How you can protect your accounts and identity

Your account numbers, PINs, passwords and personal information are the keys to your accounts. Remember that you are your own first line of defense when it comes to protecting your accounts and identity. Here are some best practices to help you keep your accounts and personal information safe and secure:

- Password/PIN Security
- Monitor your accounts frequently
- Take care of your computer and mobile devices
- Beware of phishing and spam emails
- Be suspicious about emails or telephone calls
- Bank, shop and spend wisely
- Protect yourself from mail fraud
- Other tips

Password/PIN Security

- Use a unique password/PIN for each site where you maintain an account and regularly update your passwords/PINs. Never use your date of birth or Social Security number as your password/PIN.
- Don't allow social networking sites to memorize your passwords/PINs.
- Avoid writing down or emailing passwords/PINs.
- Don't share passwords/PINs or answers to security questions with anyone.
- The strongest passwords/PINS are comprised of a chain of four unrelated common words.

Back to Top

Monitor your accounts frequently

- Monitor your financial accounts frequently, and be sure to look for unusual withdrawals, deposits and transactions. Venerable's online account access and mobile app make monitoring your account easy.

- Sign up for electronic delivery of important documents.
- Immediately open your statements and confirms to verify all activity. If you notice anything suspicious, call your financial institution immediately.

Back to Top

Take care of your computer and mobile devices

- Keep your computer up to date by installing the latest operating system, patches, and antivirus and antispyware software to prevent hackers from exploiting any known weaknesses on your computer.
- Install and update personal firewalls to regulate the flow of information from your computer.
- Use only programs from a known, trusted source.
- Backup your important files on a regular basis and store the backups in a secure place.

Back to Top

Beware of phishing and spam emails

A phishing attack is an online fraud technique that involves sending official-looking e-mail messages with return addresses and links that appear to originate from legitimate businesses, often times with corporate branding. These e-mails typically contain a hyperlink to a spoof website. Fraudsters use these techniques to fool participants into revealing personally identifiable information, financial information or login information such as account numbers, PINs, credit card numbers, etc. The stolen information may be used to gain access to financial accounts or make fraudulent purchases.

It is important to be suspicious of e-mails asking for your confidential information and look out for red flags such as urgent requests, unknown email addresses or discrepancies between actual and displayed hyperlinks. Venerable will never ask you for your personal information by e-mail.

Phishing emails often use emotions to create a sense of urgency to act quickly. A few examples of phishing email subjects that play on emotions:

- Your Account has been locked!

- You’ve been selected!
- Act now!
- You won!

Tips to identify Phishing emails:

- Look for misspellings and grammatical errors
- Signature does not match senders address
- Email creates a call for action/sense of urgency/emotion
- Hyperlinks have unknown web address
- “From” email address is not a standard looking address or is masked to appear to be legitimate. You can right click on the sender to unmask/reveal the email address

See something suspicious? Act with caution!

- Never enter your username or password into unknown websites
- Do not click on any links
- Do not open any attachments
- Delete the suspicious email from all mailbox folders
- Go directly to your account website to login and access messages
- Call the company to confirm the legitimacy of the email

Spam emails are messages sent simultaneously to thousands of email addresses from an unfamiliar sender.

- Use a spam filter to avoid seeing these messages.
- Never respond to a spam message; your email address is then recorded as live and the spam will increase.
- Should you read a spam message remember: If it sounds too good to be true, it probably is. If you received unsolicited email offers or spam, send the messages to spam@uce.gov.

Back to Top

Be suspicious about emails or telephone calls that involve the following:

- You are asked for your Social Security number, calling card or credit card number, so you can purchase products, qualify for prizes or process your potential employment.
- The organization has a name that is intended to sound like a government agency or a well-known company.
- The organization is unwilling to send you written information on the offer or give you references.
- Someone claims you've won a prize and you haven't entered a contest.
- You have to pay a fee before you receive complimentary goods or services.
- In general, your sensitive personal or financial information is required before you are able to receive the indicated benefit (internship, prize, product, etc.).

Back to Top

Bank, shop and spend wisely:

- Cancel your unused credit cards so that the account numbers will not appear on your credit report.
- Sign your credit cards immediately upon receipt and indicate SEE ID for merchants to confirm your identity.
- Do business with companies you know are reputable, particularly online.
- Use a secure browser when you conduct business online that encrypts or scrambles purchase information. Customers can verify that the web page they are entering is secure by looking for the https:// on every page to ensure your entire session is encrypted – not just the login page.
- Avoid opening e-mail from unknown sources.
- Never click on an unknown e-mail link or open an unrequested e-mail attachment. Go to the company's website yourself and fill out information there or call them.
- Ask businesses about their privacy policies and how they will use your information. Can you choose to keep it confidential? Do they restrict access to data?

Back to Top

Protect yourself from mail fraud

- Remove posted mail, especially bills, from your home mailbox every day. Signing up for electronic statements and paying bills online can help you reduce the chance of someone stealing information from your home mailbox.
- Know your billing cycles. Follow-up with creditors if bills or new cards don't arrive on time. An identity thief may have filed a change of address request in your name with the creditor or the post office.
- Shred receipts and mail, especially pre-approved credit card applications.
- Eliminate the receipt of pre-approved offers of credit by calling 1-888-5-OPT-OUT.
- Account for all new checks when you receive them in the mail.
- Remove your name from direct mail lists and write to the companies you do business with and ask them not to sell or rent your name. You can visit the Direct Marketing Association's website to learn about the laws that protect you as a consumer and how to get your name removed from these lists.

Back to Top

Other tips

- Check your Social Security Earnings and Benefits statement once each year to make sure that no one else is using your Social Security number for employment. You can obtain your statement at https://www.ssa.gov/myaccount/statement.html
- Securely destroy documents containing personal information, and be very cautious about posting personal details on social networking sites or on the internet. Criminals can use this information to commit fraud.
- Never carry your Social Security card, bank passwords or other sensitive information in your wallet.

Back to Top