Welcome to our first edition! We hope you'll find our monthly update useful. With so much of our daily routine online, we figured this could be a fun way to share our information and help you and your family become more Cyber Aware! Each month, you can look forward to a new topic and Rubes® cartoon. With October being Cybersecurity Month, we decided it would be a great time to start! Please let us know what you think or what you'd like to see in our next edition.

Visit us at any of the links below for more Cybersecurity Awareness information. Thanks!

Remember: “If you read it here, it’s probably Sketchy!”

**PHISHING**

*5 Types of Phishing Attacks:*
- **Email phishing:** most phishing attacks happen through email.
- **Spear phishing:** targets specific individuals whose data was previously collected.
- **Whaling:** targets senior management or those who have greater access privileges.
- **Smishing & Vishing:** uses a phone instead of written communication by sending SMS/MMS messages, or by having voice conversations through phone calls.
- **Angler phishing:** uses fake social media accounts that belong to well-known companies.

**How Does Phishing Work?**
It can happen to anyone, anywhere. A phishing attack can happen through emails, phone calls, texts, and social media. The more phishing emails that are sent out, the more likely someone is to fall for the attack. So, please stay vigilant!

**What Should I Watch For? What Should I Do?**
- Carefully analyze the email
- Watch for poorly written language
- Check addresses for misspellings
- Do not share personal credentials
- Do not download attachments
- Check destination before clicking links
- Delete all suspicious emails

**Fun Fact:**
Did you know RIT has it’s own Phish?

**Why Does Phishing Still Work?** A lack of cybersecurity awareness and poor protection of their personal information leaves users more vulnerable and susceptible while making attackers more successful.

**A Couple of Phishing Examples:**
An attacker pretends to work at a bank and sends the victim a link to update their banking information. Clicking on the link installs malware on the victim’s computer, giving the attacker full access to their accounts.

An attacker pretends to be an online entity and sends an email asking the victim to log in to a website that the attacker created to look exactly like the log in page for the intended destination. Once the victim logs in, the attacker steals their credentials, tells the victim the username or password didn’t work and then sends the victim to the actual log in page. This gives the attacker the access they need to misuse the victim’s account.

**Sketchy News is is sponsored by...**

**Next month’s topic: Man-in-the-Middle Attacks!**