Maintaining Your Security and Privacy

To protect your information, Northern Trust regularly evaluates and updates its security technologies and maintains physical, electronic and procedural safeguards that meet and exceed federal standards.

To protect your information, Northern Trust regularly evaluates and updates its security technologies and maintains physical, electronic and procedural safeguards that meet and exceed federal standards.

YOUR COMPUTER

Private Passport requires that you use an SSL (Secure Sockets Layer) compliant browser. SSL is a protocol that allows your personal computer to establish a secure connection to our Internet servers. We require 128-bit SSL encryption. SSL uses encryption techniques that turn all information transmitted into a series of unrecognizable characters as the information travels through the Internet. Our servers turn these characters into recognizable information after the secure connection has been made. SSL also utilizes the additional protection of digitally signed certificates that assure you are communicating with Northern Trust.

COOKIES

Private Passport utilizes cookies, which are small pieces of information that are sent from Private Passport to your browser. The cookie stores information used to safeguard your session and assist with your navigation. You must set your browser to allow cookies to use Private Passport. Private Passport uses session cookies rather than persistent cookies. Session cookies are not saved at the end of a Private Passport session and do not store personal information that other programs can access.

ESTABLISHING A SESSION WITH THE SERVER

When you log into Private Passport from any northerntrust.com Web page, your user ID and password are transmitted to us in 128-bit encrypted form. This occurs even though information on the northerntrust.com Web pages is sent to you in an unencrypted form prior to your logging into Private Passport.

The first time you sign on to Private Passport, you are required to change the initial password provided to you during enrollment. Your user ID and password must both be at least six characters in length; however, we recommend using at least eight characters. You must have at least one numeric character in your user ID and password. We also recommend that you change your password often, with an interval of no more than 30 days between password changes. As additional security precautions, after 15 minutes of inactivity you are required to re-enter your password and a limit is placed on the number of invalid sign-on attempts. Three consecutive sign-on failures will result in suspension of your user ID, requiring you to contact the Private Passport Help Center, 1-888-635-5350, for assistance.

PRIVATE PASSPORT USER ID AND PASSWORD

HOW TO CHANGE YOUR USER ID

1. From **My Passport** select **My Profile & Preferences.**
2. Under **Personalization and Security** select **Login ID.**
3. Enter your password on your new login ID and click **Save Change.**

HOW TO CHANGE YOUR PASSWORD

To change your password or if you have forgotten it, you can reset it by going to northerntrust.com and in the upper-right hand corner:

1. Select **Forgot Password?**
2. You will be asked to enter your user ID.
3. Click **Continue** and answer the security questions presented.
4. Once you are authenticated you will be provided a temporary password.
5. You will be asked to change the temporary password once you login.

SERVER SECURITY

After you have entered your user ID and password, we will authenticate your sign-on information and pass your request to the Private Passport server. This server is protected by firewall technology. The firewall allows only approved client requests to access the server and protects the server against intrusion. Both the firewall and the server are in physically protected locations. All activity on both platforms is logged and monitored for any attempts to breach security.

After your request is processed by the Private Passport server, the information is encrypted and returned via the Internet to your personal computer.

FREQUENTLY ASKED QUESTIONS ABOUT ENHANCED SECURITY

How does Private Passport's enhanced security work?

All Private Passport clients are required to select and answer a series of personal challenge questions. You may be asked these questions to help authenticate your identity. We will ask challenge questions if you access Private Passport using a different computer than usual or if the computer you usually use has significantly changed (such as changing to a new operating system or using a different browser). The challenge questions and your responses will allow us to provide an incremental layer of online security. Additionally, these questions may be used to authenticate your identity when calling our Private Passport Help Center.

Why do I need this level of online security?

Northern Trust is continually seeking ways to help improve the security of our online services. As activity over the Internet continues to increase, so have concerns about online account security. The prevalence of phishing, pharming, spoofing, malware and other identity theft/fraud activities has been a motivating factor in our online security efforts.

How does Private Passport's enhanced security protect me from phishing attacks?

If you mistakenly provide a third party with your user ID and password, our security application is designed to hinder access by the third party. For example, when a fraudster attempts to access your account, our security application will most likely not associate that individual's sign-on pattern of behavior or computer equipment with your user ID and your challenge questions will be asked. Given that the fraudster should not be able to answer the questions, access will be denied.

What type of security protects me if I access Private Passport from my smartphone?

Access to your accounts via your smartphone matches the same level of security you are accustomed to with Private Passport from a desktop. Even if your phone is lost or stolen, only you can initiate new account activity (see "Accessing Private Passport on your Smartphone").

SECURITY TIPS

Always keep your user ID and password confidential. We strongly recommend that you do not create a user ID and/or password that contains easily identifiable groups of characters, such as an account number or name preceded or followed by just one alphanumeric character.

Never leave your computer unattended while using Private Passport and close your browser when you are finished using Private Passport.

Always properly exit the system by clicking on the **Sign Off** button located on each page upon completing use of Private Passport.

Always use virus protection software and update it regularly. Do not allow a virus to remain on your computer while accessing Private Passport.

Need Help?

If you have any questions or would like more information, call the Private Passport Help Center at 1-888-635-5350. Outside the United States, call 1-312-557-5900.