Tips and Hints for secure browsing
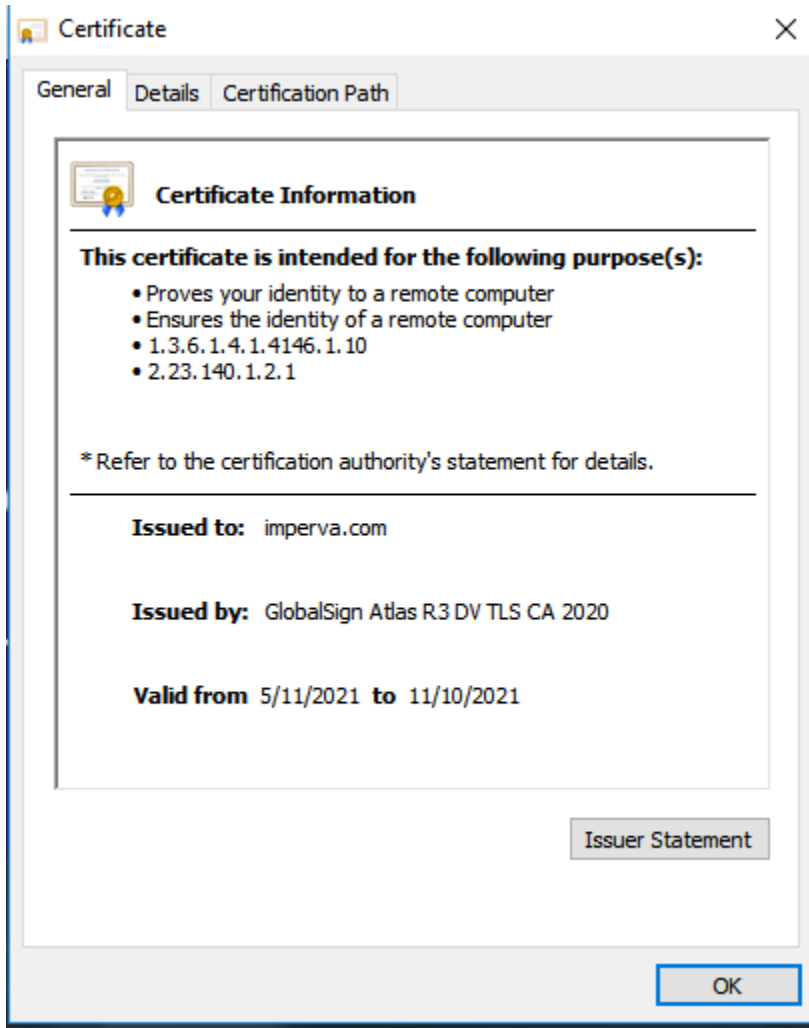
بورصة مسقط

MSX

Logging on to correct Muscat Stock Exchange Website

Always login to website by entering the official URL (https://www.msx.om/) directly into the browser address field. Then Login on the right section of the screen.

Check for the Padlock icon: The Microsoft Internet Explorer displays the lock icon at the bottom right or the top of the browser window. Click (or double-click) on it in your web browser to see details of the site's security.

Check the webpage 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.

Security from Phishing email

What should I do if I receive a Phishing email?

- Delete the email
  If you receive a Phishing email, delete the email immediately.

- Report the incident.
  If you receive an email requesting you to register or enter sensitive details, do not respond and click on any hyperlink. Immediately forward the email to info@msx.om. You can also report the same by contacting our Call Center on (+968) 24823600

- Scan your computer for viruses
  Many Phishing emails contain viruses or Trojan Horses (key logger), which are downloaded to your computer when you open any attachments or select any included links. If you have clicked on any items within the email, run a complete virus check of your computer. Muscat Stock Exchange recommends that you perform virus scans on your computer regularly.
- Change your Muscat Stock Exchange password
  After scanning your computer and ensuring it is free of viruses or Trojans, change your website password.

Given below are guidelines to protect your computer:

- Install up-to-date anti-virus software on your computer to safeguard against viruses being downloaded onto your computer.
- Use a Personal Firewall.
- Keep your browser and operating system up-to-date with Software Updates.
- Scan your computer for Virus / Trojans / Spyware regularly.
- Install up-to-date anti-virus software on your computer to safeguard against viruses being downloaded onto your computer. It is highly recommended that your computer be scanned from time to time for protection

Against viruses entering your computer through emails or browsed websites. Anti-virus software with updated signatures prevents viruses from infecting your computer.

- Use a Personal Firewall
  Firewalls stall malicious attacks and act as a filter for unwanted data entering your computer or private network. If an intruder tries to access your system harmfully, firewalls would warn you.
- Keep your browser and operating system up-to-date with Software Updates
  it is highly recommended that your computer and Internet connection be appropriately configured to ensure a secure session.
- Scan your computer for Virus / Trojans / Spyware regularly
  also, as a precautionary step, you can shut down your computer or internet connection when not in use.

Tips for using Website in a Cyber Cafe

- Avoid accessing website from a cyber cafe or a shared computer. However, if you do so, as a safe practice change your passwords from your own computer. Here are some tips to keep you safe while using a computer in a cyber cafe (or an airport or hotel).
- Always log out: While using website services that requires a username and password, remember to click 'log out' or 'sign out' when you're done.
- Stay with the computer: While you're browsing, you should not leave the computer unattended for any period of time.
- Clear history and temporary files: Internet Explorer saves pages that you've visited in the History folder and in Temporary Internet Files.

Be alert: Stay alert and aware of your surroundings while using a public computer. Beware of the persons who may be watching you key in your User id / Passwords from over your shoulders or from your sides.

Contact Us - Address & Location

CORPORATE COMMUNCATION DEPARTMENT

P.O Box 3265 Postal Code 112, Ruwi Sultanate of Oman

Phone:
+968-24823600 ext. 887/610/620
Fax:
+968-24823706
Email: info@msx.om;
web.services@msx.om