AXICOM

Networks • Computers • Security • Service

Cyber Security Tips

Phishing Scams

- Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to cause individuals to send personal information such as passwords and credit card numbers
- Companies might send you an invoice by mail; if you do not recognize the email sender, do not open it!
- Think about whether you might have ordered the item and if not, ignore and delete.
- Phishing scams are becoming more sophisticated so they might have some accurate details—be careful about those.

Ransomware

- Ransomware is malicious software designed to prevent access to your computer system until a sum or “ransom” is paid.
- Various ransomware attacks have occurred recently including WannaCry and Nyetya. Sometimes the software will ask for payment in Bitcoins (digital currency that operates outside of a central banking system).

Mobile Security

- Protect your phone with a password
- Use a backup plan: Apple iCloud (50GB/$1mo) or Google Drive (100GB/$2/mo)

Data Backup

- Cloud backup
- USB hard drive backup
- Network Attached Storage (NAS)

Protect Yourself and Your Business

- Have a geek, knowledgeable family member or computer consultant you can contact when questions come up
- Never give a stranger remote access
- Don’t believe claims from people who call/email/message you that they are from Apple or Microsoft
- Have proactive maintenance on your computer
  - Use antivirus and antispyware
  - Install security patches
  - Install application updates
- Backup your data
- Enable 2 factor authentication
- Make sure to have a firewall and router in place.

If you have additional questions or would like a cyber-security audit of your business, contact AXICOM.