TECHNICAL FRAMEWORK
MANAGED IT & CYBERSECURITY

(970) 372-4940
info@techframework.com
https://techframework.com

TECH INSIDER

Run your business more effectively with our insider advice and techniques for IT.

2022

September

Inside This Issue

HOW OFTEN DO YOU NEED TO TRAIN EMPLOYEES ON CYBERSECURITY AWARENESS?

You've just completed your annual phishing training, where you teach employees how to spot phishing emails. You're feeling good about it until about 5-6 months later when your company suffers a costly ransomware infection because someone clicked on a phishing link.

You wonder why you seem to need to train on the same information every year and yet still suffer from security incidents. The problem is that you're not training your employees often enough.

People can't change behaviors if training isn't reinforced regularly. They can also easily forget what they've learned after several months go by.

So, how often is often enough to improve your team's cybersecurity awareness and cyber hygiene? It turns out that training every four months is the "sweet spot" when it comes to seeing consistent results in your IT security.

Why Is Cybersecurity Awareness Training Every 4-Months Recommended?

There was a study presented at the USENIX SOUPS security conference that looked at users' ability to detect phishing emails versus how often they were trained on phishing awareness and IT security.

Employees were tested at several different time increments:

- 4 months
- 6 months
- 8 months
- 10 months
- 12 months

It was found that four months after their training, they were still able to accurately identify and avoid clicking on phishing emails.

However, after 6-months, their scores started to get worse. Then they continued to decline further the more months that passed after their initial training.

So, to keep employees well prepared to act as a positive agent in your overall cybersecurity strategy, it's important they get training and refreshers regularly.

Tips on What & How to Train Employees to Develop a Cybersecure Culture

The gold standard for employee security awareness training is to develop a cybersecure culture. This is one where everyone is cognizant of the need to protect sensitive data, avoid phishing scams, and keep passwords secured.

Unfortunately, this is not the case in most organizations. According to the 2021 Sophos Threat Report, one of the biggest threats to network security is a lack of good security knowledge and practices.

The report states, *"A lack of attention to one or more aspects of basic security hygiene has been found to be at the root cause of many of the most damaging attacks we've investigated."*

Well-trained employees significantly reduce a company's risk of falling victim to any number of different online attacks.

To be well-trained doesn't mean you have to conduct a long day of cybersecurity training every four months. It's better to mix up the delivery methods.

Here are some examples of engaging ways to train employees on cybersecurity that you can include in your training plan:

- Self-service videos that get emailed once per month
- Team-based roundtable discussions
- Security "Tip of the Week" in company newsletters or messaging channels
- Training session given by an IT professional
- Simulated phishing tests
- Cybersecurity posters
- Celebrate Cybersecurity Awareness Month in October

When conducting training, phishing is a big topic to cover, but it's not the only one. Here are some important topics that you want to include in your mix of awareness training.

Ecovacs Deebot X1

Remember the Jetsons? Who didn't want a robot housekeeper? This is the closest thing on the market today.

This tiny robot can vacuum or mop without any add-ons. Featuring YIKO Voice Assistant, you can call it to start cleaning without the need for a third-party smart assistant. It's also self-cleaning and auto emptying.

https://www.ecovacs.com/

HOW USING THE SLAM METHOD CAN IMPROVE PHISHING DETECTION

Why has phishing remained such a large threat for so long? Because it continues to work. Scammers evolve

All they need to do is run down the cues in the acronym.

their methods as technology progresses, employing AI-based tactics to make targeted phishing more efficient.

If phishing didn't continue returning benefits, then scammers would move on to another type of attack. But that hasn't been the case. People continue to get tricked.

In May of 2021, phishing attacks increased by 281%. Then in June, they spiked another 284% higher.

Studies show that as soon as 6 months after a person has been trained on phishing identification, their detection skills can begin waning as they forget things.

Give employees a "hook" they can use for memory retention by introducing the SLAM method of phishing identification.

What is the SLAM Method for Phishing Identification?

One of the mnemonic devices known to help people remember information they are taught is the use of an acronym. SLAM is an acronym for four key areas of an email message that should be checked before trusting it.

These are:

S = Sender
L = Links
A = Attachments
M = Message text

By giving people the term "SLAM" to remember, it's quicker for them to do a check on any suspicious or unexpected email without missing something important.

S = Check the Sender

It's important to check the sender of an email thoroughly.

Often scammers will either spoof an email address or use a look- alike address that people easily mistake for the real thing.

L = Hover Over Links Without Clicking

Hyperlinks are popular to use in emails because they can often get past antivirus/anti-malware filters. You should always hover over links without clicking on them to reveal the true URL.

This often can immediately call out a fake email scam due to them pointing to a strangely named or misspelled website.

A = Never Open Unexpected or Strange File Attachments

Never open strange or unexpected file attachments, and make sure all attachments are scanned by an antivirus/anti-malware application before opening.

M = Read the Message Carefully

If you rush through a phishing email, you can easily miss some telltale signs that it's a fake, such as spelling or grammatical errors.

Get Help Combatting Phishing Attacks

Both awareness training and security software can improve your defenses against phishing attacks. Contact us today to discuss your email security needs.

HOME SECURITY: WHY YOU SHOULD PUT IOT DEVICES ON A GUEST WI-FI NETWORK

The number of internet-connected devices in homes has been growing exponentially over the last decade. A typical home now has more than 10 devices connected to the internet.

IoT stands for Internet of Things, and it basically means any other type of "smart device" that connects online beside computers and mobile devices.

Here are two alarming statistics that illustrate the issue with IoT security:

- During the first six months of 2021, the number of IoT cyberattacks was up by 135% over the prior year.
- Over 25% of all cyberattacks against businesses involve IoT devices

Hackers Use IoT Devices to Get to Computers & Smartphones

Smart devices are a risk to any other device on a network because they are typically easier to breach, so hackers will use them as a gateway into more sensitive devices, like a work computer.

Improve Security by Putting IoT on a Separate Wi-Fi Network

Just about all modern routers will have the ability to set up a second Wi- Fi network, called a "guest network."

By putting all your IoT devices on a separate guest network from your devices that hold sensitive information, you eliminate that bridge that hackers use to go from an IoT device to another device on the same network.

Just make sure that you secure your Guest Network with a strong passphrase.

Need Help Upgrading Your Home Cybersecurity?

With so many remote workers, hackers have begun targeting home networks because they can target your sensitive business and personal data in a typically less secure environment than they would face in a business setting.

POPULAR SMISHING SCAMS TO WATCH OUT FOR

Smishing is a form of phishing that uses text messages (as opposed to emails) to trick unknowing recipients into clicking a malicious link or otherwise "mining" personal information through their replies.

They became a particularly popular method of attack during the COVID-19 pandemic and preyed on people's fear and easy spread of misinformation.

Some popular methods include:

- Text Messages Being Sent to You That Spoof Your Own Number
- Problem With a Delivery

GET MORE UNPLUGGED LAPTOP TIME WITH THESE BATTERY-SAVING HACKS

Laptops today boast ridiculously powerful batteries, a far-cry from the roughly 2-3 hours we used to get.. Most Apple laptops nowadays can easily provide up to 12 hours of batter life.
So, if you're laptop battery doesn't seem to get you past a few hours of use, try the following tips:

- Lower the Display Brightness
- Reduce PC Battery Use in Power/Sleep Settings
- Enable Battery-Saver Mode
- Use the Manufacturer's Battery

- Fake Appointment Scheduling
- Offer of a Free Gift
- Security issue with your account (often impersonates Netflix or Amazon)

Calibration Tool
- Disable Unnecessary Startup Apps in Task Manager on Windows 10/11
- Don’t Expose Your Laptop to Extreme Temperatures

5 WAYS MICROSOFT 365 CAN ENABLE THE HYBRID OFFICE

“Hybrid office” has become more than a buzzword. It is now the New Meeting Options for RSVP in Outlook reality for many companies.

63% of high-growth companies utilize a “productivity anywhere” hybrid work approach.

Here are some of the ways you can use Microsoft 365 to optimize a productive hybrid office:

Microsoft Teams & Expanded Features
- Webinar Registrations
- Full VoIP phone system

New Meeting Options for RSVP in Outlook
- RSVP in person or virtually

Better Framing for More Engaging Meetings
- The ability to adjust the room view to see faces more clearly.

Using PowerPoint to Present
- An upcoming technology called Cameo will integrate seamlessly with Teams and allow you to appear alongside your presentation.

Speaker Coach
- Personalized feedback on how to improve your presentations.