Newsletter

Celebrating 32 years serving Central, N.C. March 2022

Importance of Security Awareness Training for Employees and C-Suite Executives

Many organizations continue to lose a lot of money due to data breaches. In addition, a 2021 Cyber Threat Report by SonicWall state, there is a 62% increase in Ransomware since 2019, and the attacks are expected to increase by 2025.

If you've never experienced cyber threats or attacks, it does not mean that you are safe. It is best to prevent cyber threats before it is too late. The first and most vital element to preventing cyber-attacks is training your employees. Employees are the backbone of your business, and teaching them about cyber security has many benefits for your organization. Read on to learn more about security awareness training.

What is Security Awareness Training?

Security awareness training educates employees on preventing cyber threats and attacks. It involves various methodologies to help employees know what to do and what not to do if they encounter cyber-attacks.

Why is Cybersecurity Awareness Important?

Helps Identify Phishing Attacks

Most data breaches occur because employees do not know how to avoid them. You can prevent this by training them on identifying and dealing with potential attacks. Training your employees on cyber security helps them easily identify phishing attacks in time. They will avoid clicking on malicious links that can compromise the integrity of your data. As a result, it minimizes and prevents data breaches, thus, enabling your organization to continue its operations smoothly.

Educates Employees About New Hacking Tricks

Scammers will always devise new ways to hack systems and manipulate data, making it challenging for many organizations to prevent cyber threats. In this case, it is best to consider continuous employee training to teach them about the latest tricks that scammers are using. Employees will learn the relevant new technologies, thus keeping systems, networks, and applications safe.

Training Protects Brand Reputation

Brand image is a vital element that you should always guard all the time. Training your employees will minimize cyber breaches that can affect your brand reputation and cost your business a lot of money in the long run. In addition, employees will learn their roles in

Upcoming Events

Lunch & Learn
What Every Business Owner Needs to Know to Protect Against Cyber Attacks
March 9, 2022

Webinar
Strengthening Your Security Foundation
April 6, 2022

For more information on our upcoming events, please visit www.tcsusa.com.

"Training" Continued

enhancing security, thus, protecting your brand reputation.

Fosters a Secure Culture

Building a solid and secure culture for your organization needs time, focus, and dedication through quality training. By training your employees on cyber security, you create an open environment where they will be comfortable sharing their security experiences. In addition, it helps your employees be open to asking questions and raising security concerns in time without the fear of facing any consequences and punishments.

Best Practices for Effective Security Awareness Training

Set Flexible Goals

The first element to creating an effective security awareness training program is setting your short-term and long-term goals. It is best to work with an experienced IT professional such as Total Computer Solutions to guide and advise you about creating goals for your training program.

Determine Where to Start

Before you embark on security awareness training, it is best to identify your employee strengths. If you have an existing security training program, analyze it and determine what to add or remove to make your training resourceful.

Ensure Full Participation of the Management and Employees

It is essential to follow up with each employee and ensure full participation. This will help you close all gaps that could cause cyber-attacks. Every employee should be part of the program from the beginning to the end and actively engage in the program. You may want to test them at the end of the training to determine their strengths. An experienced IT professional such as Total Computer Solutions can help you ensure every employee benefits from the training program.

Empower Your Employees with Effective Security Awareness Training

The security foundation you create for your employees will determine their impact in implementing various measures to prevent cyber-attacks. Therefore, it is best to create a layered security approach that includes security awareness training to help you achieve your goals. Signup for a free consultation to learn more about TCS' cybersecurity awareness training.

What to Do After Clicking a Disastrous Malicious Link

It is a Friday night. You are exhausted from the work week. The bed is calling your name, but you are on your laptop, opening emails from family, friends, and your favorite store is alerting you about its sale for the weekend. Suddenly you get a new email.

You rub your itchy, half-shut eyes, and open the email out of curiosity. Supposedly your bank is asking you to change your account's password. You click on the attached link, unaware that the bank is not even the one you use.

Your stomach drops, heat surges through your body. You are wide awake now. An unexpecting page uploads. Your screen reads: MALWARE detected on your computer, act now! You want to press okay, but your mind is telling you otherwise. What if this happened to you? Do you know what to do after accidently clicking a malicious link or a virus?

In today's world, you may face this scenario. Here are a few steps that you should be aware of in case you ever fall victim to a phishing email.

Step 1: Disconnect and Shut Down

First things first, never click 'okay' or 'continue.' This will automatically fill your computer with malware – causing you to lose precious files, downloads, apps, and more. Also, do not just click the 'X,' because if the malicious site uses a JavaScript, then it can still take control of your computer and download malware.

The best response is to hold the power button for 5-7 seconds to 'shut down,' and then unplug your network cable from your computer. When shutting down your computer, do not merely 'sign off' and do not press 'restart.' At this point, if you have an IT partner, call them to see when it is safe to turn your computer back on.

This is not a sure-fire way to stop the malware, but it is the best option that can prevent spreading the malware or virus to other devices.

Step 2: Run a Security Check

Make sure you run a security audit. After rebooting, you might be able to get onto the Internet completely fine, but a virus could have attached itself to your computer before you were able to shut it down. What you do not want to do is go on as if nothing happened, because later on, you might misunderstand why your computer is running slowly or why files are beginning to disappear.

"Link" Continued

If you are not familiar with how to run a check then call a professional for extra support.

Have the partner run a malware check or install an anti-malware that can keep you more secure. It may cost you money, but it will keep you or your business better protected and save you money in the long term.

Step 3: Backup Your Data

Small businesses should back up their data. If you have not, then do not panic, check your files – see if everything you need is there. Begin to backup your data through one of the many Cloud-based sites or install a portable backup device onto your computer.

Step 4: Update Your Passwords

Once you are confident that your machine is clear of malware, another important step is to change your credentials. If malware was found on your computer, or a hacker was able to weasel their way in, the last thing you want is for them to have access to all your private information. As always, create strong passwords and do not reuse passwords for other accounts. If there is ever a necessary time to create new and strong passwords, it is after you fall for a phishing scam.

Tips If Your Are Thinking About Clicking

Here are a few other important things to remember:

First, breaking news topics that become big are picked up by hackers because the story interests you. This also happens with popular videos and articles that seem benign at first. You should continuously be wary of flashy news because they often seem normal; at the top of a Google search list or shared through a social media site.

Secondly, if an unknown source sends the email and it seems urgent, you should be wary. Hackers tend to use urgency and fear of loss to make people click links. Just remember, if there is a major issue, then the sender will use various mediums to contact you, such as phone or by mail. So, next time an email asks you to take urgent action, just delete it and communicate with the source.

Third, always check at the bottom of your screen to see if the URL looks shortened or does not use https. Both of these are signs that something could be wrong.

It is easy to fall victim to a phishing email, a malicious link, or a video containing malware.

New Guide: Cybersecurity Tips for Employees

How do business owners keep their data secure?

Find out in our Cybersecurity Tips for Employees guide. The resources in this guide can go a long way in making sure sensitive information does not fall into the wrong hands.

Visit tcsusa.com/e-books/ to get your copy today!

tcs totalcomputersolutions
Cybersecurity Tips for Employees :
Educating Staff on Secure Online & Office Behavior

Ian Collins

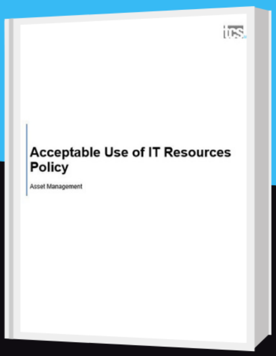
Information Security Manager

ASK A TECHIE

"What is NextGen Anti-virus?"

Next-Generation Antivirus is the next evolution in endpoint security that does not rely on signature databases like its predecessor. Instead, it leverages artificial intelligence-driven analytics and combines it with threat intelligence to prevent the execution of malicious programs and recognize attackers' tactics and techniques. This enables response to previously undetected threats.

ACCEPTABLE USE POLICY GUIDE



- ✓ Protecting Important Information and Resources
- ✓ Authorized Level of Access and Approved Tech
- ✓ Reporting Incidents and Weaknesses

DOWNLOAD THE GUIDE

www.tcsusa.com

tcs totalcomputersolutions

5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

LUNCH & LEARN: What Every Business Owner Needs to Know to Protect Against Cyber Attacks

Date: Wednesday, March 9th, 2022
Time: 12:00 PM - 1:30 PM
Location: Attend virtual or in-person at Total Computer Solutions
Speaker: Barry Utesch, President, Total Computer Solutions
Registration: Visit tcsusa.com/events/ or call 336.804.8449

Join TCS on Wednesday, March 9 at noon for an informative event with our President, Barry Utesch, as he discusses the cyber threats to your company data and concrete steps to immediately increase your organization's security.

Key Topics for Discussion

- Why Cyber Crime is Exploding
- How a Cyber Attack Affects a Small Business
- Cyber War Stories
- Things You Can Do Today

Lunch will be catered from Pastabilities and will be individually packaged. Seating at the event will be socially distanced. The event will be adhering to the Guilford County guidelines.