1991 – 2021
30
YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

May 2023

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

The Hidden Threat: What Is The Man-In-The-Middle?

How many cyberattacks has your Security Awareness Training taught you to identify? It's not always about recognizing suspicious activity on the network or learning how to flag phishing messages. Some cyber-threats lay in wait for you to wander into their trap, and before you realize it, you've personally spilled your private information to a bad actor.

A very common way that this plays out in the real world is through what's called a **man-in-the-middle attack (MitM)**.

What are MitM Attacks?

By infiltrating a trusted, legitimate website, cybercriminals are able to "eavesdrop" on your activity there. That way, *you* enter your own log-in credentials like you've done so many times before – not knowing that this time, someone else is looking in on everything you type. These are called man-in-the-middle attacks because they are positioning themselves between you and the server or site you're trying to access. There are 7 types of MitM attacks.

1. **DNS Spoofing**. Domain Name System is what translates unique IP addresses from number sequences to memorizable names, i.e. Google instead of 0123456789. By spoofing DNS, attackers can redirect traffic to their fake website set up to steal your data.
2. **HTTPS Spoofing.** Before a website's URL, you'll notice the letters HTTP or HTTPS. The *S* means that the site is *Secure*; but with this kind of man-in-the-middle attack, hackers convince your browser that an unsafe site is HTTPS-certified when it isn't.

Continued on pg.2

Continued from pg.1

3. **IP Spoofing.** When you connect to the Internet, you're assigned an internet protocol (IP) address that connects your device to its geolocation. By spoofing their IP, cybercriminals pretend to be a reliable website so that you're more likely to divulge private information to them.
4. **Email Hijacking.** Instead of targeting *you*, the hacker first goes after the emails of a legitimate business, like your bank. Then they can read and copy the language of their usual customer messages, so their spoofed domain name can more effectively trick you into sending money or information.
5. **SSL Hijacking**. Secure Sockets Layers encrypts your connection to a secure HTTPS webpage. When cybercriminals spy on your interactions with the server, they hijack the SSL – hence the name.
6. **WiFi Eavesdropping.** People connect to random WiFi networks all the time when they need to look something up on the go. When users connect to fake WiFis set up by cybercriminals, they can monitor ALL of your online activity until you disconnect, this includes your usernames, password and anything else you are typing.
7. **Browser Cookie Theft.** By accessing the data in your stored Cookies, hackers can discover any passwords and other private information you might have saved to autofill! The safest thing to do is NEVER save your login information in your internet browser.

Where Am I Most Likely to Find MitM Threats?

Financial sites are most likely to become compromised by a man-in-the-middle attack, because those credentials are the most direct way into your bank accounts. From there, cybercriminals can transfer funds freely to their own offshore accounts or even use that information to affect your credit and steal your identity.

However, that does not mean that your favorite banking app is the only possible place for an invisible trap to lay in wait. Any site that requires you to log in may be a target for MitM threat actors who want your account information.

How to Avoid MitM Attacks

Multifactor authentication is the best defense for your accounts. Even if a hacker acquires your username and password, they will also have to have a secondary form of identification to get into your profile. Meanwhile, you receive an alert about unauthorized attempts to log in and you can take action to change your credentials.

Encrypted communication and virtual private networks (VPNs) are also used to hide online activity from trackers. In the meantime, be careful what public networks you use and where you go online (such as banking sites) so you don't accidentally hand over your log in credentials to an invisible observer.

Conclusion

Man-in-the-middle attacks pose a unique danger compared to most cyber-threats you may have been warned about. The hacker lays a trap and waits for people to walk into it, like a spider and its web, instead of reaching out to you first. That ensures added trust which makes you more likely to hand over delicate data without blinking an eye.

Free Cyber Risk Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber risk audit to uncover any loopholes that may exist in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these risk problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are exposed to various threats in a number of areas.

Claim Your FREE Assessment Today At:

https://www.cti-mi.com/cyber-security-audit-523/

Or Call Our Office At: 248-362-3800

Security Corner

Keylogging: What Is It And What You Need To Know

What if threat actors could see everything that you did online? Everything you searched, every message you sent, every password you entered? If your device is infected with the right software, then this nightmare can become all too real!

What You Need to Know About Keyloggers
From DMs to your search history, they can spy on it all. By recording your information and then storing it on a remote computer, keyloggers can find your login info to all sorts of private sites this way.

Protecting Your Devices from Keylogging
The good news is, we are not defenseless against malicious keylogging! Antivirus software and continuous monitoring services can help weed out intruders on your network and purge malware from the system. **Multi-factor authentication** can also help here. Even if a threat actor were to steal your log-in and password, they wouldn't be able to access your one-time code, fingerprint or whatever other form of secondary identification you use to log in.

Conclusion
Keylogging software may be harder to spot because it does not necessarily cause suspicious behavior on your device. As scary as this sounds, *you are not defenseless!* Continuous monitoring from your IT provider and smart software can go a long way toward protecting your network and all your data.

For more information about phone theft and other cyber threats, call us at 248-362-3800 or visit: https://bit.ly/3HpV3w7

What Is App Fatigue & Why Is It An Issue?

The number of apps and web tools that employees use on a regular basis continues to increase. Most departments have about 40-60 different digital tools that they use. 71% of employees feel they use so many apps that it makes their work more complex.

Many of the apps that we use every day have various alerts. We get a notification popup that an update is available. We get an alert of errors or security issues.

App fatigue is a very real thing and it's becoming a cybersecurity problem. The more people get overwhelmed by notifications, the more likely they are to ignore them.

Just think about the various digital alerts that you get. They come in:

- Software apps on your computer
- Mobile apps and tools
- Email banners
- Text messages

Some employees are getting the same notification on two different devices. This just adds to the problem and leads to many of the issues that impact productivity and cybersecurity.

Besides alert bombardment, every time the boss introduces a new app, that means a new password. Employees are already juggling about 191 passwords. They use at least 154 of them during the month.

How Does App Fatigue Put Companies at Risk?

Employees Begin Ignoring Updates
When digital alerts interrupt your work, you can feel like you're always behind. This leads to ignoring small tasks seen as not time-sensitive. Tasks like clicking to install an app update.

Employees overwhelmed with too many app alerts, tend to ignore them. When updates come up, they may quickly click them away. They feel they can't spare the time right now.

Ignoring app updates on a device is also dangerous.

Many of those updates include important security patches. When they're not installed, the device and its network are at a higher risk.

Employees Reuse Passwords (and They're Often Weak)
Another security casualty of app fatigue is password security. The more accounts someone must create, the more likely they are to reuse passwords. It's estimated that passwords are typically reused 64% of the time.

Credential breach is a key driver of cloud data breaches. Hackers can easily crack weak passwords. The same password used several times leaves many accounts at risk.

Employees May Turn Off Alerts
Some alerts are okay to turn off. For example, do you really need to know every time someone responds to a group thread?

But, turning off important security alerts is not good. There comes a breaking point when one more security notification can push someone over the edge.

What's the Answer to App Fatigue?
You can put a strategy in place that puts people in charge of their tech, and not the other way around.

- Streamline Your Business Applications
- Have Your IT Team Set up Notifications
- Automate Application Updates
- Open a Two-Way Communication About Alerts

These Everyday Objects Can Lead To Identity Theft

You wouldn't think a child's toy could lead to a breach of your personal data. But this happens all the time.

Many everyday objects can lead to identity theft:

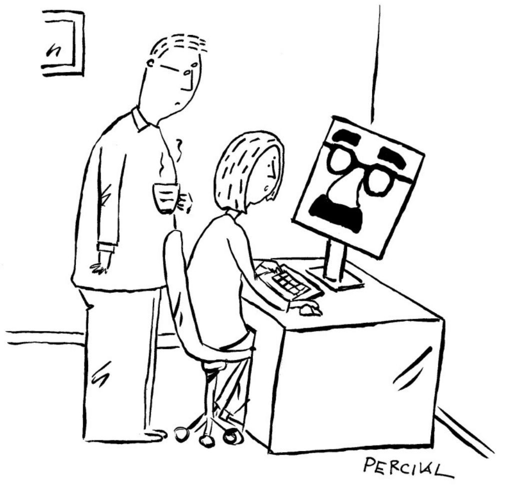
Old Smart Phones
A cybercriminal could easily strike data theft gold by finding an old smartphone. Make sure that you properly clean any old phones by erasing all data.

USB Sticks
You should never plug a USB device of unknown origin into your computer. This is an old trick in the hacker's book. They plant malware on these sticks and then leave them laying around as bait.

Old Hard Drives
When you are disposing of an old computer or old removable drive, make sure it's clean. Just deleting your files isn't enough. It's best to get help from an IT professional to properly erase your computer drive. This will make it safe for disposal, donation, or reuse.

Trash Can
Identity theft criminals aren't only online. They can also be trolling the neighborhood on trash day. Be careful what you throw out in your trash.

Children's IoT Devices
You should be wary of any new internet-connected kids' devices you bring into your home. Change the default username and password and install all firmware updates and do your homework.



"The computer's acting funny."

CartoonStock.com

6 Things You Should Do To Handle Data Privacy Updates

Once data began going digital, authorities realized a need to protect it. Many organizations have one or more data privacy policies they need to meet.

Industry and international data privacy regulations are just the tip of the iceberg. Here are a few things you should look into to handle data privacy updates:

1. Identify the Regulations You Need to Follow
2. Stay Aware of Data Privacy Regulation Updates
3. Do an Annual Review of Your Data Security Standards
4. Audit Your Security Policies and Procedures
5. Update Your Technical, Physical & Administrative Safeguards As Needed
6. Keep Employees Trained on Compliance and Data Privacy