Dustin Mooney
Cybersecurity From Home

BIG i SM
AGENTS COUNCIL FOR TECHNOLOGY.

Questions and Answers from the ACT Meeting April 22, 2020

Q: Can you talk a bit more about Endpoints & protection? If I am a small agency, and have minimal budget and have already spent a lot on in-office workstations, can I allow my employees to use their personal computers? Or is the best practice to purchase dedicated laptops for remote work?

A: Contact your MSP or endpoint protection vendor. Some are doing 90 days trials for additional licenses or capabilities. They may also allow you to transfer the license from your work computers to home users computers.

Q: Please elaborate a bit more on creating our own WFH Network and what this entails.

A: Yes, it does indeed include commas and periods. While search engines are probably smart enough to know they are the same, all the experts say we don't need to make it unnecessarily hard. So, whether you abbreviate suite with a period or spell it out, the format needs to be the same across all online listings.

Q: This seems like a LOT for my employees to understand. Are there 'best practices' on planning, especially communications through a remote environment?

A: NIST has a lot of planning guidelines that can be found here: https://www.nist.gov/itl/smallbusinesscyber/planning-guides. Communication to employees is not cybersecurity specific, so you'll need to determine your own policy for communications. However, some concepts you'll want to repeat are: Report malicious or phishing emails, report potential malware or breaches, sending out cybersecurity reminders or newsletters. Acquire a security awareness training platform to facilitate test phishing emails and training campaigns.

Q: What is realistic when it comes to multi-factor authentication for a smaller-sized agency? I know there are different types.

A: Realistically, all logins should require two-factor authentication. This is a huge risk reduction step for very little effort. Application needs will vary company to company, so work with your MSP to identify all the places where two factor can be turned on. Configure those systems and applications to require two factor authentication. Determine which ones do not and enforce strong passwords for those systems.