infiltrated the Punjabi National Bank's website compromising the systems of several customers when they clicked a hyperlink provided at the bottom of the bank's homepage (www.pnbindia.com), during 9-11 January 2010. Net-Square, Ahmedabad (an IT security firm) informed the bank about the malware when an employee accessed the bank's website to view his father's account. He received a fake email from the Punjab National Bank. The email addressed recipients as "Dear Valued Customer," while its subject line read "Important Notification from Punjab National Bank." The text of the forged email stated that, it was an official warning from the Punjab National Bank and informed the recipient that as a result of failed login attempt, his account access had been restricted. In order to restore the account, a form attached had to be downloaded and filled as per instructions. The bank immediately took corrective steps.

Recently, a customer found a mail in the spam folder, which was almost similar to phishing mails. Here is the screenshot of the mail:

In March 2010, the number of phishing websites on Indian government bank brands increased by 35%. Six banks were the primary targets, including the Reserve Bank of India (RBI). The attack on RBI continued in April, with two phishing websites being hosted on servers based in the USA.
When a customer re-activates his online account, it directs the user on to a forged page that purportedly contains the user's important information. There are very minor differences, but not even regular users can easily notice the difference. The first difference is that, in the fake website, on the upper left corner a box for "Internet Banking" has been added. The second difference is that in the fake website "Information Bulletin" is missing. If the customer enters the user ID and password in the fake website, the next window that appears asks for User ID, ATM card number, email, and transaction password. If the customer fills up the required fields, a message appears: "Upgrade complete new protocols implements. Close Browser and give 24 hr for commit completion." Perhaps the bad language used could be a giveaway.

Bank of India: Here is another case of a bank being subjected to a phishing attack. The phishers use the local language to sound authentic to the user and make them believe that the email is coming from the bank's own site. The English language email diverts the user to the link given below and asks for the User ID, password and transaction password.

The Hindi email connects the user to the following link:
Industrial Credit and Investment Corporation of India Bank (ICICI):
An ICICI customer received a mail from a fraudulent URL, which is as under:

The subject of the mail is: "ICICI Bank Alert: Please Re-Confirm Your Online banking Details". There are links to the phishing or the fake ICICI site, which looks similar to the ICICI login page. When he clicked the link, he was directed to the fake ICICI site where he was asked to input all personal information including his account password, card number, security code in the card, and even passport information.

Housing Development Finance Corporation (HDFC):
An HDFC customer complained that he received a mail from HDFC Bank saying: "Your HDFC Bank Account Need Authentication. To Keep Your Account Activate Otherwise It Will Get Blocked". There was a link to login to the HDFC Bank account. When he moved his mouse over it, it pointed to some other IP address. To investigate further, he clicked the link and the page he got was exactly similar as the actual HDFC login page.

Axis Bank:
A customer of Axis Bank received a message from Axis Bank asking for his account information for improving the online services. Taken in by the fraud, the customer passed on necessary information including PIN to the phisher. He was shocked when he was informed that the email was a hoax, and that its sender had made a withdrawal of Rs.16,000 from his bank account, as reported by *Mid-Day* on June 30, 2009.
Citibank India: Now look at this message supposedly from the Citibank. When the customer clicked on the link, he saw the Citibank web page and a popup that prompted for login information. Although the Citibank web page actually came from Citibank, the popup came from a non-Citibank server. Victims who entered banking information in the popup gave their account information to an unknown scam artist.

Beware of Phishing

In India, the concept of phishing is relatively new. Scam mail generally targets those customers who lack experience in online banking or awareness of such activities. On the Internet's global black market—where stolen identities are bought and sold 24 hours a day—e-criminals can even purchase "phishing kits" that enable them to create a fake Web page that convincingly mimics a bank's log-in page. According to NASSCOM, an IT trade group based in India, more than 80 Indian banks lack the security safeguards they need to thwart attacks from phishers and identity thieves.

The RBI has talked about an alarming increase in bank frauds, especially in private banks, in comparison to public sector banks. Therefore, it is important that customers remain vigilant during online banking transactions. RBI has issued guidelines for banks to incorporate automatic system for providing additional authentication and validation, an online alert system for card transactions, and a notification system to detect and report fraudulent transactions to customers and banks in a timely manner.

The RBI has created a comprehensive document discussing security-related guidelines and strategies for banks. The guideline explains the types of risks associated with online banking (different types of attacks and the ways in which they can compromise a system, like sniffer attacks, DoS, and e-mail bombs), the technology and security standards, the legal issues involved, and regulatory and supervisory concerns. There are guidelines for training and awareness, authentication technologies like tokens, smart cards, and smart cards are described. The concept of firewalls, proxy servers, cryptography, digital signatures, certification, SSL, and PKI are explained in detail.

The RBI also recommends that customers use secure means to log on to their online banking accounts. The customer should always log on to the site using the browser and not click on any link in an email or a popup window.

1. Identify the place of origin: Phishing emails can look like real email from the bank. However, the sender address is the key. This address is NOT a guarantee that it came from the person or organization it says it did. These emails are more likely to be sent from a different organization.

2. Dear Valued Customer: The emails containing text "Dear Valued Customer" in subject or in salutation are another way to trap phishing mail. Fraudsters use this word without knowing the real name or indeed anything else about the customer.

3. Take a closer look: No bank usually asks customers for their password or any other sensitive information by email. The message is also likely to contain odd "spelling" or capitalization in the "Subject:" box (this is an attempt to get around spam filter software), as well as grammatical and spelling errors.

4. It is always suggested NOT to log-on to online banking account by clicking on a link in an email or any popup window's link. It is better to open the web browser and type the bank’s address in the address bar. If in any doubt about the validity of an email purporting to come from your bank, contact them telephonically.

5. Security tools like scanners, sniffers, and IDSs are also described. Physical security is talked about followed by guidelines of a security policy and a number of recommendations. The recommendations talk about access control, isolation of application servers, security logs (audit trails), penetration testing, backup and recovery practices, monitoring against threats, and education.

(Continued on page 42)
Protection Measures

Fool them.

If you’re worried that you’ve reached a phishing site’s certificate to be authentic? VeriSign was guilty of issuing security certificates to sites that claimed to be part of Microsoft not so long ago. The latest versions of browsers, IE 7 and Opera 9 will soon be able to provide users with EV SSL (Extended Validation SSL) certificates that assure customers of being on a genuine site. The address bar shows green for the good guys and red for the doubtful ones.

Practically, it is impossible to eliminate the chance of identity theft completely. Individuals can affordably reduce their risk by

- Staying conscious on shared networks.
- SMS Alert Service. Nowadays almost all banks have started delivering only content from those in your address book.
- Be careful on online security questions. On opening of online account number. These emails will often warn of a problem with your account and then provide a link to a legitimate-looking site, hoping you will enter information such as your Social Security Number or account number. Be aware on phishing websites that typically ask for credit card and account numbers.
- Be aware of phishing emails. Phishing usually takes the form of authentic-looking emails that try to get you to reveal information such as your Social Security Number or account number. These emails often appear to come from acquaintances or colleagues. They may mimic your colleagues as high-ups. Stab phishing.
- Be aware of confusing websites. These are sites that look like online banking services but do not contain the security features of a genuine bank site. Be aware, not to give general information that is easily predictable or commonly known.
- Be careful on online security questions. On opening of online banking account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Be careful on shared networks. Be aware.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Be careful on shared networks. Be aware.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
- Always go through a link in a new browser window. Always close your browser while using online banking. Some of your account information may stay in your browser’s memory—and accessible to others—until the browser is closed.
New scams. As consumers are wising up to their scams, phishers are moving on to newer media to launch their scams. Mobile phones, a necessity in today’s world, are the latest ones to get targeted.

Image with a message saying: "Ignore these messages, they are always spam."

Biometrics supported transactions with required details. To bring online banking frauds to a halt, one has to spruce up the security system that only accepts the biometrics of the accessseer and the joint holder along with other required details that cannot be stolen from the database. Such a measure will not only stop fraud but also add credibility in banking affairs.

Always follow bank instructions. Banks say that appropriate upgradations are carried out from time to time by their IT departments for risk mitigation. They urge customers to be aware and follow instructions. A recent online banking transaction carried out in the account appears on the account holder’s screen as a record of the transaction.

Since the sums of money made by criminals through such banking scams are huge, the complexity and frequency of attacks will continue to rise. Awareness about the tools available for fighting phishing attacks as well as of the appearance and mechanics of a phishing attack is absolutely crucial in online banking. Customers using online banking should also update their anti-virus software and browser application, so that their computers do not support any spam or any back door entry.

Better communication and customer awareness is the key to a better online banking environment and better banking. RBI had been wise to clarify in its online banking guidelines that if banks do not adopt digital signatures, they have to take the legal risk. This single line is sufficient to say that the system is safe and there is no need to fear for funds. Better communication and customer awareness is the key to a better online banking environment and better banking.

Mr Prshant Kumar is Manager, Library, Punjab National Bank, Central Staff College, 8, Underhill Road, Civil Lines, Delhi-110054; Email: prashantkumar@pnb.co.in

Dr. Bhaskar Mukherjee is Assistant Professor, Department of Library and Information Science, Banaras Hindu University, Varanasi, Uttar Pradesh-221005; Email: mukherjee.bhaskar@gmail.com