

## **BEWARE OF FRAUDS**

Various types of frauds are known to have been perpetrated the world over. While you may not have fallen prey to any of them, thankfully, it's our responsibility to make you aware of them so that you are alert of how to protect your money.

Online fraud occurs when someone poses as a legitimate company (that may or may not be in order to obtain sensitive personal data and illegally conducts transactions on your existing accounts. Often called “phishing” or “spoofing”, the most current methods of online fraud are usually through fake emails, Web sites and pop-up windows , or any combination of such methods.

The main objective of online fraud is to steal your ‘identity’. This phenomenon is commonly known as "identity theft". Identity theft occurs when someone illegally obtains your personal information — such as your credit card number, bank account number, or other identification and uses it repeatedly to open new accounts or to initiate transactions in your name.

Identity theft can happen even to those who do not shop, communicate, or transact online. A majority of identity theft happens offline. Stealing wallets and purses, intercepting or rerouting your mail, and rummaging through your trash are some of the common tactics that thieves can use to obtain personal information. The more you are aware about identity theft the better prepared you will be.

## **PHISHING**

### *What Is Phishing?*

Phishing is an attempt by fraudsters to 'fish' for your banking details. A phishing attempt usually is in the form of an e-mail that appears to be from your bank. The e-mail usually encourages you to click a link in it that takes you to a fraudulent log-on page designed to capture your details. E-mail addresses can be obtained from publicly available sources or through randomly generated lists. Therefore, if you receive a fake e-mail that appears to be from your Bank, it does not mean that your e-mail address, name, or any other information has been taken from our systems.

### *How The Fraudsters Operate?*

Fraudsters send fake e-mails claiming that your information has been compromised, due to which your bank account has been de-activated/suspended, and ask you to hence confirm the authenticity of your information/transactions like credit card number, personal identification number (PIN), passwords or personal information, such as mother's maiden name. In order to prompt a response, such e-mails usually resort to using statements that convey an urgent or threatening condition concerning your account.

While some e-mails are easy to identify as fraudulent, others may appear to be from a legitimate source. However, you should not rely on the name or address in the “From” field alone, as this can be easily duplicated.

Very often, such phishing e-mails may contain spelling mistakes. Even the links to the counterfeit websites may contain URLs with spelling mistakes, to take you to a fake website which looks like that of your bank.

Some fake e-mails promise a prize or gift certificate in exchange for your completing a survey or answering a few questions. In order to collect the alleged prize, you may be asked to provide your personal information.

Fake e-mails appear to be sent by companies to offer a job. These are often for work-at-home positions that are actually schemes that victimize both the job applicant and other customers.

Fake e-mails may direct you to counterfeit websites carefully designed to look real. Hence such websites may look very similar and familiar to you, but are in fact used to collect personal information for illegal use.

Such e-mails attempt to convey a sense of urgency or threat. Example: “Your account will be closed or temporarily suspended if you don't respond.” Or, “You'll be charged a fee if you don't respond.”

#### Examples of Phishing E-mails

**Date of e-mail****New Innovation! 13-02-2009****Instructions to credit your account with the sum of US\$6,500,000.00 18-12-2008****Urgent Notification! From XYZ Internet Banking 25-08-2007****Confirm your online account details! (Message id: b38403334) 10-08-2007****XYZ Bank Technical Verification****31-07-2007****Alerts !!! Upgrade and Secure Your Online Account Immediately 31-10-2006****Urgent Security Warning****05-07-2006****XYZ Online Banking Account Security Upgrade****25-06-2006**

### *Tips To Protect Yourself from Phishing*

1. If you receive an e-mail requesting your Internet Banking security details like PIN, password or account number, you should not respond.
2. Whenever you use a link to access a website, be sure to check for the URL of the website and compare it with the original. We recommend that you type in the URL yourself whenever you access your bank website or bookmark/store the URL in your list of 'Favourites'.
3. Delete suspicious e-mails without opening them. If you happen to open them, do not click any link or attachment they may contain.
4. If you receive a job offer via e-mail, ensure that it's from a genuine and reputed company.

## **SPOOFING**

### *What Is Spoofing?*

Website spoofing is the act of creating a website, as a hoax, with the intention of performing fraud. To make spoof sites seem legitimate, phishers use the names, logos, graphics and even code of the actual website. They can even fake the URL that appears in the address field at the top of your browser window and the Padlock icon that appears at the bottom right corner.

### *How The Fraudsters Operate?*

Fraudsters send e-mails with a link to a spoofed website asking you to update or confirm account related information. This is done with the intention of obtaining sensitive account related information like your Internet Banking user ID, password, PIN, credit card / debit card / bank account number, card verification value (CVV) number, etc..

### *Tips To Protect Yourself from Spoofed Websites*

1. If you receive an e-mail requesting your Internet Banking security details like PIN, password or account number, you should not respond.
2. Check for the Padlock icon: There is a de facto standard among web browsers to display a Padlock icon somewhere in the window of the browser. For example, Microsoft Internet Explorer displays the lock icon at the bottom right of the browser window. Click (or double-click) on it in your web browser to see details of the site's security. It is important for you to check to whom this certificate has been issued, because some fraudulent websites may have a padlock icon to imitate the Padlock icon of the browser.
3. Check the webpage's URL. When browsing the web, the URLs (web page addresses) begin with the letters "http". However, over a secure connection, the address displayed should begin with "https" - note the "s" at the end.

## VISHING

### *What Is Vishing?*

Vishing is a combination of Voice and Phishing that uses Voice over Internet Protocol (VoIP) technology wherein fraudsters feigning to represent real companies such as banks attempt to trick unsuspecting customers into providing their personal and financial details over the phone.

### *How The Fraudsters Operate?*

A typical vishing attack could follow a sequence such as this:

- The fraudster sets up an automatic dialler which uses a modem to call all the phone numbers in a region.
- When the phone is answered, an automated recording is played to alert the customer that his/her credit card has had illegal activity and that the customer should call the recorded phone number immediately. The phone number is with a caller identifier that makes it appear that they are calling from the financial company they are feigning to represent.
- When the customer calls the number, it is answered by a computer-generated voice that tells the customer they have reached 'account verification' and instructs the consumer to enter his/her 16-digit credit card number on the key-pad. A visher may not have any real information about the customer and would address the customer as 'Sir' and 'Madam' and not by name or the prefix 'Mr....' or 'Ms...!'.  
• Once a customer enters his/her credit card number, the "visher" has all of the information necessary to place fraudulent charges on his/her card. Those responding are also asked for the security number found on the rear of the card.
- The call can then be used to obtain additional details such as security PIN, expiry date, date of birth, bank account number, etc.

### *Tips To Protect Yourself from Vishing*

1. Your bank would have knowledge of some of your personal details. Be suspicious of any caller who appears to be ignorant of basic personal details like first and last name (although it is unsafe to rely on this alone as a sign that the call is legitimate). If you receive such a call, report it to your bank.
2. Do not call and leave any personal or account details on any telephone system that you are directed to by a telephone message or from a telephone number provided in a phone message, an e-mail or an SMS especially if it is regarding possible security issues with your credit card or bank account.
3. When a telephone number is given, you should first call the phone number on the back of your credit card or on your bank statement to verify whether the given number actually belongs to the bank.

## SKIMMING

### *What Is Skimming?*

Skimming is a method used by fraudsters to capture your personal or account information from your credit card. Your card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read into and stored on the skimmer or an attached computer. Skimming is a tactic used predominantly to perpetrate credit-card fraud – but it is also a tactic that is gaining in popularity among identity thieves.

#### *How The Fraudsters Operate?*

##### At ATM machines

Fraudsters insert a skimming device to the ATM's card slot. This device scans the card and stores its associated information. While a customer keys in his PIN, the wireless skimming device transfers the data to the fraudsters. This information is then used by the fraudsters for online shopping or to make counterfeit credit cards.

##### At Restaurants / Shopping Outlets

At restaurants and shopping outlets, the credit card is swiped twice, once for the regular transaction and the other in the skimmer that captures the personal information which is retrieved later by the fraudsters.

#### *Tips To Protect Yourself from Skimming*

1. Sign on the reverse of your credit card as soon as you receive it.
2. Collect your receipts / charge slips at ATM's, restaurants and shopping outlets.
3. Use your card with merchants that you know and can trust. Never allow a shopkeeper to take your card to a different shop/room for swiping.

## **MONEY MULE**

#### *What Is Money Mule?*

Once the fraudster has captured personal information using anyone of the ways mentioned above, they need an account to which they can transfer funds from the compromised account. This is where a “Money Mule” comes into picture. A Money Mule is an unwitting participant in the frauds who is recruited by fraudsters to launder stolen money across the globe.

#### *How The Fraudsters Operate?*

Fraudsters contact prospective victims (money mules) with job vacancy ads via spam e-mail, Internet chat rooms or job search Web sites. Jobs usually are advertised as financial management work, and ads suggest that no special knowledge is required.

The crime rings persuade the victim to come and work for their fake company. Some fraudsters even ask mules to sign official-looking contracts of employment.

Once recruited, money mules receive funds into their accounts. These funds are stolen from other accounts that have been compromised.

Mules then are asked to take these funds out of their accounts and forward them overseas (minus a commission payment), typically using a wire transfer service.

As the account of the mule has been involved in the transaction, the mule also becomes an unwitting participant in the frauds.

#### *Tips To Protect Yourself from Money Mule*

1. Be cautious about any unsolicited offers or opportunities offering you the chance to make some easy money. Be especially wary of offers from people or companies overseas as it is harder for you to find out if they really are who they say they are.
2. Money mule adverts or offers can take a variety of different forms and they may even copy a genuine company's web site and register a similar web address to add authenticity to the scam.
3. These adverts will normally state that they are an overseas company seeking "representatives" or "agents" to act on their behalf for a period of time, sometimes to avoid high charges for making payments, or local taxes.
4. The advert may be written in poor English with grammatical and spelling mistakes and they may urge you not to inform the bank or the police about the reason for making the payments. The adverts may seek people with accounts at certain banks, or Internet payment systems.
5. Take steps to verify any company which makes you a job offer and check their contact details (address, phone number, email address and web site) are correct and whether they are registered.

#### **COUNTERFEIT WEB SITES**

Online thieves often direct you to fraudulent Web sites via email and pop-up windows and try to collect your personal information. One way to detect a phony Web site is to consider how you arrived there. Generally, you may have been directed by a link in a fake email requesting your account information. However, if you type, or cut and paste, the URL into a new Web browser window and it does not take you to a legitimate Web site, or you get an error message, it was probably just a cover for a fake Web site.

#### **NIGERIAN 4-1-9 SCAM**

This scam is often referred to ironically as the 4-1-9 scam after section 4-1-9 of the Nigerian Penal Code, which relates to fraudulent schemes.

The scam starts with bulk mailing/e-mailing of offers asking the recipients to enter into a business or to extend help in getting money transferred in return for huge commission.

The most common forms of these fraudulent business proposals are:

- Offer of disbursement of money from wills
- Contract fraud (purchase of goods or services)
- Purchase of real estate
- Transfer of funds from over-invoiced contracts
- Sale of crude oil at below market prices

#### *Other Indications*

- There is always a sense of urgency.

- There are many foreign-looking documents and sometimes, references of actual Nigerian government buildings are used.
- Often, blank letterheads and account numbers are requested.
- There is a variety of processing fees or bribes that must be paid, and the transaction is asked to be kept confidential.

*Remember*

- Use caution while dealing with foreign buyers and sellers
- Beware if the buyer or seller asks you to send money quickly.
- No legitimate company will offer to pay you by arranging to send you a cheque and asking you to wire some of the money back. If that's the pitch, it's a scam.
- If it sounds too good to be true, it is .

## **SAFETY MEASURES**

### **Internet Banking Safety**

*Use Internet Banking To Minimise the Risk of Fraud*

- Utilize paperless options. Restrict receipt of paper statements by subscribing to e-mailed bank account statements, credit card statements and demat account statements.
- Monitor your account activity regularly by checking your balances and statements online. This helps you to detect fraudulent transactions, if any, quickly. The earlier a fraud is detected, the lesser will be its financial impact.
- Restrict the use of cheques. Transfer funds online between your Bank accounts or send money to other Bank customers through your bank website.
- Receive and pay bills online for free with Bill Pay facility. Fewer the personal documents sent through the mail, lesser the chance of fraud.
- Register for Mobile Banking and receive alerts upon all significant transactions in your account. Learn more about Mobile Banking.

*Tips for Use When Banking Through the Internet*

1. Avoid accessing your Internet Banking account from a cyber cafe or a shared computer. However, if you happen to do so change your passwords from your own computer.
2. Every time you complete your online banking session, log off from your bank website. Do not just close your browser.

3. To access your Bank's Internet Banking, always type in the correct URL into your browser window. Never click a link that offers to take you to our website.
4. If your log-in IDs or passwords appear automatically on the sign-in page of a secure website, you should disable the "Auto Complete" function to increase the security of your information.
5. To disable the "Auto Complete" function:
  - Open Internet Explorer and click "Tools" > "Internet Options" > "Content".
  - Under "Personal Information", click "Auto Complete".
  - Uncheck "User names and passwords on forms" and click "Clear Passwords".
  - Click "OK".
6. Change your Internet Banking passwords (both log-in password and transaction password) after your first log-in, and thereafter regularly (at least once in a month).
7. Your password should be complex and difficult for others to guess. Use letters, numbers and special characters [such as !,@, #,\$, %, ^, &,\* (, )] in your passwords.
8. For additional security to financial transactions through Internet Banking, create and maintain different passwords for log-in and for transactions.
9. If you have more than one Internet Banking user ID, use a different password for each of the user IDs.
10. Never share your Internet Banking passwords with others, even family members. Do not reveal them to anybody, not even to your Bank employee.
11. Always check the last log-in to your Internet Banking account.

### **E-mail Safety Measures**

#### *E-mail Safety Tips*

1. If you receive an e-mail requesting your Internet Banking details like your PIN, password, account number, you should not respond.
2. Delete suspicious e-mails without opening them. If you happen to open them, do not click any link or attachment they may contain.
3. Secure your computer, read our "Computer Safety Measures".

### **Computer Safety Measures**

### *Install and Update Anti-Virus Software*

Always protect your computer by using up-to-date anti-virus software that is capable of scanning files and e-mail messages for viruses. This will prevent your files getting corrupted or lost and also prevent your computer from getting infected with the virus.

Anti-virus software protects you from Trojan horses. Trojan horses are sent to computer systems typically through e-mail. They are particularly dangerous because they have the potential to allow others to gain control of your computer system remotely, without your knowledge or consent. These programs can capture and send sensitive information stored on your hard drive to any other person who has gained remote access to your computer.

### *Use a Personal Firewall*

Any computer or device connected to the Internet that is not properly protected is vulnerable to a variety of malicious Internet intrusions and attacks. This applies to all users of cable modems, digital subscribe lines (DSL) and dial-up lines. However, cable modem and DSL users are particularly vulnerable because both connection methods provide "always-on" connection capability. The likelihood of a malicious person entering your computer increases significantly the longer your computer is on and is connected to the Internet.

A personal firewall will help protect you from intrusion. Firewalls create a barrier between your computer and the rest of the Internet. A firewall can be a hardware device, a software application or a combination of the two. Firewalls can prevent malicious attacks and block certain types of data from entering your computer or private network. They can also be set up to alert you if anyone tries to access your system.

### *Keep Your Browser and Operating System Up-To-Date With Software Updates*

The software you use and the Internet itself can impact the security of your online activities. Therefore, you should watch for security bulletins that warn you of various security "holes" or "bugs" that may impact the software and web browser you are using. It is very important to check the websites of your operating system and web-browser vendors for software "patches" and "updates". Some operating systems and software can be configured to automatically check for new updates.

### *Activate a Pop-Up Blocker*

Several free, publicly available programs exist that will block all pop-up windows from occurring while you are online. You can download such programs from the Internet.

### *Scan Your Computer For Spyware Regularly.*

Spyware and adware are programs that monitor your Internet activity and potentially relay information to a disreputable source. Free spyware-removal programs are available on the Internet.

### *When You Are Not Using Your Computer, Shut It Down Or Disconnect It From The Internet.*

Do not leave your computer unattended for a long time. When not in use, disconnect from the Internet or shut it down.

## **Online Shopping Safety Measures**

### *Tips for Safe Online Shopping*

1. Be very sure of the website address. The website address is reflected in the address bar of your Internet browser. This check is recommended every time you access any website from a link given elsewhere. Always type the website address into the address bar or bookmark the websites that you use frequently.
2. Never enter, confirm or update your account-related details in a pop-up window.
3. If you tend to use your credit cards for online shopping frequently, make sure that you sign up for the Verified by VISA and/or MasterCard Secure Code program(s).
4. Confirm that the website is a secure one. Make sure any Internet purchase activity you engage in is secured by encryption to protect your account information. Look for "secure transaction" symbols.
5. Shop only from reputed websites. Beware of online offers that require you to provide your account details "for verification".

## **Tips on the Use of Mobile Banking**

### *Set up the password of your mobile phone*

Usually, all mobile phones have the optional feature of a password or a PIN which can be set up once you switch on the mobile phone or make some configuration changes. It is advisable to enable this feature.

### *Protect your mobile phone against virus*

- Like computers, a mobile phone – especially if it is a smart phone with GPRS – is vulnerable to viruses. Viruses may harm your phone when it is connected to the Internet. They may also give hackers the opportunity to access your mobile phone to steal or alter your personal information. Therefore, always ensure the following:
- Install anti-virus software in your mobile phone.
- Delete junk messages and chain messages.
- Do NOT follow any URL in messages that you are not sure about.
- Do NOT download any file from sites (e.g. applications, games, pictures, music) or people (e.g. e-mail attachment) that you are not sure about.

### *Beware of Trojans/Spyware*

- Do not download any software without verifying its security and privacy features from the website. We recommend the following to shield your device from this threat:

- Install anti-spyware software in your mobile phone. There are products designed specifically for PDAs (personal digital assistants) such as McAfee PDA Virus Scanner and PDA Spybot.
- Educate yourself on spyware. Be alert to any spyware-like activities on your mobile phone. Be suspicious if you get lots of unsolicited e-mails/messages.

*Always have the latest software updates of your mobile phone*

The manufacturer or dealer of your mobile may provide updated software for your mobile phone from time to time. You must check the availability of software updates, and install them regularly.

*Avoid sharing your mobile phone*

Do not forget the following if you have to share your mobile or send it for repair/maintenance:

- Remove the temporary files and the cache that were stored in the memory of the phone, as the temporary files and the cache may contain some of your sensitive information such as account numbers.
- Clear the browsing history regularly.
- Do NOT allow others access to your mobile phone before logging out from the sites (banking/financial/shopping) that you entered.

*Beware of online offers that require you to provide your account details for 'verification'.*

- Do not share your passwords with anyone.
- Banks will never ask you for your Internet Banking passwords on your mobile.

*Be cautious.*

Do not leave your Mobile Banking application session unattended. Always sign off from a session.

Acknowledgement: NPCI thanks ICICI Bank for preparing this article.