PRIVACY AND DATA SECURITY

1. Conduct an inventory to help you answer:
   - *What kind of data do you have?*
   - *How is the data handled and protected?*
   - *Who has access to the data?*
2. Once you've identified your data, keep a record of its location and move it to more appropriate locations as needed.
3. Develop a privacy policy
4. Protect data collected on the Internet
5. Create layers of security
6. Plan for data loss or theft

SCAMS AND FRAUD

1. Train employees to recognize social engineering
2. Protect against online fraud
3. Protect against phishing
4. Don't fall for fake antivirus offers
5. Protect against malware
6. Develop a layered approach to guard against malicious software
7. Be aware of spyware and adware
8. Verify the identity of telephone information seekers

NETWORK SECURITY

1. Secure internal network and cloud services
2. Develop strong password policies
3. Secure and encrypt your company's Wi-Fi
4. Encrypt sensitive company data
5. Regularly update all applications
6. Set safe web browsing rules
7. If remote access is enabled, make sure it is secure
8. Create Safe-Use Flash Drive Policy

EMAIL

1. Set up a spam email filter
2. Train your employees in responsible email usage
3. Protect sensitive information sent via email
4. Set a sensible email retention policy
5. Develop an email usage policy certain types of sensitive data

FCC CYBER SECURITY CHEAT SHEET

Download Cyber Security Guide

WEBSITE SECURITY

1. Carefully plan and address the security aspects of the deployment of a public web server
2. Implement appropriate security management practices and controls when maintaining and operating a secure web server
3. Ensure that web server operating systems meet your organization's security
4. Ensure the web server application meets your organization's security requirements
5. Ensure that only appropriate content is published on your website
6. Ensure appropriate steps are taken to protect web content from unauthorized access or modification.
7. Use active content judiciously after balancing the benefits and risks
8. Use authentication and cryptographic technologies as appropriate to protect certain types of sensitive data
9. Employ network infrastructure to help protect public web servers
10. Commit to an ongoing process of maintaining web server security.

MOBILE DEVICES

1. Use security software on all smartphones
2. Make sure all software is up to date
3. Encrypt the data on mobile devices
4. Have users password protect access to mobile devices
5. Urge users to be aware of their surroundings
6. Employ these strategies for email, texting and social networking
7. Set reporting procedures for lost or stolen equipment
8. Ensure all devices are wiped clean prior to disposal

Useful Links:

Center for Internet Security (CIS)
Free online security check ups
SANS Institute's Most Critical Internet Security Vulnerabilities
NIH Online User Training
FCC Ten Cybersecurity Tips for Small Businesses