Cyber Security Awareness

SLC CYBER Security: Avoiding Ransomware

Ransomware has been in the news a lot in the last few years, with growing attacks. But what is Ransomware and why should you be concerned about it? Ransomware is a form of Malware or infection that can attack your device, that when triggered, will lock your device until you either inadvertently infect other devices or are forced to pay a ransom. This is where the name comes from.

Why this particular form of malware is to be taken seriously, is the loss of access to information. Keep in mind what you store on your devices: Personal banking, tax information, school records etc. This information all poses a risk if exposed to the public or even just one person with bad intentions. Keeping your information safe is important, as we saw back in November, when our newsletter looked at issues such as Identity Theft.

CYBER Security: Ransomware

1. **Back up your files regularly.** Back-up your files to either a removable hard drive or to a cloud-based service such as One Drive by Microsoft. This is good to do as piece of mind against any form of Malware, so that your information is not lost. Additionally, this can assist you in keeping your device uncluttered.
2. **Disconnect from the internet when not in use.** If you suspect an issue, or are not using the internet, disconnecting from the network is suggested. Not only does this give your network a break, this also shuts down the communication pathway for ransomware to access your device.

3. **Anti-malware software.** We have mentioned this one before, and about keeping your anti-virus software up to date, but this just goes to show how important it is! You don’t need multiple programs, but having one is a must. You can even install anti-malware programs on most mobile devices now!
4. **Watch your emails.** When you are opening your emails, watch what you open and the links you click. If you don’t know the sender or the link seems wrong, delete it! Even here at the College, we get spam and most often it is the email address that gives it away.
5. **Read between the lines.** When reading a website or email check the spelling and grammar. Often if a website has been faked you will see typos and errors. Don’t forget to check the web address as well.

Now that you are an expert in ransomware… SHOUT OUT TO US! Let us know your top five ransomware tips by tweeting us or mentioning us on FB!

For more topics on e-security click here.

Got a great idea for next month’s **SLC CYBER Security –** timely information, you need to know? Share it! Let us know here or tweet us using #SLCE-security.