PARNASSUS INVESTMENTS®

Online Account Cybersecurity Recommendations

Overview

We at Parnassus Investments and Parnassus Funds ("Parnassus," "we," "us") value the trust you have placed in us, and we take your online security and peace of mind very seriously. We are dedicated to protecting your online account and providing you with information and resources to make it even more secure. Most importantly, we must work together to ensure the highest levels of security, which are only possible when Parnassus and you share the responsibility for this endeavor.

In this document, we describe the things you can do to secure your account from fraud, unauthorized access, or other cybercriminal activity. These are in addition to the many steps Parnassus takes to secure your online account, including encryption and risk-based technologies, identity verification, monitoring for unauthorized account access and cybersecurity and privacy training for our employees.

Efforts You Can Take to Keep Your Parnassus Online Account Secure

I. Establish a Secure Password, Keep Your Account Details Confidential, and Take Advantage of Parnassus' Security Measures

It is critical that you maintain the security of your account details with Parnassus. This includes never sharing your account access information, whether your username, password, or both, with anyone you do not trust. Keep in mind that actions taken on your account by someone you provided your account username and password to, including an investment advisor, will be your responsibility.

In addition, we recommend that you select a unique, long, complex, and secure password that you do not re-use on other websites or accounts. If you use the same password across various websites or accounts, and one of those websites or accounts has a security incident, your password can be re-used by attackers to break into any account with the same password, including your Parnassus account.

II. Frequently Check Your Account and Notify Parnassus Immediately of Any Suspicious Activity

You should check your online account frequently, analyze the activity to confirm all of the activity was performed by you or on your behalf, and notify Parnassus immediately at (800) 999-3505 of any unauthorized activity.

You should also promptly review any statements, notices, confirmations, and correspondence you receive from Parnassus, and contact us immediately if you do not recognize transactions or suspect unauthorized activity.

III. Practice Good Cybersecurity Hygiene at Home and Online

Because you must use a computer, the internet, and your email account to access your Parnassus account and receive communications from us, it is vital that you use good cybersecurity practices in every piece of technology you use. A weakness in any element of your cybersecurity hygiene could allow an attacker to gain access to your Parnassus account, intercept or alter communications between you and Parnassus, or steal your Parnassus account credentials. Practicing good cybersecurity hygiene means:

1. Securing your computer and devices by keeping any installed software up-to-date, and by utilizing up-to-date antivirus software and a personal firewall. Where possible, we would encourage you to enable auto-update for any software on your computer, including your antivirus software.

2. Securing your mobile devices, including cell phones and tablets, especially if you receive emails from Parnassus or access your Parnassus account on those devices, by enabling encryption, utilizing a complex unlock passcode, auto-locking the device after a short period of time, and utilizing biometric access like facial recognition or a fingerprint to unlock the device. You should also exercise caution when downloading mobile applications—check to see if any suspicious activity or fraud has been reported for that application, and carefully decide what information you allow a mobile application to access.

3. Keeping your email account secure by using a multi-factor or two-factor authentication, which adds an extra step to your account login to confirm it is you accessing the account. Also, avoid sharing your email account credentials with individuals you do not trust. Finally, beware of suspicious emails asking for your login credentials or attempting to trick you into clicking on links, and exercise caution when opening any attachments you were not expecting or that look suspicious, even if they appear to be from legitimate senders.

4. Ensure that your home WiFi network is secured with a password or passcode, and that it is not public. Do not provide your WiFi password to people you do not trust, and consider changing the password periodically.

5. Avoid accessing your Parnassus account (or any financial account) and your email from computers or devices that are shared or that are available for use by the public—for example, computers or devices in the airport, at hotels, or in internet cafes. Because you do not know what software is installed on those devices, and you do not have control over the security of the devices, using them could compromise your account credentials.

6. Avoid sharing your personal information on social media or other public websites, especially if that personal information could give insights into your Parnassus password, or be used to identify or contact you.

7. Being wary of phone calls, email, or texts from unfamiliar sources. If there is any question about the veracity of the company or individual contacting you, stop communicating, and instead reach out to the company or individual using the contact information from their official website. Parnassus will never call you to ask for your password.

8. Continuously monitoring your credit report and your other financial accounts from indications of fraud, identity theft, or other unauthorized activity. If your identity is stolen, or a cybercriminal is engaging in fraud on other accounts held by you, there is a heightened risk that someone may try to gain unauthorized access to your Parnassus account.