Internet Security Policy

Tips for Protecting Your Account

In today's quickly changing world of online access to information and social media sharing, it is important to realize that your personal information is an attractive target for fraudsters, hackers, phishers and others. While these threats can never be completely eliminated, you can help safeguard your sensitive, personal information by actively managing the security of your accounts using the tips below.

1. **Keep your sensitive, personal information safe offline.**
   - File account statements or any documents with personal information in a safe place.
   - Keep passwords, PINs and account numbers confidential.
   - Using a cross-cut shredder, shred any papers that might contain personal information before disposing of them.

2. **Follow best practices for secure online activity.**
   - Keep your computer's antivirus, firewall and spyware protections up to date.
   - Do not use unsecured, public networks to log in to accounts with sensitive information.
   - Always log out before closing your browser window.
   - Do not email sensitive, personal information (unless it is encrypted).
   - Use strong passwords (for example, a "passphrase" that uses the first letter of each word of a sentence that you create, plus a number and/or special character).
   - Use different passwords for different accounts.
   - Consider what information you post to social media carefully—don't share details about your background that could be used in a challenge question.
   - Some systems will ask if you want to register your device. This is a matter of personal preference and convenience. Not registering your device usually means that you will be asked additional authentication questions, which could be a more secure option.

3. **Beware of callers, spoof sites and "phishing" attempts.**
   - Never provide personal, sensitive information to someone who phones you. You cannot verify their identity, and financial institutions will not ask for this information by phone.
   - If you receive a call from VestHQ regarding your account and have any concerns about the validity of the call, hang up, contact VestHQ based on the contact information on the VestHQ's website and ask to speak to a supervisor.
   - Don't open attachments or click on links in suspicious emails. These are often openings to install malware on your computer or to re-direct your browser to spoof sites designed to capture personal information.
   - Always use a search engine to get to a service provider's account log-in page or cut and paste the address into your browser yourself.

4. **Secure your smart phone too!**
   - Use a lock screen with a PIN, password or swipe pattern that only you know.
   - Download apps from reputable sources only.
   - Install malware protection and keep your operating system and apps updated.
   - Back up your phone's data and set up a "remote wipe" app that allows you to remove data from your phone in the event it's lost or stolen.

5. **If you haven't yet, please created an online account with VestHQ** as fraudsters have been known to set up online accounts with financial services companies using personal information from actual account holders.
   - Once you register your information, make it a habit to review your account regularly for suspicious activity.
   - Check profile information and transactional activity frequently.

6. **Boost your VestHQ account safeguards.**
   - Make your user ID and password as unique as possible (see below for more tips).
   - Choose challenge questions based on answers only you would know. Or make up answers to the challenge questions—as long as you can remember what answer you provided.
   - Review statements and confirmations promptly. These notices are our way of letting you know that what actions have been taken on your behalf.
   - If you hear from any service provider that your personal information has been compromised, immediately update your Prudential Retirement security settings and passwords.

7. **Strengthen your user ID and password.**
   You have a lot of flexibility to choose a user ID and password that no one else can guess.

   User IDs:
   - Must contain both letters and numbers
   - Should not contain your Social Security number
   - Cannot contain spaces

   Passwords:
   - Must contain both letters and numbers
   - Must be between six and 20 characters
   - Are case sensitive
   - Should not contain your Social Security number
   - Cannot contain spaces

8. **Any time you see something suspicious, contact VestHQ to verify the information.**
   - If you receive a communication that looks suspicious or feel you may have been a victim of a fraud involving the VestHQ name or logo, forward the information to VestHQ's client services at **hello@vesthq.com**.
   - In addition, if you have been a victim of a fraud, call your local police department, the Canadian task force against telemarketing fraud at **888-495-8501** and/or the U.S. Federal Trade Commission's Consumer Help Line at **877-FTC-HELP** (877-382-4357).

9. VestHQ may at any time revise this Internet Security policy (the "Security Policy") by updating this document. You agree to be bound by subsequent revisions and agree to review this Security Policy periodically for changes. The most updated version of this Security Policy will be available for your review under "Security" link that appears on the VestHQ website and mobile platform.

   For any retirement specific questions, please email us at hello@vesthq.com

   VestHQ values the trust you place in us. We hope these tips will empower you to navigate the digital world with confidence.

   Version 1b – July 12, 2018