

Cyber security in the age of Covid-19

July 2020

Phishing has increased 6000% (!) since the Covid-19 crisis started. With the current exponential rise in cyber attacks, this may be an opportunity to list some of the cyber security suggestions we've found particularly useful. These are from several sources, including a continuing education course by a cyber security expert, John Silio of the Silio Group, at the (virtual) May NAPFA meeting of CFP's. We are *not* cyber security experts and the following list is not complete, but we hope some of the ideas may be useful:

- "Social Engineering":
Protection against ransomware, malicious downloads and phishing attempts relies on email recipients (you!) not clicking on anything that doesn't quite look right. Check the source before downloading or giving private information.
Hover your mouse over any link and the linked URL will appear. The text of a link in a document may look legitimate, but it can always be a spoof, and the only way to know what you are linking to is with the hover technique.
- Password protection:
Use a password manager. This stores your passwords and fills in password fields with strong passwords when logging into websites. The program is accessed with only one very strong master password you create. For example, use a statement describing some personal event only you know, with added special characters. Password manager programs are well worth it, and not expensive (e.g. the basic version of LastPass is free).
Special characters in passwords have become essential – code breaking computing is now so powerful that passwords without them are much less safe than before.
Use two-factor authentication. Yes, this can be inconvenient, but it's a small price to pay for protecting sensitive information, such as access to cloud vaults, bank, and financial accounts.
- Protect your computer with a good malware program, such as Malwarebytes.
- Use automatic updates for your software.
- Password protect your wi-fi.
- One of the best defenses against ransomware is backing up regularly to an external drive not connected to either your computer or the cloud.
- Texting is more secure than email
- Use a virtual private network (VPN) for your mobile phone to protect your privacy when out and connecting to a public network

On a personal note, we want to emphasize that you will never receive an invitation from us to send sensitive information via email. If it looks like us, it's *not*. We never ask for sensitive information to be communicated by email. We have one of the most secure cloud vaults for that purpose, Citrix ShareFile, approved for use by both HIPPA and eCommerce banks.

From time to time we send a Newsletter that contains only non-sensitive information and does not share your names or email addresses with others. Soon we will be sending a mid-year 2020 briefing, but it is just that, a news brief with timely information we think may be useful, not sensitive or private information.

We hope these suggestions are helpful, especially now!