Safe Trading Tips

At ICICI Direct, we are committed to making your trading with us a wonderful experience. We have adopted several measures to enhance the security of your holdings and protection of your account. ICICI Direct's safe trading guidelines set out simple steps you can take to ensure that your money and your personal details are safe and secure.

Whether it's about online-trading security or traditional-trading security threats, BE INFORMED. Know how scamsters operate, know how to keep your password secure.

The following links will give you information about security issues, help you make the right decisions and hence avoid costly surprises.

Computer Safety:

1. Install and update anti-virus software.
2. Use a personal firewall.
3. Keep your browser and operating system up-to-date with Software Updates.
4. Activate a pop-up blocker.
5. Scan your computer for spyware regularly.
6. When you are not using your computer, shut it down or disconnect it from the internet.

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 subscriber 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.

For Safety tips and guidelines on how Internet Explorer 8 is safer and secure browser, please visit http://www.microsoft.com/windows/internet-explorer/features/safer.aspx

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.

Shut Down Your Computer, when Not in Use 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.

PIN And Password Safety Measures:

User ID Safety

Destroy the User ID mailer after memorizing the User ID.

Password Safety

1. Your password should be complex and difficult for others to guess. Use letters, numbers and special characters [such as !, @, #, $, %, ^, &, *(,)] in your passwords.

2. Don't use passwords that are obvious, like your name/nickname, names of your family members, your address, phone number, or any other information that a thief might find in your purse or wallet.

3. Do not use the same password as the one, which you use to log in to your computer or access your e-mail.

4. If your log-in IDs or passwords appear automatically on the sign-in page of a secure web site, you should disable the auto-complete function to increase the security of your information.

5. To disable the "Auto Complete" function
   a. Open Internet Explorer and click on "Tools">>"Internet Options">>"Content"
   b. Under "Personal Information", click on "Auto Complete
   c. Uncheck "User names and passwords on forms" and click on "Clear Passwords"
   d. Click "OK"

6. Change your Internet Trading password after your first log-in, and thereafter regularly (at least once in a 14 Days).

If you access any website (including icicidirect.com) from a cyber-cafe, any shared computer or a computer other than your own, change your passwords after such use in your own computer at your workplace or at home. It is very important to do so especially when you have entered your login password in such a cyber- cafe computer or shared computer.

Never share your passwords with others, including family members. Do not disclose your Online Trading password to anybody, not even to an ICICI Direct employee/Call centre employee.

Our Unique Features

Secure Login

For logging in into your icicidirect.com account, you need to use your Internet Trading user id and password. The web page on which you are required to input these details is a secure page.

When you login successfully, your web browser will establish a secure SSL connection between your computer and our Web servers. This will allow you to communicate with us privately and to conduct online transactions trading. How to identify a secured web page?

Number of Login Attempts

In case you are unable to provide the correct user id and password, you will not be granted access. After 3 unsuccessful login attempts, your user id will be blocked automatically by our system. To re-enable your Internet trading User ID, please call our 24-Hour Phone Trading numbers. After authenticating yourself, you can place your request for re-activation of your user id.

You may also request for re-issue of your Internet Trading passwords; in case you have forgotten them. In case of password lock you can unlock it online by filling the form in the link "Unlock trading account or Issue new password" of Customer Service section.

Timed Logout

Our unique security features continue to protect you once you have logged in successfully. To protect your accounts against unauthorized access, our systems are designed to automatically terminate a secure online session if extended inactivity is detected. Hence if you login and leave your session inactive for an unduly long period, the session will be terminated. If your session terminates automatically, you can login again to continue your activities.

What type of Bank Account can I use with my e-invest account?

You will need an ordinary savings account with ICICI Bank Ltd for your e-Invest account. You can specify the account in the form and it will be linked with your e-Invest account. In case you do not have an ICICI Bank account, an online banking savings account can be opened with an e-Invest account.

Do's & Don'ts

Do's

1. **Change your Passwords Periodically**: We recommend that you change your passwords regularly, at least every 14 days or so. To change your Passwords, login to icicidirect.com and go to the 'Customer Service' section, then click on the 'Change Password' option given on the left column of the screen.

2. **Keep your Internet Trading Passwords Confidential**: We assure you that ICICI Direct officials will never ask you for your Internet Trading Passwords.

3. **Take Care to Log Off:** Log Off from icicidirect.com every time after you complete your online Trading session. Do not close your browser.

4. **Add icicidirect.com to your List of Favourite Sites:** We recommend that you bookmark / add to your favourites the URL: www.icicidirect.com in order to access information and transact on your account with ICICI Direct. Look for the padlock symbol on the bottom bar of the browser to ensure that the site is running in secure mode before you enter sensitive information.

5. **Clear your browser's cache**: Clear your browser's cache and history after each session so that your account information is removed, especially if you have used a shared computer to access Internet Trading on icicidirect.com. How to clear your browser cache.

6. **Disable the "Auto Complete" function on your browser:** If you are using Internet Explorer, turn off the 'Auto Complete' function on your browser to prevent your browser from remembering Passwords.

7. **Shred unnecessary financial documents immediately**: Discard pin or password mailers immediately after memorizing them. Never write them down.

Don'ts

1. Do not leave personal information lying around in an unprotected place.

2. Avoid downloading programs from unknown sources: Some sources may have hidden forms of spyware or viruses that could compromise the security of your computer.

3. Do not open attachments sent through mails, if you do not know the sender.

4. Never open email attachments that have file extensions like .exe, .pif, or .vbs. Such files are usually dangerous.

5. Do not keep computers online when not in use: Either shut the PC off or physically disconnect it from the Internet connections.

6. Do not use shared computers: We recommend that you avoid accessing icicidirect.com from a public / shared computer, for e.g.: cyber cafe etc.

What Is Phishing?

Phishing is an attempt by fraudsters to 'fish' for your trading details. A phishing attempt usually is in the form of an e-mail that appears to be from your trading site.

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 ICICI Direct, it does not mean that your e-mail address, name, or any other information has been taken from our systems.

How The Fraudsters Operate?

1. Fraudsters send fake e-mails claiming that your information has been compromised, due to which your trading account has been de-activated/suspended, and ask you to hence

confirm the authenticity of your information/transactions like user id, 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.

2. 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.

3. 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 trading site.

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

5. 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.

6. 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.

7. 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

Subject	**Date of emails**
Urgent Notification! From ICICI Direct	25-08-2007
Confirm your online account details! (message id: 38403334)	10-08-2007
ICICI Direct Technical Verification	31-07-2007
Alerts!!! Upgrade And Secure Your Online Account Immediately	31-10-2006

Urgent Security Warning	05-07-2006
ICICI Direct Account Security Upgrade	25-06-2006

Tips To Protect Yourself from Phishing

1. ICICI Direct will never send e-mails that ask for confidential information. If you receive an e-mail requesting your Internet Trading security details like user id, password, 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 www.icicidirect.com 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.