August 2022

TechTidbit.com

brought to you by Tech Experts

How Often Do You Need To Train Employees On Cybersecurity Awareness?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

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 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.

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 six 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 agents in your overall cybersecurity strategy, it's important they get training and refreshers regularly.

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
- Periodic simulated phishing tests
- Cybersecurity posters
- Celebrate Cybersecurity
- Awareness Month in October

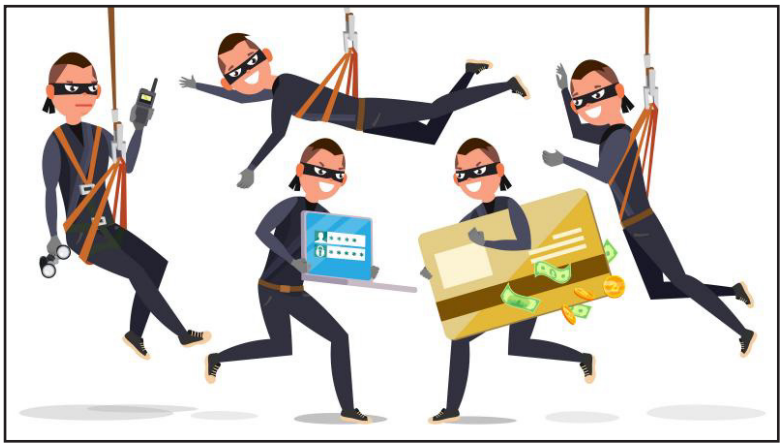
The gold standard for employee security awareness training is to develop a cybersecure culture. This is one where everyone is cognizant of the need to protect sensitive data, avoid phishing scams, and keep passwords secured.

The SLAM Method Can Improve Phishing Detection

"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"

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

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

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.

You can double-click on the sender's name to ensure the email address is legitimate.

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.

Look for words or phrases not normally used by the person who's emailing you. Words like "kindly" and "revert" are telltale clues the email come from someone who's not your normal sender.

Also, be on the lookout for pressure to act quickly or unexpected banking change requests. While it happens, it is rare for a company to change banks without months of advance notice.

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.

Watch Out For Reply-chain Phishing Attacks

Phishing. It seems you can't read an article on cybersecurity without it coming up. That's because phishing is still the number one delivery vehicle for cyberattacks.

80% of surveyed security professionals say that phishing campaigns have significantly increased post-pandemic.

Phishing not only continues to work, but it's also increasing in volume due to the move to remote teams.

Many employees are now working from home. They don't have the same network protections they had when working at the office.

One of the newest tactics is particularly hard to detect. It is the reply-chain phishing attack.

What is a Reply-Chain Phishing Attack?

You don't expect a phishing email tucked inside an ongoing email conversation between colleagues.

Most people are expecting phishing to come in as a new message, not a message included in an existing reply chain.

The reply-chain phishing attack is particularly insidious because it does exactly that. It inserts a convincing phishing email in the ongoing thread of an email reply chain.

How does a hacker gain access to the reply chain conversation? By hacking the email account of one of those people copied on the email chain. Often, the target isn't even aware.

The hacker can email from an email address that the other recipients recognize and trust. The attacker also gains the benefit of reading down through the chain of replies. This enables them to craft a response that looks like it fits.

They may see that everyone has been weighing in on a new idea for a product called Superbug. So, they send a reply that says, "I've drafted up some thoughts on the new Superbug product, here's a link to see them."

The reply won't seem like a phishing email at all. It will be convincing because:

1. It comes from an email address of a colleague. This address has already been participating in the email conversation.
2. It may sound natural and reference items in the discussion.
3. It may use personalization. The email can call others by the names the hacker has seen in the reply chain.

Business Email Compromise is Increasing

Business email compromise (BEC) is so common that it now has its own acronym. Weak and unsecured passwords lead to email breaches. So do data breaches that reveal databases full of user logins.

Tips for Addressing Reply-Chain Phishing

Here are some ways that you can lessen the risk of reply-chain phishing in your organization:

- Use a business password manager
- Put multi-factor controls on email accounts
- Teach employees to be aware

"They may see that everyone has been weighing in on a new idea for a product called Superbug. So, they send a reply that says, 'I've drafted up some thoughts on the new Superbug product, here's a link to see them.'"

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 besides 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 or a VPN connection to your office.

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.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Which Form Of MFA Is The Most Secure?

Credential theft is now at an all-time high and is responsible for more data breaches than any other type of attack.

With data and business processes now largely cloud-based, a user's password is the quickest and easiest way to conduct many different types of dangerous activities.

One of the best ways to protect your online accounts, data, and business operations is with multi-factor authentication (MFA).

It provides a significant barrier to cybercriminals even if they have a legitimate user credential to log in.

This is because they most likely will not have access to the device that receives the MFA code required to complete the authentication process.

What Are the Three Main Methods of MFA?

When you implement multi-factor authentication at your business, it's important to compare the three main methods of MFA and not just assume all methods are the same.

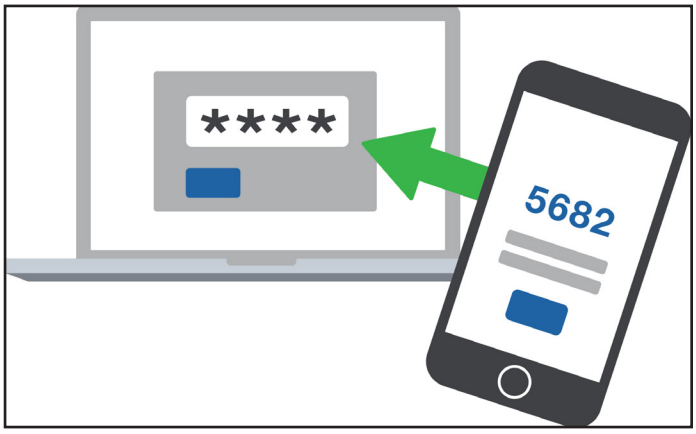
There are key differences that make some more secure than others and some more convenient. Let's take a look at what these three methods are:

SMS-based

The form of MFA that people are most familiar with is SMS-based.

This one uses text messaging to authenticate the user.

The user will typically enter their mobile number when setting up MFA. Then, whenever they log into their account, they will receive a text message with a time-sensitive code that must be entered.



On-Device Prompt In An App

Another type of multi-factor authentication will use a special app to push through the code. The user still generates the MFA code at log in, but rather than receiving the code via SMS, it's received through the app.

This is usually done via a push notification, and it can be used with a mobile app or desktop app in many cases.

Security Key

The third key method of MFA involves using a separate security key that you can insert into a PC or mobile device to authenticate the login.

The key itself is purchased at the time the MFA solution is set up and will be the thing that receives the authentication code and implements it automatically.

The MFA security key is typically smaller than a traditional thumb drive and must be carried by the user to authenticate when they log into a system.

Now, let's look at the differences between these three methods.

Most Convenient Form of MFA?

The most convenient form of MFA would be the SMS-based MFA. Most people are already used to getting text messages on their phones so there is no new interface to learn and no app to install.

The SMS-based is actually the least secure because there is malware out there now that can clone a SIM card, which would allow a hacker to get those MFA text messages.

Most Secure Form of MFA?

If your company handles sensitive data in a cloud platform then it may be in your best interest to go for better security.

The most secure form of MFA is the security key. The security key, being a separate device altogether, won't leave your accounts unprotected in the event of a mobile phone being lost or stolen. Both the SMS-based and app-based versions would leave your accounts at risk in this scenario.