YOUR LOCAL IT COMPANY DECEMBER 2025

STI MSP NEWSLETTER

MANAGED SERVICE PROVIDER

Servicing the technology needs for businesses of all sizes. SINCE 1996

Issue 3

Tip of the Month

I hope you were able to try camelcamelcamel.com to see if you are getting a good deal from Amazon. Since it is holiday shopping time, I am going to list a couple of other sites that people find useful for shopping.

https://flipp.com – This site will show you all the current shopping circulars for your area. Go to this site and enter your zip code. You will get all the stores and supermarkets. It will allow you to click on the circulars and then click on products and save them to a shopping list.

https://retailmenot.com – This site lists coupon codes for many retailers' websites. Sign in with your gmail or non-business email. You will see a list of stores and websites. Click on them to see the deal or copy the promo code you will use when checking out.

Plugging The Biggest Hole in Security

From Al Toper, Director of Technical Services –

As we continue to find ways to protect you, we know that the biggest threat can be found somewhere between the chair and the keyboard. It is the end user. The criminals have tried to phish you with emails, adding tempting boxes on websites, or sending you texts that lead you to a place where you enter credentials.

We have implemented tools that are going to protect you from attacks from criminals that are looking for easy prey. What we call, low hanging fruit. They look for businesses or people that do not install cybersecurity tools or patch software running in their homes and offices.

The most successful ways that criminals do get into your systems, are by mass phishing or spear phishing campaigns. Mass phishing campaign are where they send phishing emails to a large mail list and hope that people click on them. Spear phishing is when they go after people which they have information about and are specifically tailoring their emails to fool that person. These are the ones you get that maybe from someone you know or businesses you have done worked with in the past.

Artificial Intelligence (AI) has taken this to the next level. In the past, when a hacker from a foreign country sent phishing emails, you could see they were put through a language translator. The grammar was bad and sounded like the email was written by a toddler. Using AI, they now can tell the AI agent to write the email using American grammar. They can tell it to make it sound urgent, humorous, or any other style that they feel may work.

That is where Security Awareness Training (SAT) comes in. SAT is a cybersecurity system that we have been implementing at our client's sites. I have spoken about it in the past. I want to clarify how it works, some of the roadblocks we have discovered now that most clients have had it, and a change we recently made. We recently switched the vendor we usedfor this service. Our new vendor has a better management service in the background and integrates with

Continued next page –>

Plugging The Biggest Hole in Security (continued)

Some Facts to Know

1. When the new tool is installed, you and your staff will have to sign up for an ID on the training platform.
2. The monthly trainings are 5-10 minutes.
3. You will be awarded a certificate for each training taken and they will be tracked by management.
4. The monthly training email and will come from the email address: **STI Security Awareness Training** *<notifications@alerts.mycurricula.com>*. Read these emails and take the associated training .
5. You and your staff will receive one fake phishing email per month. These will not come from any one address. They could come from an address you receive valid emails from presently or in the past. (They will have a link in them that you DO NOT want to click on.)
6. The manager should review how their staff is doing each month. It is understandable if someone does fall for one. We are looking for folks who fall for it every month. If you have an employee who does, they will most likely be the point of entry by a hacker in the near future.

other tools we use. Once a month, you will receive a training video. We need our clients' managers to assure that their staffs take the training. It is usually a 5-10 minute video, which are followed by a few questions to make sure the employee watched and paid attention. These videos are made with the understanding that almost any age could watch and understand them. Personally, we find them a little archaic, but they do show real world examples, and the content is on topic and important.

The 2nd part of SAT is Fake Phishing. You and your staff will randomly receive, during the month, a fake phishing email. This is to test you and keep you on your toes. The email will look like it is from a real vendor. It may sound urgent or use terms that make you want to click on it. If you do click on it, it will request that you enter credentials. If you click on the link in the email, you will be taken to a page that will tell you that you were tricked. It will add you to a list of folks who were fooled and send you for more training. By knowing this could happen, which is much better than clicking on an actual phishing attempt, you and your staff will get better at staying sharp against these attacks. We implemented the new tool at STI recently and I am glad to say that our staff is now suspicious of any email we get. We want the same outcome for our clients.

BONUS TIP

Do you ever want to read an article or webpage, but the page has a paywall in front that wants you to sign up before it will show you the page? If this happens, you can go to the top of the page and copy the URL and go the site, www.removepaywalls.com and copy it into the URL box. It will show you the page. There are Option icons at the top if it doesn't work for the page on the first try. Just click Option 2 or 3 to try another way.