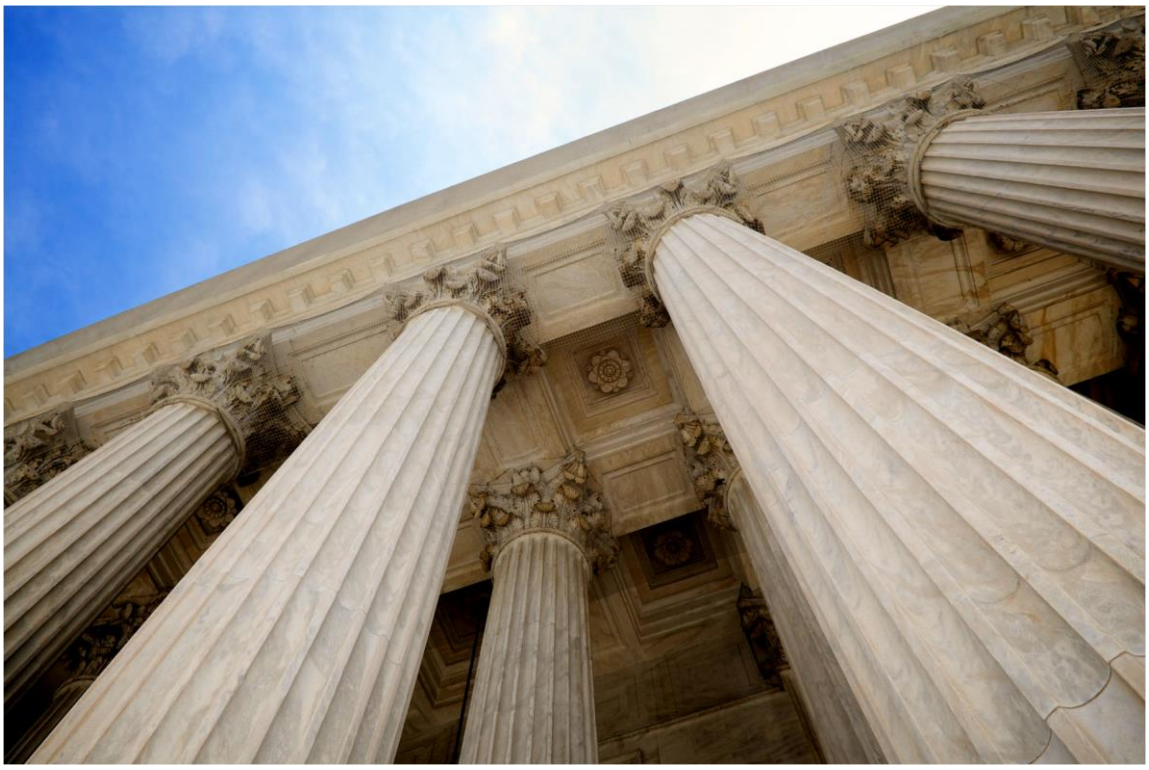

Security During Covid-19

SYSTEM SECURITY DURING COVID-19

Halifax County Government ITS| Security Tips/COVID-19) | July 2020

Phishing

Phishing emails are designed to trick an unsuspecting person into providing sensitive information that can give them access to both organizational and personal data.

Hackers use publicly available information on websites, including your website, to identify key information that can be used to trick you, such as your email domain and senior staff names. The email will actually look like it is coming from management. Pay close attention to the "from" email address, which will usually be an individual's account.

APP Scams

Scammers are also creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise user's devices and personal information.

Charity Scams

Scammers are soliciting donations for individuals, groups and areas affected by COVID-19.

Treatment Scams

Scammers are offering to sell fake cures, vaccines and advice on unproven treatments for COVID-19. Scammers are also posing as national and global health authorities, including the World Health Organization (WHO) and Centers for Disease Control and Prevention (CDC), tricking recipients into downloading malware or providing personal identifying and financial information.

Supply Scams

Scammers are creating fake shops, websites, social media accounts and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.

Provider Scams

Scammers are also contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19 and demanding payment for that treatment.

Investment Scams

Scammers are offering online promotions on various platforms, including social media, claiming that the product or services of publicly traded companies can prevent, detect or cure COVID-19 and that the stock of these companies will dramatically increase in value as a result.

COVID-19 Specific Scams

There is a lot of phishing activity related to COVID-19 that asks people to provide information in order to access benefits or information. These are examples highlighted by KnowBe4:

- Coronavirus Stimulus Package (SSN): Claims that the person is eligible for a $1,200 stimulus check, and they just need to enter their Social Security number to confirm.
- Coronavirus Testing Kit (SSN): Claims that due to new government regulation, the person can receive a free coronavirus testing kit sent to their home.
- Coronavirus School Schedule (SSN): Targets parents by referencing a change in their child's school schedule due to the coronavirus, then asks for the Social Security number to confirm identity.
- Increased Coronavirus Cases in Your Area (zip code): A call from the local "county commissioner" claims that there has been an increase in coronavirus cases in their area and requests their zip code to confirm their location.

The best way to protect yourself and your organization against phishing threats is to train your staff to be aware that they exist and to know how to spot and report them as they come in.

Malware Clickbait

Cybersecurity researchers have identified several fake COVID-19 tracker maps like the one below that infect people's computers with embedded malicious code when you click on the image to open it. The tactic is one of many ways hackers and scammers are capitalizing on people's fears about COVID-19 to spread malware.

Best Practices to Follow

Here are some simple best practices to keep in mind, regardless of whether you have a remote workforce or you've returned to your office:

- Only open email from known email addresses (always check the email address twice).
- If something looks suspicious, check with your management team, HR, or IT team before clicking any links. Use phone or chat to verify. Don't reply to the email to check.
- Never click a link or attachment in an email unless you know what it is and who it is from.
- Only get your news from trusted sources such as reputable news sites, official government websites (with the .gov domains), or sites with security certificates.
- Always be aware of who you are following on social media and be thoughtful before clicking links to those cute dog videos or COVID-19 live tracking maps.
- Know who built that COVID-19 mobile app before you download — only get COVID-19 apps from health departments, hospitals, and trusted sources.
- Never save organization passwords in your browser on your home computer.
- Don't store confidential data on your home computer.
- When in doubt, don't click the link. Contact the sender by other means, like the phone.

Home Network Security

There are a few simple steps you can take to better secure your home Wi-Fi network:

- Make sure your router and Wi-Fi system are not using the default passwords.
- Hide your SSID by configuring your system to not broadcast it.
- Some systems allow you to have a "guest" network so you can separate your work traffic from the rest of your family's traffic.
- For extra protection, configure your router and Wi-Fi system to only allow approved devices on the network.
- For information on how to configure these settings for your router and Wi-Fi system, consult the documentation for your specific system.

Other Basic Cybersecurity Tips

Here are a few more actions to consider that will keep your organization more secure. Again, these aren't just security measures to implement during this crisis — they're widely adopted practices that you should consider no matter the circumstance.

- Use multi-factor authentication (MFA). MFA provides an extra layer of security when user credentials have been compromised by bad actors. MFA requires an extra identity check to authenticate your login credentials by asking you to provide something that you know, such as an answer to a specific question (like what color was the house you grew up in) or cross-checking your identity by texting a code to your mobile phone. Most applications have this feature or they use an app like Google's Authenticator.
- Communicate clearly with remote workers. Send best practices, security alerts, and updates as soon as they become available