

Is transacting through Transact Online safe?

Yes. Quantum Mutual Fund website uses SSL technology to ensure that the information transmitted between you and us across the internet is safe and secured. 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 one 256-bit encryption level and is obtained from Verisign (Safescript).

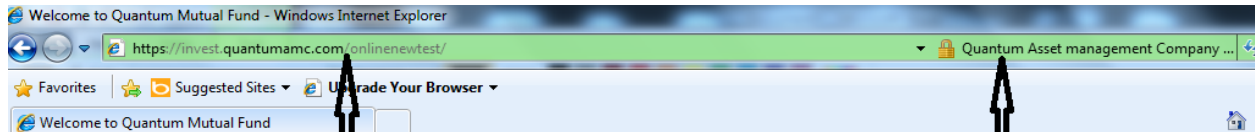
What level of encryption does QuantumMF use?

QuantumMF uses the most powerful Verisign secure socket layer (SSL) for encrypting customer data during transmission. [Click here \(Link to Verisign certificate\)](#) to verify our certificate. We are using SSL with EV (Extended Validation)

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 [It scans entire website for any Malware and provide the current status on website security.](#)

For example, if you use Microsoft® Internet Explorer 7 to go to a Web site secured with an SSL Certificate that meets the Extended Validation Standard, IE7 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 (VeriSign, for example).



Green address bar, indicates that website is secured by an EV Certificate

To verify a sites identity, the security status bar toggles between the Business name and the Organization that issues EV certificates, making it important to look for verisign

What is the VeriSign Trust™ Seal?

The VeriSign Trust Seal is a dynamic, animated graphic that displays on Web pages secured by VeriSign® SSL Certificates and Web sites authenticated by VeriSign. When users click the VeriSign seal, a

verification page opens containing information about organization, the status of malware scan, and SSL Certificate details



I am a first time Investor with Quantum, and also need to create a User id and Password
[Click Here...](#)

I have a Quantum User Id and Password
[Click Here...](#)

I am an offline investor with Quantum and want to create an Online account
[Click Here...](#)



Is your website secured from Hackers?

Yes, 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.


Is my Prepaid card/Debit Card/Bank Account information *secure* and safe?

Yes. QuantumMF is a *secure* application. It follows the best *security* practices and the most stringent safety protocols adopted by major online transaction companies. Any information you enter when *transacting* with QuantumMF is sent in an encrypted format through SSL to protect you against unintentional disclosure to third parties.


Are my Prepaid card/Debit Card details safe with you?

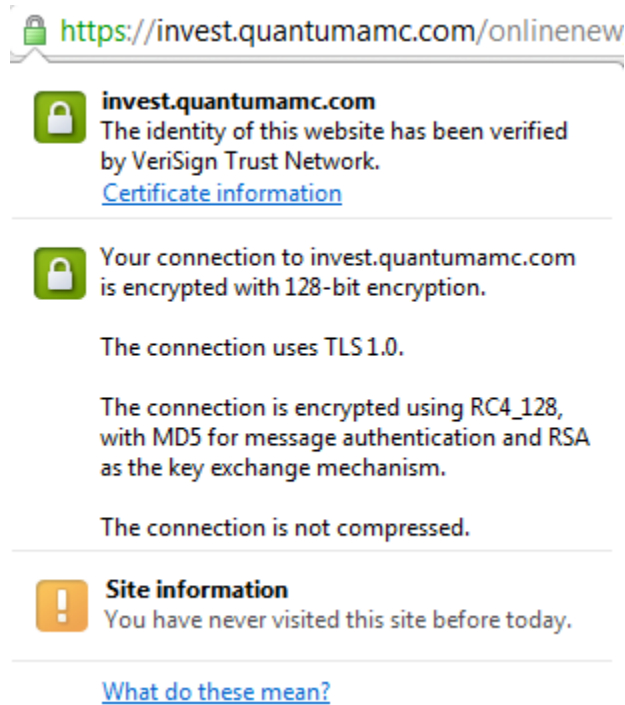
We take utmost care to store such sensitive data and used advanced encryption techniques to keep such details safe. As an additional safe guard, we do not save your CVV number, without which your card can not be used. Even when you return and choose to pay by using your stored card, you would need to enter your CVV number to authorize the card.


[How can I tell if I have a secure connection?](#)


In Internet Explorer, 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.



 <https://invest.quantumamc.com/onlinenew>


 **invest.quantumamc.com**
The identity of this website has been verified by VeriSign Trust Network.
[Certificate information](#)

 Your connection to invest.quantumamc.com is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with MD5 for message authentication and RSA as the key exchange mechanism.

The connection is not compressed.

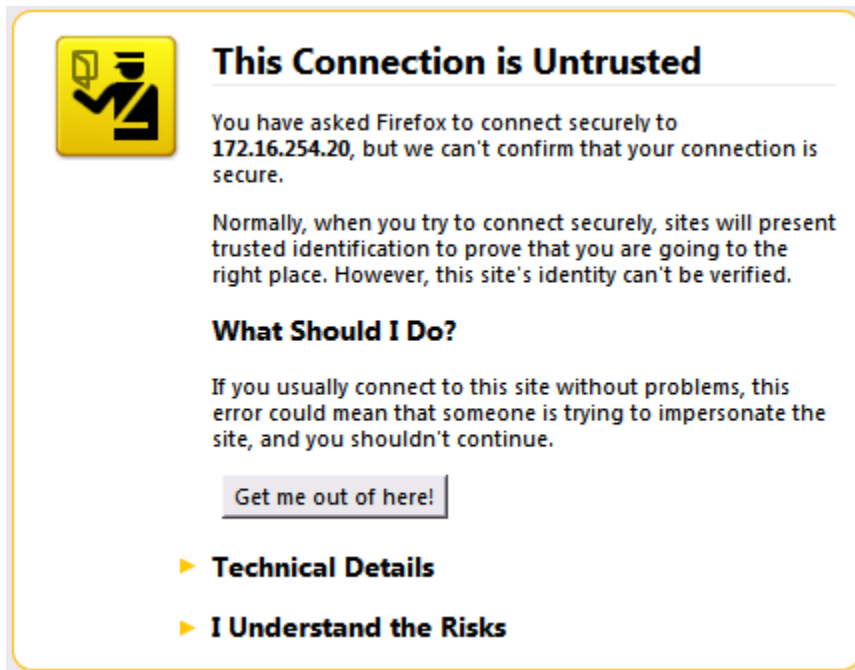
 **Site information**
You have never visited this site before today.

[What do these mean?](#)

I am using Firefox and getting “This connection is untrusted” while visiting invest online section on your website. Is your website untrusted 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 actually the site that it claims to be. If there is a problem with the certificate, you will see the **This Connection Is Untrusted** alert page.



This Connection is Untrusted

You have asked Firefox to connect securely to 172.16.254.20, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

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.

What Should I Do in such Cases?

You have two options in such case, either you can leave the website and write to us at customer@QuantumAMC.com about such problems, or you can bypass the warning by following steps:

On the warning page, click **I Understand the Risks**.

1. Click Add Exception.... The Add Security Exception dialog will appear.
2. Read the text describing the problems with this site.
3. Click Confirm Security Exception

What are the Security Certificate Warning on Different Browsers , and How to fix these these warnings?

Security warning looks like as shown below for IE, Mozilla, and Firefox web browsers

Microsoft IE- There is a problem with this web site Security Certificate

Mozilla Firefox – Secure Connection Failed

Google Chrome – The server’s Security Certificate is not yet valid

Microsoft IE



Firefox- Mozilla



Google Chrome



Main Reason for such Errors are:

The main reasons for such errors are:

1. Your Computer's date is set to a wrong value
2. The Security Certificate has really expired
3. The web-site is not trustable

Most common reason for such security certificate error is that the certificates are valid for a certain period of time, 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 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 site is not trustable.