DEVELOPMENTS THAT MATTER

Improving Your Cybersecurity During the Pandemic

COVID-19 has forced millions of Americans to work from home. With virtual meetings and digital commerce becoming the new normal, workers and businesses have had to adapt. But so too have cybercriminals, making employers and employees susceptible to cyberattacks in new ways.

The U.S. Chamber of Commerce and FICO today released their *Special Report on Cybersecure Remote Working During COVID-19*. It digs into the evolution of cybersecurity threats during the pandemic and offers insights on how companies can protect themselves.

There is one constant with cybercriminals: Malicious actors will always try to exploit vulnerabilities. This becomes easier for them in times of change, disruption and, uncertainty, which we have experienced during the pandemic.

According to Trend Micro, COVID-19 related cyberthreats surged from January to June 2020. Nearly all of them (91.5%) were via email. At the same time, average ransomware demands from cybercriminals increased by $500,000 since last year to an average of $1.3 million in 2020.

How to protect your business:

1. Consider the benefits of using cloud services
2. Instruct employees on the proper components of a home office network
3. Use a properly configured virtual private network (VPN)
4. Take steps to introduce elements of security to teleconferencing
5. Have a plan to identify and manage third-party and supply-chain risk
6. Think through—and adhere to—sound Bring Your Own Device (BYOD) policies and procedures

We know Americans have enough to worry about with economic uncertainty, health concerns, job losses, and so forth, and we want to ensure business owners have the right tools to increase the security of their virtual working environments. This report provides recommendations and expert opinions that will help that process.

—Christopher Roberti, Senior Vice President for Cyber, Intelligence, and Supply Chain Security Policy, U.S. Chamber of Commerce