# COVID-19 Brings an Increase in Cyber Attacks

By Jamie Perry, FVP – Chief Security Officer

While financial institutions are looking for the best way to serve their customers during the coronavirus pandemic, many attackers are using the current environment for their benefit. Industries across the globe are witnessing an increase in malicious cyber activity as attackers use a variety of means to target organizations. Cyber criminals are using many of the same tactics they always use, but they are using COVID-19 to prey on fear and exploit individuals who are willing to help others and not anticipating a scam.

The large amount of employees working from home has attackers on the hunt for insecure environments such as home networks, which often have less security defenses than what exists in the office. This leaves financial institutions vulnerable to cyber threats.

Ransomware and malware continue to be among the most severe threats facing financial institutions. There have been reports of attackers standing up informational maps on the virus outbreak which are infected with malware designed to steal credential information and sometimes infect the host with additional malware. Phishing e-mails are being used to target individuals by posing as the World Health Organization, the Centers for Disease Control and Prevention and other legitimate organizations. These are just a few methods used to exploit a public in search of information on the pandemic.
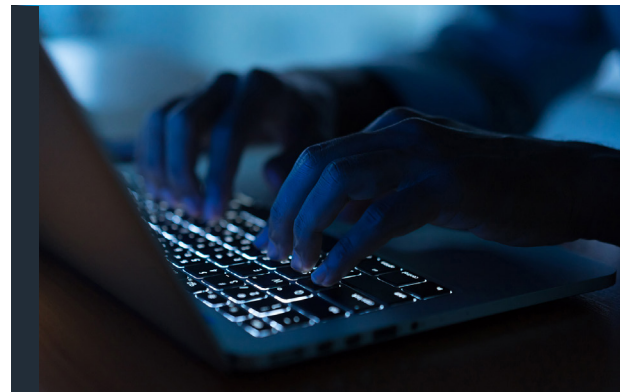
Next Steps for Security

In light of the increased activity among cyberattacks, here are a few tips to help you stay especially alert during the pandemic.

- Use trusted sources—such as legitimate, government websites – for up-to-date, fact-based information about COVID-19.
- Avoid clicking on links in unsolicited emails and be wary of email attachments. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Use multi-factor authentication (MFA) on your accounts where possible.
- Remind employees not to use personal workstations for business purposes. Organizations may not know how these assets are protected in home environments.
- Consider ramping up security awareness training.
- Ensure your devices have the latest security updates and antivirus definitions.
- The Cybersecurity and Infrastructure Security Agency (CISA), a division of Homeland Security, is a great source for further information regarding COVID-19 and cybersecurity threats during the pandemic.

Security is always at the forefront for financial institutions. However, during this pandemic, it is even more important to stay vigilant about your cybersecurity for the safety of your customers, your employees and your institution.