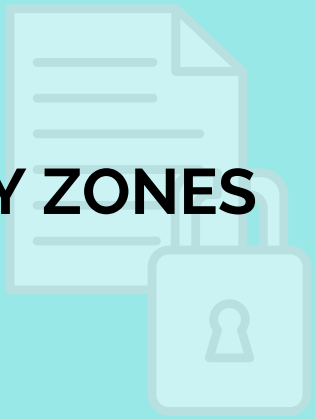
5

Know & Defend Your
CRITICAL CYBERSECURITY ZONES

Tips for setting up processes and developing habits to increase your cyber safety.



COMPUTER

Lock & Update

- Use multi-factor authentication to log in and to unlock your computer.
- Lock your screen before you leave your workstation.
- Check with your IT department to be sure that anti-virus and anti-malware are installed, and that your computer is set to automatically update your operating system and applications.

PASSWORDS

Change Often!

- Change your passwords frequently.
- Create a unique password for every online account.
- Avoid storing passwords in plain text or on paper.
- Use longer passwords of upper and lowercase random words such as “BlueHamburgerMovie,” adding numbers and punctuation marks.
- Don’t share your passwords!

CLOUD

Be Smart About How You Connect

- Never use unsecured WiFi.
- Only send information when you’re sure the connection is secure and you know the recipient.
- Use the VPN or SSH set up by your IT department.

EMAIL

Know What to Look For

- Check the “from” field: Is the sender’s email address legitimate?
- Do not use a personal email address for business purposes.
- Contact your IT department if the sender or attachment seems odd.
- Call any known sender directly to ask about any suspicious email.

YOU

Think Before You Click!

- Hover over links to check that the URL is legitimate.
- Never download or open attachments from an unknown source.
- When in doubt, call your IT department.