FINANCIAL TIPS

QUICK AND ACTIONABLE IDEAS TO HELP IMPROVE YOUR FINANCIAL WELL-BEING

Cybersecurity Tips

Safeguarding against identity theft

Password Do's and Don'ts

Creating a strong, complex password is key to helping prevent a cyberattack. To increase the security of your password, follow these simple steps:

Do

- Do use a combination of letters, numbers, and symbols.
- Do substitute letters for numbers whenever possible in a password. Example: Replace "s" with the number "5" (pa55word).
- Do change your passwords frequently.
- Do use different passwords for different accounts
- Do answer security questions with answers only you would know and that cannot be accessed by public information.

Don't

- Don't use personal information such as a pet's name, birthdates, or hobbies.
- Don't use words found in the dictionary. Read the above for examples on how to build a safe password.
- Don't mirror or slightly alter your User ID as a password.
- Don't use simple letter or number sequences. Don't email your User ID and password to anyone.

O'Keefe Stevens Advisory, Inc.
1 Bausch & Lomb Place, Suite 920
Rochester, NY 14604

O'Keefe Stevens
Advisory, Inc.

Email: info@okeefestevens.com
Phone: 585-340-6538

Keep Your Information Private

Protecting yourself from identity theft all begins with making sure your personal and financial information is not shared. Your name, address, Social Security number, and account information should not be made accessible to others.

- Don't share or write down online account information - including your log-in details such as user names and passwords.
- Avoid accessing your account from public computers or networks, including internet cafes, libraries, hotels, parks, and more.
- Always log off and close your browser after accessing your account.
- Secure any data stored on your smartphone by deleting images of checks and other important personal information.
- Contact your wireless provider to inquire about the security of the information on your smartphone and the network you use to transmit data.

Protect Your Computer and Network

The online security landscape is constantly evolving, so it's critical to keep updating your defenses against new threats.

- Install antivirus and anti-spyware software and configure automatic updates.
- Always use the latest version of your preferred browser.
- Only add software to you are familiar with to your computer.
- Use a secure password to protect your wireless network.

Trust Your Email Instincts

Many internet scams involve emails that appear to be from a trusted source. Links and attachments are often used to remotely install malware on your computer without you even knowing it. That's why it's important for you to handle your emails with caution.

- Don't reply to any email asking for personal information such as a password, User ID, Social Security number, or other account details.
- Avoid clicking on embedded links in the body of an email or attachments.
- Look out for emails that appear to come from a friend or known acquaintance, but contain a generic message directing you to a link or attachment.
- Turn off your "preview pane" to disable the ability for malware to be executed indirectly.

WE'RE HERE TO HELP

Our team is dedicated to helping ensure your financial information and accounts are safe and secure.

For any questions, concerns, or for advice on a suspicious phone call or email you received, please call our office at 585-340-6538. Any member of our team will be willing to assist you.