Newsletter

Celebrating 30 years serving Central, N.C. *March 2020*

What to do After Clicking a 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 up emails from family, friends, and your favorite store is alerting you about its sale for the weekend. All of a sudden 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 expecting page uploads. Your screen reads: MALWARE detects on your computer, take action. 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 clicking a malicious link or a virus?

In today's world, you may face this scenario. There are a few steps that you should be aware 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 don't 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. If you are not familiar with how to run a check then call a professional for extra support.

Upcoming Events

TCS Security Madness: Your Best Defense is a Good Offense
March 20, 2020

Webinar: Office 365: How to Fully Protect Your Data
April 2, 2020

Life in the Cloud: Security & Backups Panel Discussion
April 22, 2020

For more information on our upcoming events, please visit https://www.tcsusa.com/calendar/.

"Malicious Link," Continued

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 You Are Thinking About Clicking

There are a few other important things to remember:

- First, breaking news topics that become big are picked up by hackers because they the the story interests you. This also happens with popular videos and articles that seem benign at first. You should continuously be wary 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 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. If you need further assistance about what to do after clicking a malicious link, TCS can help as a partner with this ongoing and ever present IT problem.

5 Cybersecurity Trends You Should Know for 2020

From smartphones to the electrical grid to interference by foreign countries in elections, cybersecurity is on everyone's mind these days. Since you are reading this, you are likely looking to understand cybersecurity trends in 2020. Here are serveral examples that might aid you on your way.

Are you prepared to fight the expected increase in cybersecurity attacks? **Experts expect that there will be 3.5 million cybersecurity jobs unfilled by 2021.** That's an alarming statistic for companies looking to upgrade or fill IT staff positions. Businesses face attacks every day by cyber hackers trying to loot bank accounts, commit all types of fraud, and disrupt businesses with ransomware. Companies that do not have the necessary IT staff or third-party IT support may face the hundreds of millions of dollars in expected data breaches. The average data breach cost for U.S. businesses in 2019 was $8.19 million. Wholly automated cybersecurity protection decreases that amount significantly to $2.6 million. However, the pool of skilled, experienced cybersecurity personnel required to the effect that change will continue to shrink just as businesses ramp up.

IoT and data theft. The Internet of Things (IoT) has changed the world we live in. Data thieves rejoice at the many devices consumers have rushed to adopt, such as machine sensors, smartphones, Alexa, GPS devices, and various entertainment platforms. All of these represent data mills that provide cybercriminals a giant, lucrative playground. Unfortunately, security standards for IoT devices have not kept up with the IT expansion. Just imagine cyber hackers invading the cloud where consumers and businesses store sensitive personal information or hacking into Alexa, who has information about the household she serves. Add to that the growing concerns about self-driving cars, and it becomes apparent that data processed and stored in the U.S. is at a critical juncture.

Experts expect ransomware to shift to smaller targets. In recent years, ransomware attacks have focused on big banks because of the multi-million-dollar payoffs. Experts now believe that cybercriminals will "go small" in 2020 for purely economic reasons. Smaller profile attacks are easier to plan and execute with fewer helping hands and more significant profits.

Follow us on social media!

"Cybersecurity Trends," Continued

With this in mind, **beefing up IT staff with experienced cybersecurity professionals is a priority for small-to-midsize businesses in 2020.**

As software goes, so goes the digital world. **Telecom companies are just one example of businesses expected to become more dependent on software run from the cloud.** In practical terms, that trend means that software security code inspection must begin at the creation/development of an app and be part of every phase until production. Savvy businesses will keep abreast of this "pipeline code" movement to ensure that the software they buy and the cloud services they employ are onboard with this security model.

What about the safety of the trucking industry pipeline? A trucking network consists of computers in the cabs of trucks that keep drivers on the road in touch with dispatchers. Trucking logistics depends on sophisticated software programs that, in turn, rely on computer networks that run with little downtime. Experts have accumulated evidence that malicious actors have their sights on carrying out direct attacks on the trucking industry. In October 2019, cybersecurity experts speaking at the American Trucking Association's Management Conference and Exhibition told attendees that the trucking industry is now the number five most ransomware attacked industry in the U.S. Small trucking companies are the biggest targets for cyber hackers, and this industry sector does not yet have sophisticated protections on their computer networks, and hackers believe they are likely to pay the ransom. Large trucking companies are targets, too, because they can afford to pay more substantial blackmail fees. Unpaid ransomware attacks can shut down entire trucking lines and even infect the trucking company's customer relations management software. Once hackers find a soft target, they will attack repeatedly. All of this has created a lucrative field for cybercriminals. If it's true that consumers drive digital transformation, then businesses need to demand more cybersecurity expertise from their transportation partners.

Cybersecurity issues continue to increase at a rapid pace. Most companies possess unprotected data and exhibit poor cybersecurity practices. Both conditions mean most companies remain vulnerable to cyberattacks and data loss. The reasons that companies remain largely unprepared is because they have not yet caught up with this new type of crucial behavior.

If you would like to receive our newsletter digitally, please email alimbers@tcsusa.com.

Meet Our Team: Bill Gwaltney

Please join us in welcoming our new Analyst, Bill Gwaltney to the TCS team. He is a graduate of UNC-G and is also a Staff Sergeant in the United States Air Force Reserves. Bill is from Madison, North Carolina, and enjoys golfing.

FREE Guide: Protect Your Company from Phishing Attacks

Computer network security is no longer just the responsibility of the IT department instead it is a company-wide effort that requires buy-in from the entire organization. While the news plays up data breaches of large national corporations, it's worth noting a few statistics that point to the truth because any size company is vulnerable. Throughout this guide, we will share how to train your team to spot phishing email, ways to protect your company with a multi-layered security approach and how you can avoid downtime, data loss, and reputation damage.

Get your FREE copy today!
Visit tcsusa.com/resources/e-books/

TCS Tech Tips | Search

Watch our new TCS Tech Tip videos! Visit tcsusa.com and click on our resources tab to find tips and tricks to help keep you more productive.

5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

What to do After Clicking a Malicious Link

5 Cybersecurity Trends You Should Know for 2020

Meet Our Team

Protect Your Company from Phishing Attacks

TCS Security Madness

Upcoming Events

TCS Security Madness

Join us for an afternoon of watching the NCAA Tournament, and game planning for Cybersecurity!

Date: Friday, March 20th
Time: 11:00 AM - 2:30 PM
Location: Kickback Jack's, 1605 Highwoods Blvd, Greensboro, NC 27410
Presenter: Andy Purcell, *Business Development, Total Computer Solutions*
Cost: Free
Registration: Visit tcsusa.com/calendar/ or call us at 336.804.8449

Nearly half of cyberattacks target small to medium size businesses. About 60% of those companies are out of business within 6 months of the attack. For businesses, the average cost of an attack is $133,000.

At this event, we will present valuable information on how to create your Cybersecurity game plan.

Key Topics for Discussion:

- What is your exposure?
- How do cybercriminals steal information?
- When to play offense against the risk of data breaches?