FOURFRONT
advisors
Perspective. Clarity. Purpose. Confidence.

Horsham Office
200 Gibraltar Road, Suite 115
Horsham, PA 19044
Phone 215.259.4900

Exton Office
557 W. Uwchlan Avenue, Suite 240
Exton, PA 19341
Phone 610.458.5790

Is the Coronavirus a Threat to Your Information Security?

Presented by FourFront Advisors

With all of the news surrounding the health and financial implications of the coronavirus, its threat to your information security may not be top of mind. At least that's what scammers are counting on. They're hoping to exploit the global pandemic to their advantage—preying on victims with everything from phishing emails to fake charities—for their own commercial gain.

So, what can you do to mitigate the risks? In fact, the best defense against these information security threats is education. By keeping abreast of the latest scams, you will be well prepared to avoid them.

Phishing Scams: Don't Get Caught!

To start, let's define one of the most prevalent means that fraudsters use to gain access to your personal information (e.g., bank account, credit card information, username and passwords, social security number): *phishing*. Phishing scams can come in the form of an email or text message, often appearing to be sent from someone you know or an organization you trust.

Phishing scams are designed to trick us into either clicking on a link or opening an attachment. The most effective are those designed around current trends or events. As such, it's no surprise that we're seeing an uptick in the number of coronavirus-related phishing scams. Here are just a couple to be aware of.

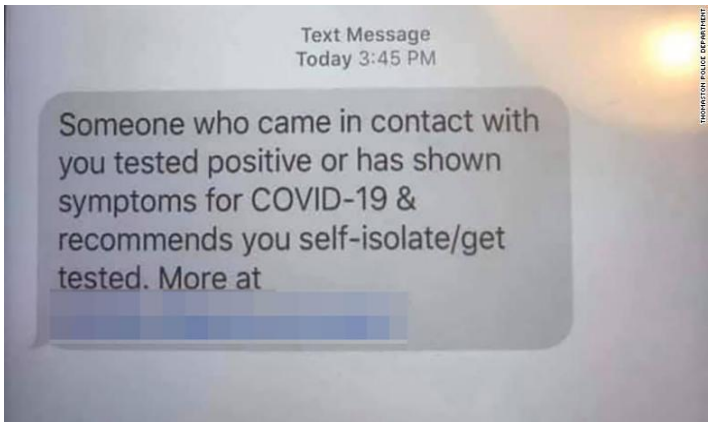
The insidious email. One of the most deceptive coronavirus-related scams has been fake emails that look like they're from the World Health Organization (WHO) or Centers for Disease Control and Prevention (CDC). At first glance, these emails look legitimate. Some even include "safety measures" and feature the WHO or CDC logo.

So, what gives them away as phishing attempts?

- Contain spelling and/or grammatical errors
- Request your email address and password
- Ask for a donation (sometimes via bitcoin)
- Include instructions to click on suspicious links or open attachments

It's important to know that the CDC and WHO would never ask for your login credentials. To find the facts and real coronavirus safety measures, go directly to the CDC or WHO website.

Not-so-positive text messages. Another coronavirus-related scam making the rounds is a text message claiming the recipient has come into contact with someone who has tested positive for or shown symptoms of COVID-19. If you receive a text message like the one below, delete it and block the number. *Do not click the link.* It will not lead to "more information" but, rather, will likely provide a gateway to your personal information.



In fact, best practice is to never click on a link from an unknown source or from someone you weren't expecting an email or text from—as fraudsters generally use these links to download malware on to your devices.

Social Engineering: Separating Fact from Fraud

A major goal of fraudsters is to trick victims into providing their personal information, which can be used to commit fraud. In times of uncertainty like those we're currently experiencing, we might not always have our guard up or may feel particularly vulnerable. Scammers are ready to exploit these emotions, trying to blur the line between fact and fraud.

- **The phony phone call:** If you receive a call claiming to be from the IRS or another government agency and are asked to verify your bank account information or provide your social security number so that your stimulus check can be deposited, hang up immediately. The IRS will *not* contact you by phone, email, text message, or social media to convey information about your stimulus payment; however, the IRS website offers a plethora of reliable information on coronavirus tax relief.
- **That's not charitable:** It's natural to want to help others in times of crisis. Unfortunately, scammers have figured out ways to exploit this generosity. Using names similar to those of real charities, scammers will often try to rush you into making a donation—preferably using methods that are difficult to trace (e.g., cash, wire transfer, or gift card). To ensure that your money is going exactly where you want it to go, do your research! Also, keep in mind that the safest options for making donations are credit card and check.

Best Practices for Every Situation

It's true that the number of scams hitting the headlines seems to multiply by the day. But here's some good news: there are some common information security best practices to employ that will help you mitigate the risks, no matter the situation:

- From your bank account to your home Wi-Fi, use a strong, unique password or, ideally, a pass phrase, as they are easier to remember but difficult for fraudsters to crack.
- If you think an account has been compromised, change your passwords immediately.
- Use multifactor authentication (i.e., requiring a second form of identification after entering your password) wherever possible, as this adds an extra layer of security.
- Do *not* use the same password on multiple accounts. If you do, the likelihood of your accounts becoming compromised increases.
- Use trusted sources for up-to-date, fact-based information. Here are just a few that we recommend:
  - https://www.justice.gov/coronavirus
  - https://www.fcc.gov/covid-scams
  - https://www.consumer.ftc.gov/features/scam-alerts
- Avoid clicking on any links or opening attachments in an email or text, especially those coming from an unexpected or unknown source.
- If something is too good to be true, it likely is. Verify, verify, and then verify again.
- If you believe you have fallen victim to a scam, visit the Federal Trade Commission website for help and to report the scam.

Stay in the Know

When it comes to the latest scams, being aware of the warning signs is half the battle. By knowing what to look for—and what to do if you suspect you've fallen victim—you will be well positioned to protect yourself and your personal information.