

# CYBERSECURITY AWARENESS

ROBERT L. HOSTER, CPA, CISA, CFSA, CFIRS  
SUPERVISOR

*FEBRUARY 17, 2022*



Guidance You  
Can Count On.



## **ROBERT L. HOSTER, CPA, CISA, CFSA, CFIRS**

- Supervisor
- Joined SEK in 2013
- 40 years of experience
- Graduated from Pennsylvania State University with a Bachelor of Science degree in Accounting and Information Systems
- Specializes in providing internal audit, tax audit, information technology audit, loan review, and Sarbanes-Oxley services

# **CYBERSECURITY AWARENESS – EMAIL**

# CYBERSECURITY AWARENESS – EMAIL

Safety tips for your email:

- Change your password often
- Use strong passwords
- Use a different password for each of your accounts
- Don't open any suspicious attachments
- Beware of "Enable Macros"
- Use updated anti-virus software

# CYBERSECURITY AWARENESS – EMAIL

- Learn how to recognize phishing attempts:
  - Messages that contain threats to shut your account down
  - Requests for personal information, such as passwords or Social Security numbers
  - Words like “Urgent” – false sense of urgency
  - Forged email addresses
  - Poor writing or bad grammar
  - Look at the time the email was sent
- Hover your mouse over links before you click on them to see if the URL looks legitimate
- Don’t give your email address to sites you don’t trust

# CYBERSECURITY AWARENESS – EMAIL

- Don't post your email address to public websites or forums
- Don't click the "Unsubscribe" link in a spam email
- Don't send personal information in an email message
- Don't reply to spam
- Don't share passwords
- Be sure to log out



# **CYBERSECURITY AWARENESS – SOCIAL MEDIA**

# CYBERSECURITY AWARENESS – SOCIAL MEDIA

- Never “click and tell”
- Update your privacy settings
- Connect only with people you trust
- Report suspicious or harassing activity



# **CYBERSECURITY AWARENESS – TRAVELING**

# CYBERSECURITY AWARENESS - TRAVELING

- Before you go
  - Backup your information
  - Connect only with people you trust
  - Keep software up-to-date
  - Double your login protection
- During your trip
  - Stop auto connecting
  - Stay protected while connected
  - Guard your mobile devices

# **CYBERSECURITY AWARENESS – IMPOSTER SCAMS**

# CYBERSECURITY AWARENESS – IMPOSTER SCAMS

- Examples of imposter scams:
  - Posing as a bank
  - Downloading of apps to your cell phone
  - Gift cards
- Preventative measures
  - Customize your passwords
  - Enable multi-factor authentication
  - Use encryption
  - Don't reveal personally identifiable information (PII)

# **CYBERSECURITY AWARENESS – WORK FROM HOME – EMPLOYEES**

# **CYBERSECURITY AWARENESS – WORK FROM HOME – EMPLOYEES**

- Secure your home office
- Secure your home router
- Separate work and personal devices
- Encrypt your devices
  - Windows: turn on BitLocker
  - macOS: turn on FileVault
  - Android: enabled by default since Android 6
  - iOS: enabled by default since iOS8



# **CYBERSECURITY AWARENESS – WORK FROM HOME – EMPLOYEES**

- Use supported operating systems
- Keep your operating system up-to-date
- Keep your software/applications up-to-date
- Enable automatic locking
- Use a strong PIN/password on your device
- Use an anti-virus software

# **CYBERSECURITY AWARENESS – WORK FROM HOME – EMPLOYEES**

- Invest in a password manager
- Enable two-factor authentication and use an authenticator app
- Enable Find My Device and Remote Wipe
- Wipe any devices before you share, sell, or dispose of
- Use a Virtual Private Network (VPN)

# **CYBERSECURITY AWARENESS – WORK FROM HOME - EMPLOYERS**

# **CYBERSECURITY AWARENESS – WORK FROM HOME – EMPLOYERS**

- Invest in Cybersecurity Awareness Training
- Monitor your third-party vendors and service providers
- Implement adequate email security practices
- Use access controls

# **CYBERSECURITY AWARENESS – WORK FROM HOME – EMPLOYERS**

- Use security metric applications to monitor your cybersecurity performance
- Enforce strong passwords on employee devices
- Invest in organization-wide password management tools
- Encrypt all company devices



# Q&A

---

ROBERT L. HOSTER, CPA, CISA, CFSA, CFIRS  
SUPERVISOR  
RHOSTER@SEK.COM