



## Applying Social

# Distancing Guidance to Your Digital Life

By Dean Choudhri, CISSP, CISM, CRISC\*, Assistant Vice President, Cybersecurity and Information Assurance, Alloya Corporate FCU

---

In March of this year, things changed for nearly everyone in this country. Virtually every aspect of our daily lives and routines were turned upside down due to stay-at-home orders resulting from COVID-19. Many of us were required to work from home where we had to share bandwidth, and perhaps devices, with our spouse and/or kids. The past few months made us change how we approach everyday activities, but also became a great opportunity to change our approach to cybersecurity.

Like many organizations early on during the pandemic, some credit unions found themselves unprepared for the sudden move to remote work. To ensure they were able to continue serving members some credit unions may have relaxed their cybersecurity controls, including:

- Allowing employees to use unsecured personal computers and devices
- Copying data to thumb drives to work from home
- Providing additional access to a vendor

All these adjustments were thought to be temporary. And while credit unions were doing everything they could to continue serving members, cybercriminals saw a great opportunity to capitalize amongst the chaos and uncertainty as COVID related phishing and other cyberattacks skyrocketed.

Now that we are six months into this, organizations need to reevaluate their cybersecurity posture by conducting a risk assessment to help understand the following key questions:

- Are employees still using unsecure devices?
- Are VPN capabilities sufficient?
- Have unnecessary privileges been revoked?
- Do we have visibility into remote users and workstations?

Social distancing measures were recommended to ensure that you remain safe from COVID-19. The same concept should be taken to our digital presence as well by practicing *digital distancing*. Digital distancing can help keep your computing assets from being infected and infecting others. Think of it like this:

- A network or host-based firewall serves as a face mask
- Validating patches and vulnerabilities before allowing a device to enter the network serves as the temperature check
- Quarantining assets with critical vulnerabilities until patched serves as the 14-day quarantine
- Keeping your systems healthy by only connecting to known networks and using a VPN serves as social distancing (digital distancing!)

This pandemic will end, however, the social and digital lessons learned should help ensure that we are better prepared for the next one. For more information on cybersecurity risks during the COVID-19 pandemic, be sure to listen to our cybersecurity webinar recording **[here](#)**.

---

Dean Choudhri can be contacted at **[dean.choudhri@alloyacorp.org](mailto:dean.choudhri@alloyacorp.org)**.

\*CISSP: Certified Information Systems Security Professional

\*CISM: Certified Information Security Manager

\*CRISC: Certified in Risk and Information Security Control