New year, new habits

Cybercrime is on the rise and becoming increasingly advanced. This month's newsletter highlights some of the major security threats and habits you can form (and stick to!) to stay cyber-safe.

Malware and phishing threats and how to avoid them

Malware is short for "malicious software." Malware is any kind of malicious software a hacker can get onto your computer. A computer virus, for example. But any type of device that transfers data is at risk for a malware attack. So what can you do to protect yourself?

The most common attack method is via ***phishing***. Phishing emails look innocent, but those links hide malware ready to attack your system. Millions of phishing messages are sent daily, and they don't always come in the form of an email: text messages, phone calls and even paper mail have been used for phishing.

You receive an email with a malicious link or attachment. **Being suspicious** of odd emails is key to staying safe. Review your emails carefully before you click on anything.

Another malware attack method is through removable media, like a USB drive. An attacker might drop a malicious USB drive in a parking lot or an entryway, hoping someone will pick it up and plug it in. If you ever find a random piece of removable media, **report it!** Give it to your IT department. Never plug in any device or piece of removable media unless you know for certain that it's safe.

Cybersecurity best practices

There are ways to stay on top of cyberattacks. Here are a few tasks that you can add to your New Year's resolution list!

1 Create a strong passphrase

A passphrase is a string of words that's easy for you to remember but hard for someone to guess. The more complex the passphrase is, the stronger it is.

2 Keep your software up to date

Setting our devices to automatically update is helpful for staying on top of system updates. Updating keeps security risks at a minimum.

3 Use multi-factor authentication

MFA adds an additional layer of protection to your account. If a hacker breaks through one factor (such as a password), you still have another form of protection to keep your information safe.

4 Verify links and websites

Hover over links in emails to check the destination URL. If it seems suspicious, don't click! And be wary of websites that say HTTP instead of HTTPS (HTTP Secure). HTTPS websites are not 100% foolproof, but they are more likely to be safe.

A look into the DarkSide

DarkSide is one of the newer hacker groups. It is believed that they started their work in November of 2020. On their website, they stated that they are in the business of making money, "not creating problems for society." The group claimed that they will only go after profitable companies and will not hack hospitals, nursing homes or funeral homes.

The group has also donated to two different charities. They donated $10,000 to an organization that provides education to disadvantaged children and another $10,000 to an organization that helps provide clean water to communities in Africa. However, DarkSide is most widely known for the 2021 Colonial Pipeline hack, which disrupted fuel supplies to the eastern United States.