DECMEBER 2021 SAFETY
CYBERSECURITY

The Internet is a wonderful tool, but it is also loaded with traps and scams to be aware of. This month I will go over a few of these issues to help you both at work and at home to keep you and your information safe.

Passwords: This is the frontline issue that exposes your accounts. Weak passwords

Use the following tips to secure accounts –

1. Passwords should be 10+ characters in length, and a mix of upper and lower case letters
2. Include Special Characters (!#@$*%) and numbers
3. Avoid using only common words and NEVER personal information as passwords
4. Rotate or change your passwords every **90 DAYS**.
5. Consider using a phrase combination as a password, like: WhatTime!083O (last symbol is the letter O)

Phishing: This is the process of sending phony emails that will ask you to do something; follow a link, update account information or review a fraudulent statement. The emails are normally made to look like they are coming from popular companies: Apple, Amazon and Microsoft being three of the most popular ones that are faked. Here are things to look for:

1. Phishing emails have 'Sent From' address that does not match the company it claims to be. Example – Email claiming to be from Amazon could show: *Amazon.co.uk <anj3samaz0srvcs@himilowecomp.org>*
2. Poor grammar and punctuation is very common in fraudulent emails.
3. Hover the cursor over a link shows the address it will direct you to – What looks like Amazon could take you to himilowecomp.org and trick you into giving up your account name and password.

Ransomware: This software is that has the primary purpose of locking up your data and computer to force you to pay them to get access back. This can be extremely serious issue, and cities governments like Baltimore and recently New Orleans have fallen prey to these. Here are some things to look for:

1. Most ransomware comes in as part of a Phishing email.
2. They can appear as an attachment or a link that directs you to a website that immediately installs it.
3. Watch for the type of file you received. A file ending in a .exe is an executable file meant to install software
4. Keep your system up to date. Run your updates on Windows, browsers and antivirus regularly.
5. Keep Windows Firewall turned on and use your home router's firewall if it has one.
6. Scan ALL files after you download them, AND before you open them.

WIFI Security: Most of us have wireless internet access at home or use it when out in public places. Wi-Fi access is a great benefit but can also leave you vulnerable. Follow these tips to protect your home network and while away from home:

1. Be cautious using public access Wi-Fi. Do not log into sensitive accounts (banking, email) as it may expose your user name and passwords to hackers connected to the same Wi-Fi network.
2. At home, change your Wi-Fi Settings soon as you get it. Change the default name of the router to something personalized. Change the access name and password and use a strong password for getting to the router settings. For the Wi-Fi password, this also must be strong to keep others from gaining access to the signal.
3. Change the router encryption to WPA2. The encryption scrambles the data passed between devices and the router to prevent the information from being captured from outside and used.
4. Keep the router up to date. Companies like Netgear have made it very easy to check and install firmware updates.

I JUST GET THE FEELING OUR NETWORK ISN'T SECURE
offthemark.com
MarkParisi@aol.com
MARK PARISI
9-11
©2011 MARK PARISI DIST. BY UNIVERSAL UCLICK FOR UFS