IMPORTANT Network Security Measures

(These policies will go into effect July 1st, 2019)

Desktop Users:

- Screen Saver is back! Screen saver must turn on after 45 seconds (computer must be password protected after 20 minutes).
- Personal documents must be stored in “Downloads” folder (These are stored locally on your computer and NOT backed up. (We are not responsible for lost personal documents).
- Work materials must be stored in Shared drive (Y:) for department use. You should have a Public folder and a Department folder.
- NEVER save IDs and passwords to a document your computer.
- NEVER leave an open computer unattended--you are required to lock your workstation if leaving for any reason.

Laptop Users:

- Use a secured network (that means a unique password is required).
- Use VPN client on a Hot Spot or from your secure home WiFi when accessing work files. If you’re traveling, use the Hot Spot instead of Hotel Wifi.
- Mark your laptop with a unique sticker so it doesn’t get confused with others. It’s easy for your plain black laptop to blend in.

Safe Practices:

- Do not bring files to work on USB stick and NEVER borrow a USB.
- Never send or share documents on unsecured websites. (“https://” websites are secure--look for the lock on chrome 🔒)
- Never open an email from someone you don’t know--follow up with a phone call for emails involving sensitive information (address hijack).
- Never visit non-work websites.
- Never stream videos (always ask management for training videos).
- Use Chrome, not Internet Explorer or Microsoft Edge.
- Do not give out “BLCO Staff” and “PEAP” WIFI passwords for public use--If your guest would like to use a personal device, phone, or laptop, etc,, always direct them to Public WIFI (password: public411).

New security measures MAY result in:

- Websites that worked before might be blocked.
- Emails with attachments will be scanned and can cause a delay.

- Mass mailer emails (groups larger than 50) might need special attention so they don’t get blocked or end up in a Spam folder.
- Blount County websites where data is accessed may require user registration before accessing content.
- Generic IDs and passwords will be prohibited (eg. multiple people using one account).

Viruses and attacks are always a possibility

- If you see an email from someone you don’t know, never open, forward, or reply to the email (PHISHING).
- Your bank, IRS, Social Sec Admin, Ebay, Amazon, etc. will NEVER ask for account information over email -- this is a scam no matter how convincing it looks -- go to the correct website of that institution to see your account.
- Check the email address -- not just the name -- for matters involving sensitive information, or follow up with a phone call to make sure it is who you think (PHISHING).
- Double check URLs and email addresses from your vendors. For example, scammers use @de11.com instead of @dell.com (PHISHING)
- Misspelled words and bad grammar are typical scam giveaways (PHISHING).
- NEVER send sensitive information over email--information must be delivered in person or over the phone (PHISHING)
- If screens are displaying differently -- random unknown pop-ups -- leave the site (MALWARE OR ADWARE)
- If you see strange programs you don’t remember loading, alert IT! (MALWARE)

REMEMBER: anything suspicious must be reported IMMEDIATELY; any delay in reporting can put others at risk.
You can never be too cautious. If you suspect anything at all, disconnect your blue ethernet cord and turn off your computer, then call IT. You can’t hurt anything by disconnecting, even if nothing is wrong!

For more info, please visit:

https://www.blounttn.org/1545/Cybersecurity-Central