10 Data Protection Tactics to Act on for Remote Working

Mike Scott, CSO at Spirion

9 April 2020

Agenda

- Introduction
- Overview
- WFH Data Protection Tactics
- Questions
- How Spirion can help

Housekeeping Matters

A few things before we start…

- We will email out a copy of this presentation and the recording to the email you used to register
- There will be time at the end for questions, but use the chat function if you want during the presentation; if we don't get to all of the questions, we will follow up with you individually afterwards
- If you are having sound/viewing issues, please check your computer's settings first. If the problem isn't fixed, please alert us with the chat function. If more than one person reports a problem, then we'll know that the issue lies with the platform rather than your device. There is also a small amount of lag between when the slides change on the presenter's computer and when you see them on yours.

ON TO THE WEBINAR!

Mike Scott, Chief Security Officer at Spirion

- More than 20 years of experience providing scalable and secure solutions for global organizations.
- Executive Director, Office of the CISO with Optiv, Inc.
- Chief Information Security Officer for The Wendy's Corporation
- Global Information Security Manager for Verint.

1. Is a VPN enough for security?

By itself, it is not enough.

- VPN provides a secure connection over the internet
  - Split tunneling has additional risks
  - Restrict traffic over VPN
  - Enforce Multi-Factor Authentication
  - Enforce idle time-outs and re-authentication
- Defense in depth is still the best approach
  - Software firewall
  - Anti-malware software
  - Update all applications
- Talk to your IT department before you do anything
  - Installing unapproved / unsupported software could create several problems.

2. What areas should an effective work from home security and use policy cover?

NIST 800-46

- What forms of remote access are permitted?
- What types of devices are permitted (corporate, BYOD, mobile)
- What kind of access is permitted? (full access, email only, etc.)

Set clear expectations

- Do you want users to self-remediate technical issues?
- What about installing software?
- Think about privacy, help your employees understand the dangers of letting their family use their device

3. Advice to decrease employee data proliferation when using multiple devices from home

Business is anything from usual right now

- Stress and anxiety is a factor
- Pressure to deliver has never been higher
- Combined, these factors can lead to clouded judgement

Educate your employees, encourage feedback

- Systems that are overly complex may be circumvented
- Shadow IT is just too easy today

Use your existing / approved centralized file storage.

- Verify that backups are occurring and that restoration is functional
- Limit local file storage
- Don’t use email as a file transfer mechanism
- Name your files logically

4. Data privacy *after* work from home ends—what to do with leftover company data that might not make it back to the office

Protecting data privacy after work from home ends…

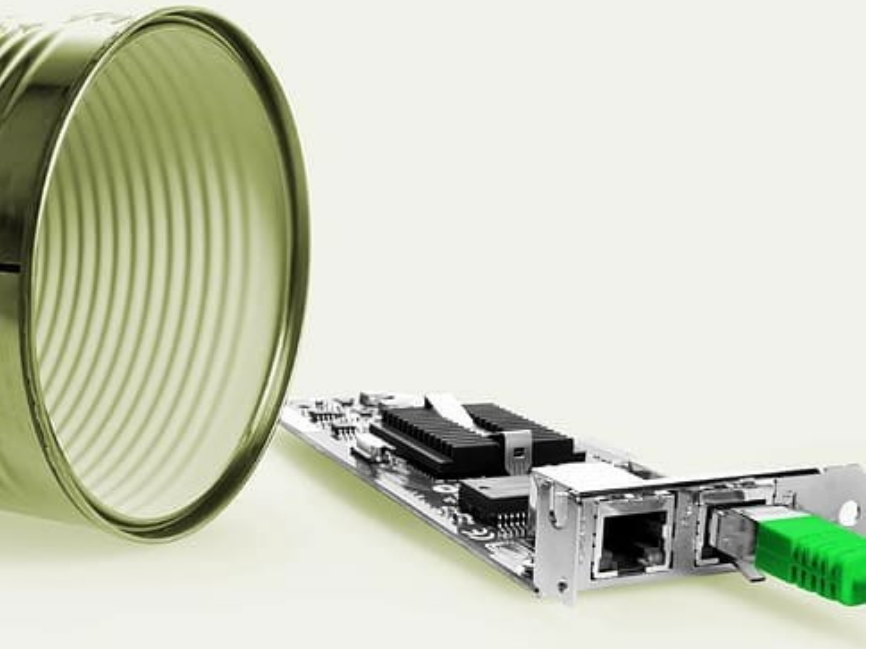
- Educate your employees, set expectations
- Avoid using your personal devices if you can
- Limit access to match your risk tolerance
- Keep the files in a central location
  - Company approved storage
  - Do not sync company data to your personal devices
- Keep printed work documents in one location
  - Your work backpack for example
  - Shred unneeded printed files

SPIRION

5. How to ensure data privacy when your home is crowded with multiple people

- Be aware of your surroundings
  - Can anyone see your screen?
  - Can anyone hear your conversation?
- Can anyone overhear your conversation?
  - Legal issues
  - Interpersonal issues
- Don’t share your device with your family
  - Accidental data deletion or modification
  - Longer meantime to repair due to damage

6. Ensuring security on home networks with multiple devices connected, especially IoTs like fridges and Alexa



- Take advantage of existing security features on network devices
- Segment your network
    - Guest network for IoT, Xboxes, Etc.
    - Enable host firewalls
- Consider eliminating split-tunneling

Resources to test your home firewall

Use at your own risk!

- Censys.io
- Grc.com / ShieldsUp

7. The higher risk of phishing scams and social engineering by hackers in a crisis

Phishing/Malicious sites have increased 350% since January*

Over 300k suspicious COVID-19 related sites**

Educate your users

- Don't click on links – navigate directly to trusted resources.
- Be paranoid. If you aren't sure…ASK
- Don't get caught off-guard, pause, think, then act

Review your SPAM filter, consider increasing sensitivity levels

*Report from Google
**RiskIQ

8. Safe browsing habits:

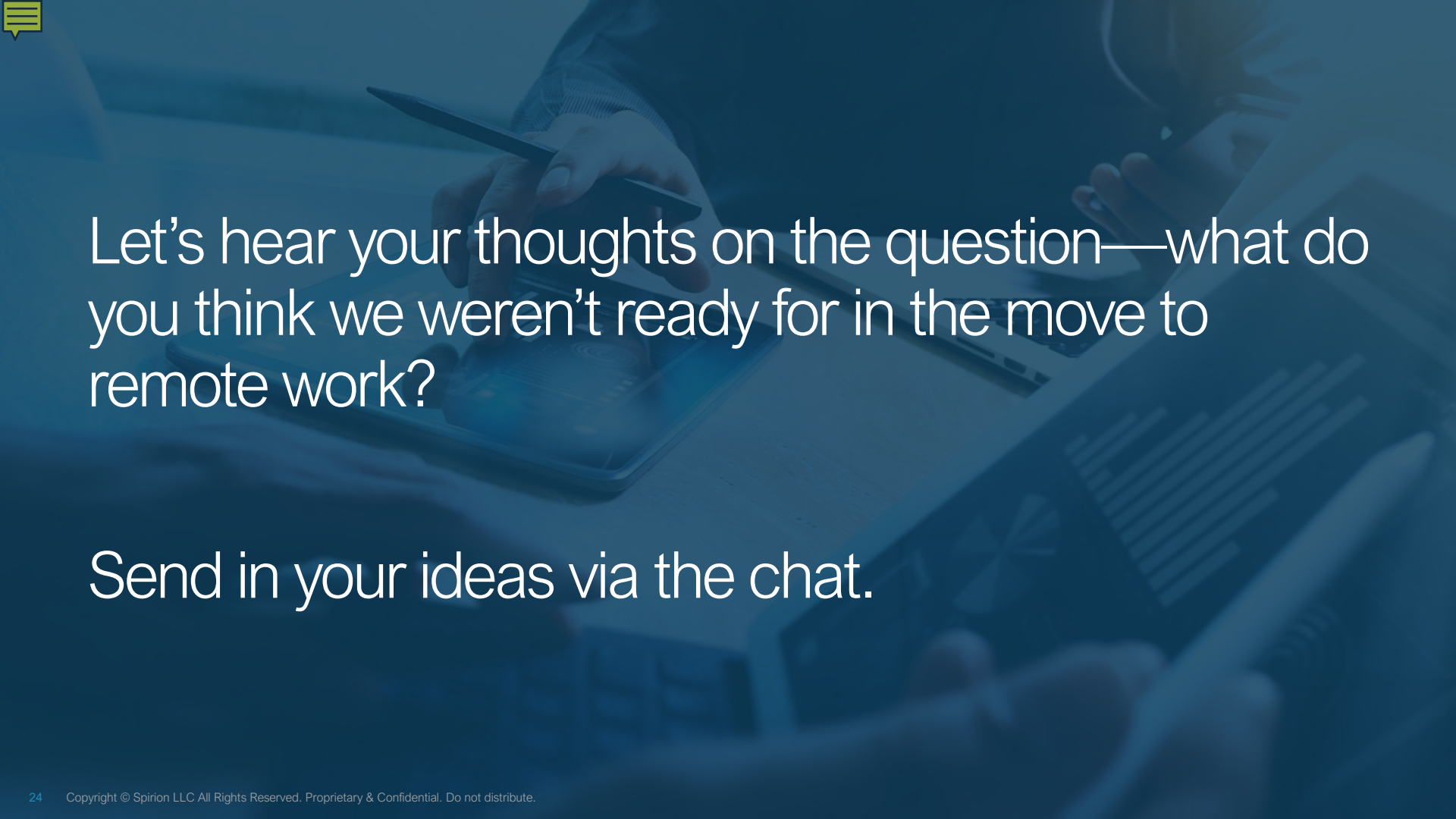
How to avoid scammy websites set up by bad actors to mimic CV-19 help

- Implement existing security features on your home firewall or security software
- Upgrade your home firewall (examples)
  - Firewalla
  - Ubiquiti
  - Eero
- Leverage device based security options.
  - Norton – includes features for anti-spam and anti-malware for example
  - OpenDNS (Cisco) - proven service Prosumer $20 a year per user.

9. How to deliver effective cyber security training (and ongoing communication) to at-home employees in the midst of the sudden shift to WFH

- Build lessons from current events
  - Zoom bombing, UNC issues, backgrounds, oh my
  - Phishing COVID-19 examples
  - IRS scams
- Continually reinforce key messages
- Keep things interesting, fun if possible
- Free resources are abundant
  - SANS - Free “Work-from-Home Deployment toolkit
  - FTC Consumer Information

10. What did we miss in the sudden rush to go remote? What security and data privacy concerns are companies overlooking that weren't covered in tips 1-9?



Let’s hear your thoughts on the question—what do you think we weren’t ready for in the move to remote work?

Send in your ideas via the chat.

Questions

SPIRION

How Spirion Can Help with Remote Data Protection

Try our Discovery Agent

COVID-19's global impact is forcing change upon organizations to mobilize their work-forces. In many cases, employees and students are completing their daily tasks at home on personal devices that may contain sensitive data.

Spirion's free data discovery agent allows you to:

- Discover what sensitive data lives on your personal desktop (i.e. credit card numbers, social security numbers, bank account numbers, driver's license numbers, and passwords)
- Identify the location of unsecured sensitive data
- Understand how to protect your sensitive data

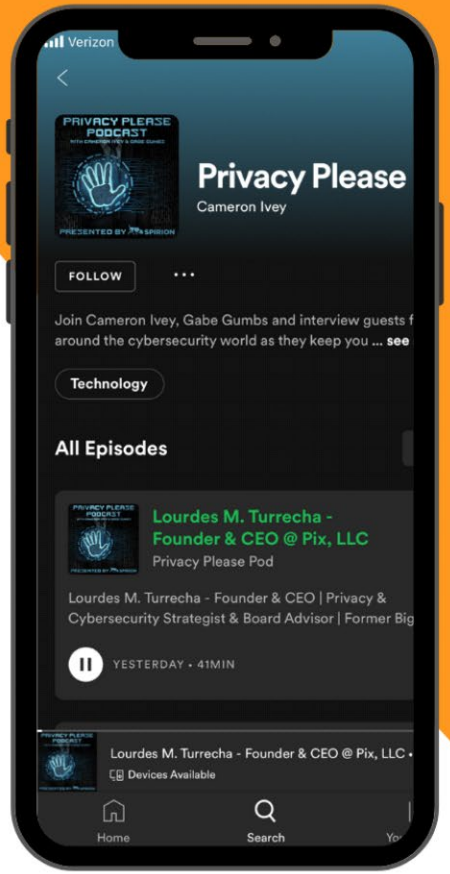
Try out the Discovery Agent: Click here to learn more (link will also be in the chat)

SPIRION

Visit Our Privacy Please Podcast

Available on Spotify, Google Podcasts, iTunes or anywhere you get your podcasts.

LISTEN NOW



Thank you!

Want to follow up?

Mike.Scott@Spirion.com