EST. 1890
MOORS & CABOT
INVESTMENTS

An Important Advisory from Moors & Cabot

M&C is well aware of the impacts from coronavirus (or COVID-19). At the forefront of our concerns are cleanliness, the health of our loved ones, and social distancing during this difficult time.

However, there are other significant threats that have been here long before the virus. Those include hackers, scammers, and bad actors seeking to take advantage of the fear induced by the virus.

There have been many warnings issued during this time, and we would like to outline a list of ways that scammers will try to take advantage of a person, as well as a list of important ways to protect yourself.

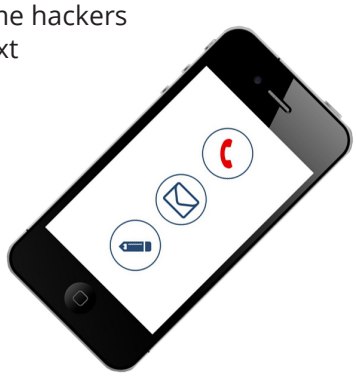
FAKE ALERTS

You may receive legitimate-looking alerts that appear to be sent by known organizations that are, in fact, fake. The alerts appear to have been sent by government agencies, financial institutions, and health agencies via email or text message and might make mention of:

- COVID-19 Testing Kits
- COVID-19 Charities
- COVID-19 Cures
- Stimulus Check Bank Account Confirmation
- Stimulus Check Bank Account Sign Up
- IRS Confirming Direct Deposit
- IRS Payments due in order to receive stimulus

ROBOCALLS

Robocalls are also on the rise, and they will target the same subjects above. Some hackers will follow up an email, text message, or a phone call to try and boost their validity. Remember, no government agency will call to request personal information from you directly.



FEAR MONGERING TACTICS

Watch out for messages inciting fear. It may be hard to believe, but hackers have received and gathered personal information from previous hacks conducted on large platforms, such as Facebook and Yahoo (amongst others). The information can be spread between hacker groups and can be posted on the dark web, as well. Do not respond to a message with a known password. If the password is still in use on any accounts, change it immediately. Do not respond to messages stating that you have been caught doing nefarious activities and will be exposed without payment or acknowledgement of the message. These messages are intended to incite fear so that you will desperately respond. These tactics have been around for many years and will be more prevalent during these unprecedented times.

STAYING AWARE

We have a couple mottos that we use at Moors & Cabot to remain vigilant against threats:

1. Stop. Think. React.
2. Know & No. Be in the KNOW and know when to say NO.

Securing Yourself During COVID-19

These are some important things to keep in mind in order to protect yourself.

Secured Internet Connection

Your internet connection at home should be secured with a strong password. Your password should not be posted or shared with anyone outside of your immediate family, and you should use a guest network for visitors if you have any visitors that require internet access.

Multi Factor Authentication

What is Multi Factor Authentication? It is an additional layer of security linked to your account. It can be linked to your back, email, and utility accounts (most online accounts will offer a multi factor option). The additional layer is set by sending a notification to you via text or email to verify that you are making the login request. There are other tools, such as Google Authenticator, which will create a rotating 6-digit code. These features should be used when offered as a way to deter hackers and access to your accounts.

Personal Information

Today and every day, you should be careful with your personal information. Please use legitimate government sources for legitimate, fact-based information. Your personal information should not be shared with anyone over the phone, via email, or via text to validate yourself with our government agencies.

Clicking on Links

This is the perfect time to: Stop. Think. Then React. If you get an email or text from an unknown source, ***do not*** click on the links in the message. If you get an email or text from someone you recognize, but the link or message seems odd, send them a separate message asking for confirmation or place a phone call to notify them and confirm whether they actually sent the message. Check the email address for slight variations (a misspelled name may be the first indicator). Furthermore, you can hover your mouse over a link to see if the link is in fact sending you to the real website or a site hosted by hackers. If you have any reservations, get confirmation first.

Donations

Be wary of donations that require you to use gift cards or wire transfers. These donations are likely sending money to illegitimate individuals.

Windows System & Device Updates

It is important to ensure that your systems are up-to-date with Microsoft's latest patches. Windows update should be set to run automatically on your systems to ensure timely updates. You should also ensure that you are running a relevant and up-to-date Antivirus product on your system. **It is your first line of threat detection during a breach.** Your routers, access points, wireless printers, and any network connected device should be set to automatically update its software and firmware. This will ensure that all loopholes are patched as often as necessary. Devices older than three years should be inspected to ensure they are still getting manufacturer updates.

Victims

If you have been a victim of cyber crime, what should you do next? There are resources available to those who have been a victim of a cyber crime. A report/complaint can be opened with the FTC. You can also consider contacting your local law enforcement agency. If your bank account or any of your accounts are impacted by the crime, you should contact those entities as well.

Passwords

If you were a victim of a cyber crime, you should consider changing the password to the source of the breach. Now is a good time to rid yourself of the password that was breached, and if it is used on any other accounts, c***hange the password immediately***. Your password should be long and complex, and it should not include your name, nor should it be simple or common (see Multi Factor Authentication above for additional security).