CYBERSECURITY TIPS

Staying Safe in Our Digital World

Topics

- Telemarketing / Telephone Scams
- Common Cybersecurity Dangers
- Best Practice Recommendations
  - Email and Text
  - Passwords
  - Scam and Spam
  - Social Media and Shopping
  - Computer Systems
- Backup
- Helpful Resources

Telemarketing Scams

The Warning Signs

- Caller claims to be from your bank or credit card company
- Caller claims to be from the IRS or Social Security Administration
- A stranger asks you to “help” a person who is in another country
- A caller informs you that you have won a gift, prize, or free vacation
- Caller says it’s “urgent”, return the call right away because it is a limited time offer
- To purchase a service offered, you must pay a large up-front fee

Telemarketing Scams

What to Do – What not to Do

- Verify phone requests by hanging up and calling the organization
- Do not provide financial or personal information over the phone
- Hang up if you feel pressured
- Avoid making phone purchases that require payment up-front
- Avoid high-pressure offers that require you to act immediately
- Avoid returning calls to unknown area codes
- Never pay money up front to receive a prize or credit offer

Cybersecurity

The Common Dangers

- **Phishing and Smishing** - emails or text messages leading individuals to reveal personal information like passwords and credit card numbers
- **Fraudulent Tech Help sites** that download their software and take control of your system remotely
- **Spam** – junk email, usually to sell something
- **Social Engineering** of Social Media to gather personal information
- **Malware** - malicious software used to disrupt or access your computer
- **Ransomware** - restricts or disables your computer then demands a fee to fix the problem

Email and Text Recommendations

- If you receive a suspicious email or text
  - Reach out to that person by phone to make sure they really sent you the message
- If you suspect you’re corresponding with a hacker
  - STOP emailing them, delete their emails, and change your password
- Your email address is a common Username
  - Use a strong email password and change your email address password(s) every time you turn the clocks back
- Turn on Two-Factor identification for email and especially when logging on to financial institution websites
- Place a “post-it note” over the camera on your computer

Password Recommendations

- Use STRONG passwords with at least eight characters, longer is better
- Use a mix of capital letters, small letters, numbers, and special characters
- Use stronger passwords and two-factor authentication for sensitive information like financial accounts
- Make it unique. Could be meaningful but complicated
- Don’t use common words like your name, your pet’s name or “password” or “abc123”
- Use unique passwords for different accounts. Don’t let a hacker of one account get into them all
- It’s okay to write them down but hide the paper away from the computer
- Use a secure password manager like Keeper, Blur, Sticky Password

SCAM and SPAM Recommendations

- SCAM
  - Appear to be from legitimate organizations with recognized names like Medicare, American Express, Fidelity
  - Look for telltale signs like offers too good to be true, misspellings, poor punctuation, typos, asks for personal information
  - Don’t click on links or open attachments
  - Delete and don’t respond
  - Use protective software with a SPAM filter
  - Check the SPAM folder for legitimate email then delete the rest
- SPAM
  - Junk email, usually to sell something
  - Over One Billion sent every day
  - Delete these and don’t try to “Unsubscribe”

Social Media & Shopping Recommendations

- Your personal information is valuable so be mindful of what you’re sharing
- Don’t post sensitive information
- Don’t share your location when you’re away from home
- Be aware of the privacy settings
- Don’t link different accounts like Facebook and Twitter
- Log out from public computers or Wi-Fi (e.g., Starbucks, Hotels)
- When shopping online, look for trusted sites with “https” and lock symbol
    - Look for VeriSign, BBB, Trust/Verify
- Keep or destroy receipts

Computer System Recommendations

- Protect your device with a cyber security package like Windows Defender, McAfee LiveSafe or Norton Security Suite
- Check for updates to your Operating System (e.g., Windows, IOS)
- Don’t let a help site take remote control of your system

THE IMPORTANCE OF BACKUP

- All devices can crash
- Phones, tablets, laptops can be stolen
- Backup on your system
- Backup to an external device – thumb/flash drive, external hard drive
- Cloud Backup
  - Microsoft One Drive
  - Apple iCloud
  - Dropbox

Helpful Resources

- Contact Waterfront Village
  - Request Tech Help
- Access the Tech Corner on Northwest Neighbors Village website
  - Go to: www.nnvdc.org Click on Village Info and see Tech Corner on the list
  - There are links to several valuable resources
- Visit the website of Senior Planet, a charitable affiliate of AARP
  - www.seniorplanet.org
- Visit the website of AARP Virtual Community Center
  - https://local.aarp.org/virtual-community-center/