Ginsburg Financial Advisors, Inc.
Personal Financial Planning & Investment Management
Larry P. Ginsburg, CFP®

phone: **(510) 339-3933**
fax: (510) 339-1611
LGinsburg@GinsburgAdvisors.com
www.ginsburgadvisors.com

Good Fishing is Not Bad "Phishing"

Don't Get "Caught" by Scammers!

Protect yourself with Tips for Staying (Computer) Virus-Free

The COVID-19 pandemic has had a significant impact on our daily lives. One obvious impact is how much time we spend at home due to self-quarantining or shelter-in-place orders. As we spend more time at home, our reliance upon the internet has also increased, especially for individuals working from home, shopping online, and remote learning. Ironically, the more time we spend at home avoiding being infected with COVID-19, the more we expose ourselves to being infected by computer viruses and other cyber-attacks.

Cybercriminals have taken advantage of society's increased online presence by exposing vulnerabilities to collect personal information from individuals and corporations. There have been cases of cybercriminals setting up fake websites to sell ventilators, masks, and hand sanitizer to receive electronic payments. There has also been a large increase in 'phishing' emails, which involves sending phony emails from a seemingly reputable source to induce individuals to divulge sensitive information. These attempts to steal personal information can also occur via a phone call or text message.

Be on the look-out for phishing emails, text messages, and phone calls. If you receive an out of the ordinary message requesting private information, do not respond to the message or click any links contained in an email or text. The safest way to verify the authenticity of a suspected phishing message is to contact the company directly, either over the phone or online and ask them to confirm or deny the request for sensitive information. Do not call any phone number listed in the email or text you receive to attempt to contact the company, as the ones in any message you receive are likely to connect you with the scammers.

We recommend that you take extra steps to ensure that your vital online accounts, such as your online banking accounts, are secure. Set up multi-factor authentication on all vital accounts. The most common form of multi-factor authentication is linking your mobile (cell) phone to an account and requiring a text-code verification to successfully login. Enable notifications/alerts for online accounts so that you are aware of any suspicious login attempts. Make sure all your software programs, antivirus, and operating systems are up to date. Advantage Microsystems, our outside Information Technology services company for the past twenty-three years has done everything

possible to make sure our data and communication systems at Ginsburg Financial Advisors (GFA) are secure. It is vitally important that GFA protect client data as well as all our communications.

Create strong online passwords and do not use the same password for multiple websites. Once cybercriminals obtain personal information, they will often upload it to large online databases. This can lead to multiple account breaches if the same password is used for multiple accounts. This can be challenging for many people. A password manager can help generate strong passwords and securely store account login information. Some commonly used effective password managers to consider are Dashlane, LastPass, and Keeper.

As we all continue to protect ourselves against the threat of COVID-19, we need to take concurrent actions to protect ourselves against the increased threat of cyber-attacks. While a multitude of different cyber-attacks exist, phishing and credential hacking are the two most common threats. Cybercriminals tend to cast a wide net looking for easily accessible information. The more precautions you take to keep your online presence secure, the less likely you are to end up the victim of a successful attack. Many people love to fish, whether to catch and eat or catch and release. We recommend fishing for fun but please do all you can to not be “caught” by a phishing scam!