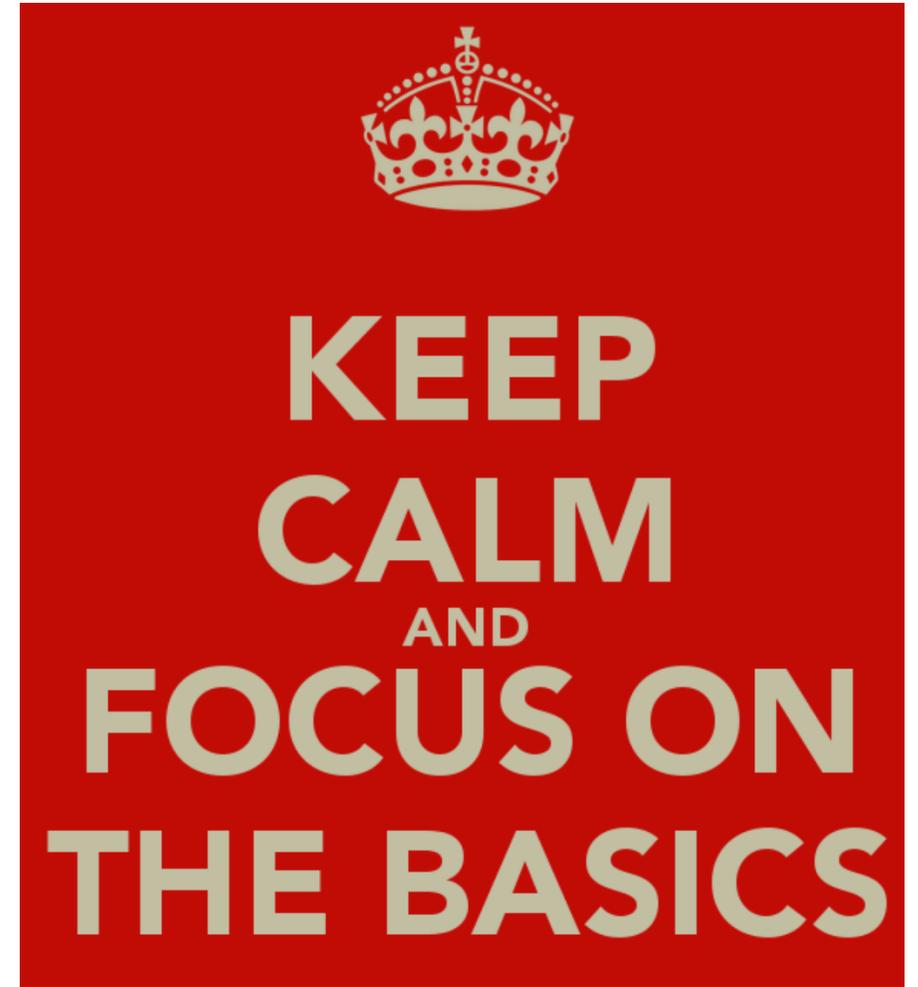


Who am I?

- Justin Jones
 - Associate Vice President, IT Risk Manager (D.A. Davidson Companies)
 - Adjunct Faculty, Cybersecurity (Great Falls College MSU)
 - MS: Information Assurance & Computer Security
 - BS: Major-Computer Science, Minor-Business Administration
 - CISM: Certified Information Security Manager
 - CRISC: Certified in Risk and Information Systems Control
 - CISSP: Certified Information Systems Security Professional
 - CISA: Certified Information Systems Auditor
 - CEH: Certified Ethical Hacker
 - And others...

Basics

- Keep Software Updated
- Backup Important Files
- Use Passphrases
- Encrypt
- Use Multi-Factor Authentication (MFA)
 - <https://twofactorauth.org/>



Phishing, Vishing, and Spear Phishing, Oh My!

Red Flags

- Unrecognized sender or *strange* email from recognized sender
- Asking you to do something outside your normal job responsibilities
- Your email is in the BCC line
- Unusual list of people (if not in BCC line)
- Bad Grammar
- Urgency
- More Red Flags: <https://blog.knowbe4.com/red-flags-warn-of-social-engineering>



Business Email Compromise (BEC)

An email address at your business or a trusted partner is compromised (hacked)

Protection

- Basics & awareness
- Email security (Technical: SPF, DKIM, DMARC)
- Report: [ic3.gov](https://www.ic3.gov) or reportphishing@apwg.org
- Notify customers and/or partners



Ransomware

How you get infected

- Phishing emails
- Infected websites
- Ads

How to protect your business

- Basics, especially backups
- Awareness & planning
- Immediately disconnect infected device(s)
- Contact authorities (local FBI)
- Notify customers



Tech Support Scams

Often work by:

1. Phone call
2. Installation of remote access software
3. Installation of persistent malware
4. Payload
 - Unnecessary software
 - Repair services
 - Unnecessary maintenance programs
 - Credit info to commit fraud



Wi-Fi Security

- Require secure connections through Wi-Fi Protected Access 2 (WPA2) or WPA3
- Only use public Wi-Fi if using a Virtual Private Network (VPN)
- Separate Guest and Business Wi-Fi
- Don't allow smartphones to automatically connect to public Wi-Fi

Cyber Insurance

I'm not an expert and can't offer legal advice, but basic coverage recommendations are:

- Data breaches
- Cyber attacks on data held by third parties
- Cyber attacks on your networks (denial of service)
- Terrorist attacks

Questions?

Helpful Resources

FCC CyberPlanner: <https://www.fcc.gov/CyberPlanner>

KrebsonSecurity: <https://krebsonsecurity.com/>

Krebs - Value of Hacked Email: <https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>

FTC OnGuard Online: <https://www.consumer.ftc.gov/features/feature-0038-onguardonline>

SANS Ouch! Newsletter: <https://www.sans.org/security-awareness-training/ouch-newsletter>