SECURITY RELATED FAQS

1. **How secure is it to transact on Quantum Mutual Fund website?**

   Quantum Mutual Fund website uses SSL technology to ensure that the information transmitted between you and us across the internet is safe and secure. Secure Sockets Layer (SSL) is a common and the most effective protocol for sending confidential information securely over the Internet. SSL works by using a private, mathematical key to encrypt (or scramble) data that's transferred between your Web browser and the website you're visiting. This Digital Security certificate has 256-bit encryption level and is obtained from GlobalSign.

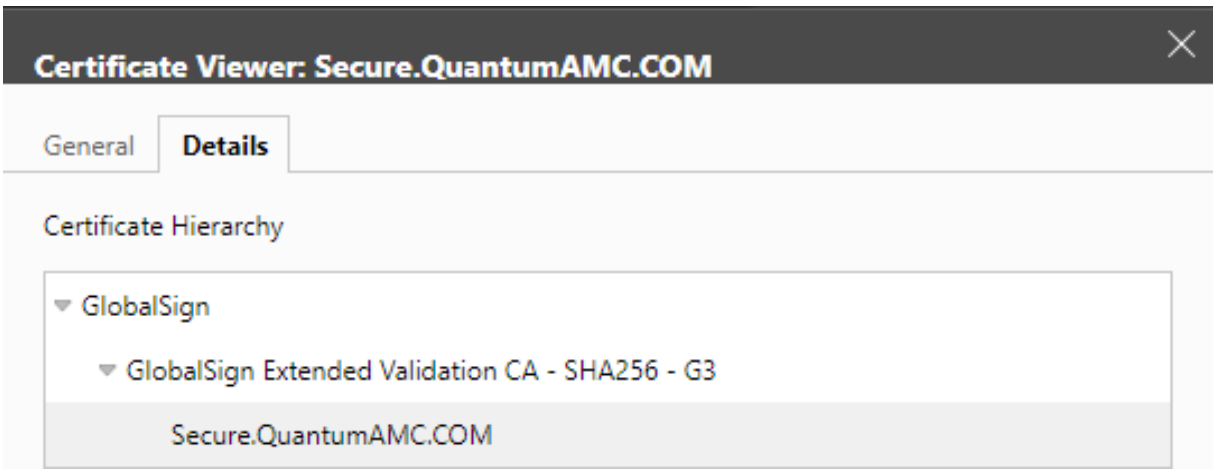
2. **What level of encryption does Quantum Mutual Fund use?**

   Quantum Mutual Fund uses GlobalSign secure connection certificate, often referred to as an SSL/TLS certificate, is a digital certificate that provides encryption for data transmitted between a user's browser and a website. This ensures that sensitive information such as personal details, payment information, and login credentials are securely transmitted and protected from interception by unauthorized parties. You may check our privacy policy for more details on Privacy Policy - Quantum Mutual Fund (quantumamc.com)

3. **What is Extended Validation SSL Certificate?**

   Extended Validation Secure Sockets Layer (SSL) Certificates are special SSL Certificates that work with high security Web browsers to clearly identify a Web site's organizational identity. Extended Validation (EV) helps you make sure a Web site is genuine and verified. One more advantage of SSL certificate is that it scans entire website for any Malware and provides the status on website security.

   For example, if you use Microsoft® Edge to go to a Web site secured with an SSL Certificate that meets the Extended Validation Standard, Edge will cause the URL address bar to turn green. A display next to the green bar will alternatively (toggle) display the organization name listed in the certificate and the Certificate Authority (GlobalSign, for example).



4. **What security measures are in place to protect Quantum Mutual Fund's website from hackers?**

We have attempted to make sure that your information with us is well protected. This is ensured through VAPT. The Vulnerability Assessment (VA) and Penetration Testing (PT) of the website has helped us to demonstrate that the security controls in place are effective in reducing the threat of internet-based attackers.

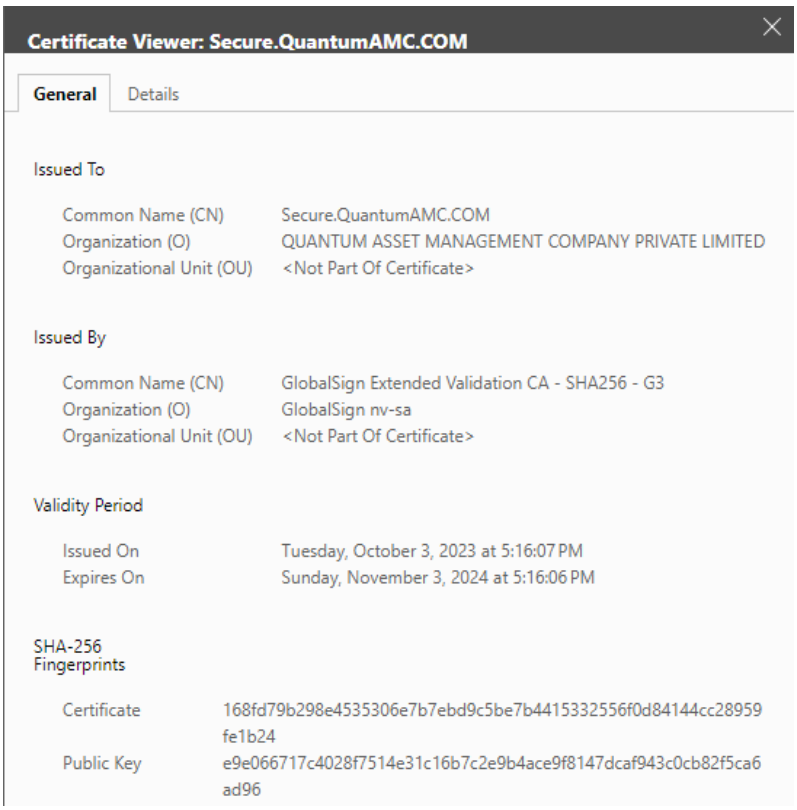
Information Security (IS) Audit is an independent appraisal activity which identifies security and processing risks in Computerized Information System and evaluates related manual and system controls to ensure security, functionality and reliability of hardware, operating system, application software and database, and to ensure confidentiality, integrity and availability of data. Regular IS audit conducted by Quantum has ensured that adequate security and control measures are in place and helped maintaining the data integrity.

5. **How can I tell if I have a secure connection?**

In Microsoft Edge, you will see a lock icon in the Security Status bar. The Security Status bar is located on the right side of the Address bar.

The certificate that is used to encrypt the connection also contains information about the identity of the website owner or organization. You can click the lock to view the identity of the website.

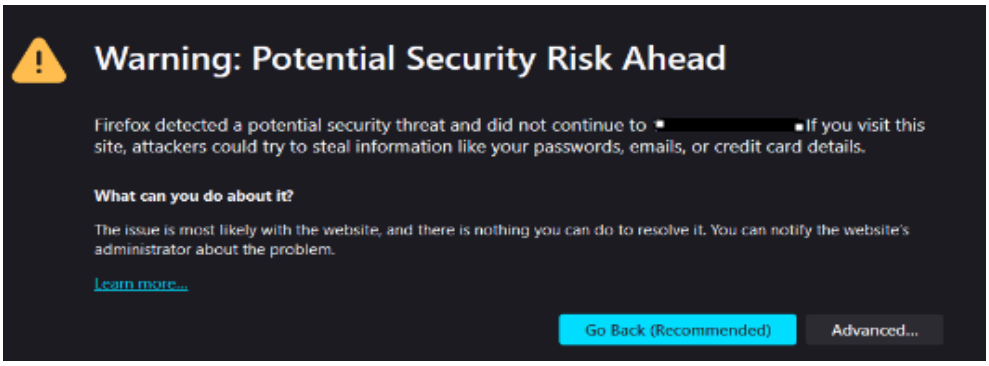
In Google Chrome, you will see a lock icon in address bar. Click on the lock icon to see the security certificate. The certificate that is used to encrypt the connection also contains information about the identity of the website owner or organization. You can click the lock to view the identity of the website.



6. **I am using Firefox and getting "**Warning: Potential Security Risk Ahead**" while visiting website. Is your website trusted for online Transaction?**

When you visit a website whose web address starts with https, your communication with the site is encrypted to help ensure your privacy. Before starting the encrypted communication, the website will present Firefox with a "certificate" to identify itself.

The certificate helps Firefox determine whether the site you're visiting is the site that it claims to be. If there is a problem with the certificate, you will see the **'Warning: Potential Security Risk Ahead'** alert page.



Seeing the alert does not necessarily mean that the website you're visiting is trying to trick you into believing it is a different website - it means that Firefox isn't able to verify the identity of the website, and that you should proceed carefully. There are several problems that can cause Firefox to reject a certificate.

With invest online website, you will not receive such alert message as we use valid trusted server certificate for secure communication between your browser and invest online server.

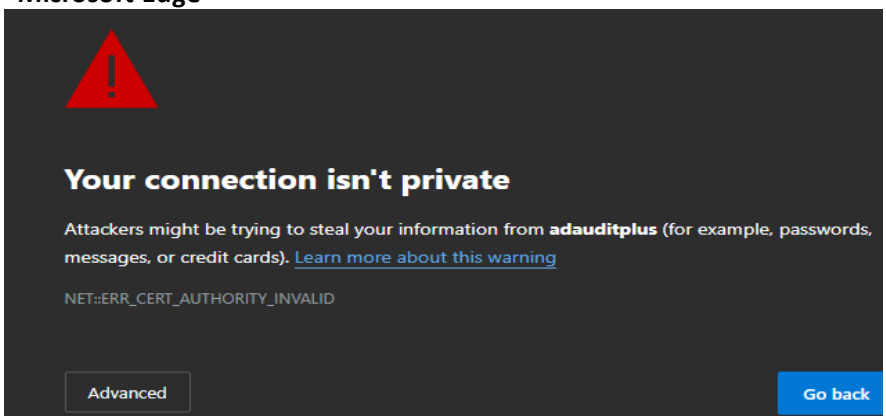
7. **What Should I do if I receive browser alert message?**

In this case you can leave the website and write to us at customercare@QuantumAMC.com about such problems.

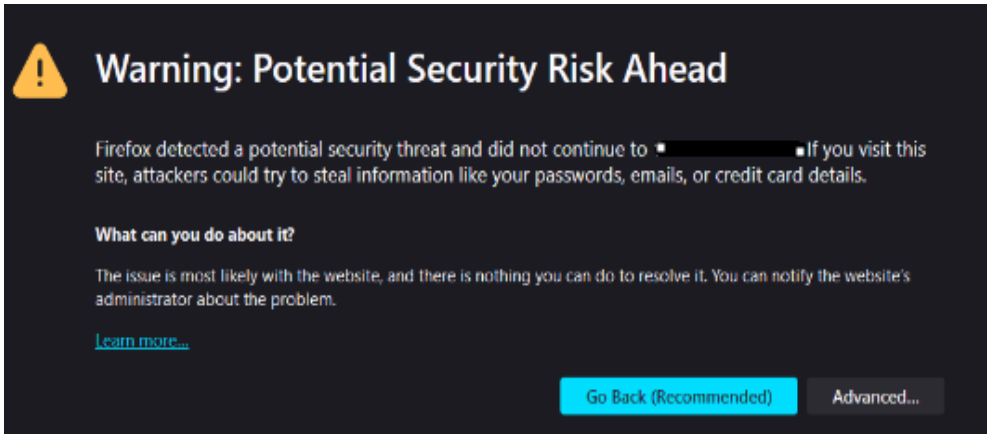
8. **What are the Security Certificate Warning on Different Browsers, and how to fix these warnings?**

Security warning looks like as shown below:
For Microsoft Edge - Your connection is not private
For Mozilla Firefox - Warning: Potential Security Risk Ahead
For Google Chrome - Your connection is not private

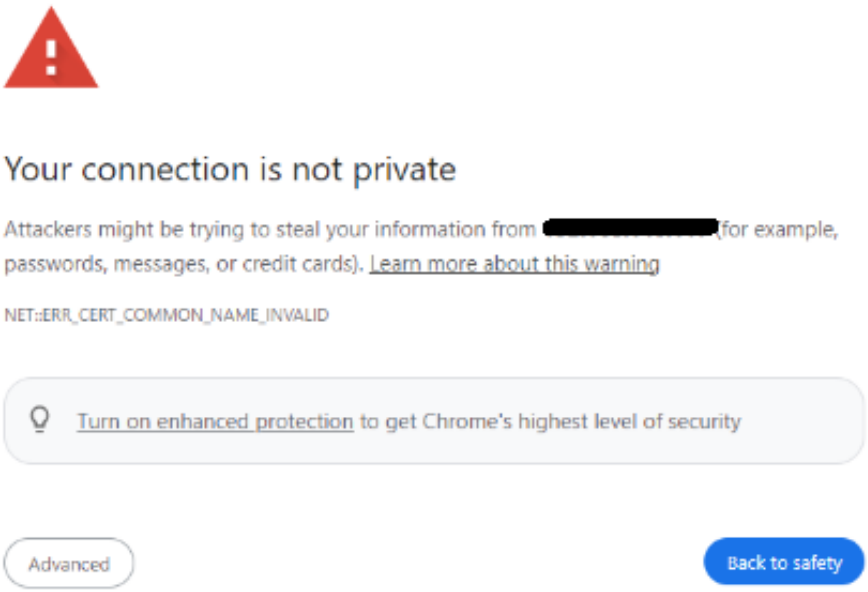
Microsoft Edge



Firefox- Mozilla



Google Chrome



The main reasons for such errors are:

1. Your computer's date or time is set to a wrong value
2. The Security Certificate has really expired
3. The website owner has configured their website improperly
4. Attackers might be trying an attempt to fool you or intercept any data you send to the server
5. Public WIFI network can sometimes be less secure
6. Cache data might interface with SSL certificate
7. Some Antivirus programs can block SSL certificates

Most common reason for such security certificate error is that the certificates are valid for a certain period, and if your computer's date is set to other than the current date or correct date, there are high chances that you will get this warning. So, the first thing to check when you receive such an error is to check your computer's date and time settings.

Now when you have set the date settings, you will most probably not see the error again. But if you see the Security Certificate error, then either the certificate of the website has really expired as it had to be renewed from time to time, or the certificate is improperly configured.

Invest Online site will not ask you to add an exception for certificate - in this case an invalid certificate can be an indication of a web page that will defraud you or steal your identity.

9. Is my Bank Account information secure and safe?

An investor who wishes to change his/her complete bank details must log on to our Invest Online website using his/her user id and password as well as OTP. Also, an online PIN must be entered by the investor before proceeding for a change in his bank details on our online portal.

10. What if scammers cancel and re-activate new SIM cards to hack into my account?

While we are unable to comment on the Mobile service providers practices, we would like to mention here that we have considered the security aspect and taken due care while designing the Quick Transact portal to update the investor via email about each transaction he performs on the portal. We would like to assure you that we have our investor's interest and the utmost security of their investment in our mind whenever we think about introducing any hassle-free transactional initiative. We have been following the same right from the introduction of our Invest Online facility.

11. What steps can I take to secure my investment accounts?

Regularly update your passwords and security settings and be cautious of phishing attempts and unsolicited investment offers.

12. What should I do if I suspect fraudulent activity on my account?

In such case you should immediately contact on customer support number 1800 209 3863 / 1800 22 3863 or write an email us to CustomerCare@QuantumAMC.com and report the issue. Also change your account password and review the recent transactions. Investors based outside India can call us on +91-22 -2278 3863 or +91-22- 6829 3863 for any assistance.

13. How should I responsibly disclose a security vulnerability found in Invest online website?

If you discover a security vulnerability, please report it to us by emailing [CustomerCare@QuantumAMC.com]. Include a detailed description of the vulnerability, steps to reproduce it, and its potential impact. Once we receive your report, we will acknowledge it within 48 hours, assess the vulnerability, and work on a fix. We will keep you updated on the status of the issue throughout the process. We request that you do not publicly disclose the vulnerability until we have had a chance to fix it, and we will coordinate the public disclosure with you once the issue has been resolved.