# Talk Nerdy To Me



# 7 Spooky Scam Calls

In the age where text rules, almost any phone call could be deemed “spooky” – especially the ones from unknown numbers. Keep an unnerved eye out for some of the scariest scams going around to keep you from getting creeped out!

1. Are you afraid of the dark?
Some scammers like to pose as utility companies and threaten to shut off your lights. As scary as it would be to lose electricity on Halloween, most utility companies will send word of your impending doom via mail before they try to contact you by phone (if ever at all). If you’re not sure, hang up and call the electricity company directly.

2. Things that go *ring* in the night.
Did you know that telemarketers have quiet hours? That’s right – they’re not supposed to call before 8 a.m. or after 9 p.m. YOUR time. Scam callers don’t follow the rules, but if you get what you believe is a legitimate sales, charity or promotional call after hours, you can report it to the FTC. Sweet dreams!

3. The disappearing money trick.
Scammers have lots of ways to grab your cash, but one of the most famous is asking you to pay “fees” or “taxes” on prizes you have won. Once the money is gone, so are the scammers…and you’ll be left high and dry without that free cruise. Bummer.

4. Is this your card?
Paying your dues with an iTunes card? It’s not magic – it’s a scam. If anyone calls and demands payment via a gift card, they’re just looking to get away without a trace. Legitimate businesses want legitimate money – period.

5. Fear Factor.
Scammers rely on two things to get you to cave: rushing you into a decision and playing into your fears. They may pretend to be a grandson in trouble and needing bail, or a medical official requiring authorization (aka, social security numbers!) to operate on a family member. Don’t be fooled by these tactics!

6. The calls are coming from the inside of the house!
There’s nothing more intriguing than being called from your own number! Scammers know you’re more likely to pick up an unknown call from an eerily similar number – or even your own. Don’t let curiosity get the cat, though. They’re just spoofing lookalike numbers to try and catch your attention.

7. Mummy’s the Word.
Like we mentioned earlier, scammers love to scare you silly. Some call posing as IRS agents, threatening to lock you away if you don’t pay your taxes (with iTunes gift cards, of course). They’ll even say they’ll report you to the police if you ask to put them on hold or tell them you’re going to call someone else! The real IRS is not a bunch of mobsters – and they like to make first contact by mail, FYI.

*Source: https://firstorion.com/7-spooky-scam-calls/#*

# Cyber Lessons: Arm Yourself With Knowledge To Stay Ahead Of The Game

**Multi-Factor Authentication - Double your login protection.**
No matter how long and strong your password is, a breach is always possible. All it takes is for just one of your accounts to be hacked, and your personal information and other accounts can become accessible to cyber criminals.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. This way, even if cyber criminals guess your password, they're still out of luck!

**Wi-Fi Safety - Stay protected while connected.**
The bottom line is that whenever you're online, you're vulnerable. If devices on your network are compromised for any reason, or if hackers break through an encrypted firewall, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi.

Practice safe web surfing wherever you are by checking for the "green lock" or padlock icon in your browser bar—this signifies a secure connection. When you find yourself out in the great "wild Wi-Fi West," avoid free internet access with no encryption. If you do use an unsecured public access point, practice good internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi.

**App Security - Keep tabs on your apps.**
Have you noticed that apps you recently downloaded are asking for permission to access your device's microphone, camera, contacts, photos, or other features? Or that an app you rarely use is draining your battery life?

Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Don't give your apps an all-access pass. The following are some steps to avoid "over-privileged" apps:

Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted sources.

**Oversharing and Geotagging - Never click and tell.**
Everyone seems to be posting their information on social media—from personal addresses to where they like to grab coffee. You may figure, if everyone's doing it, why can't I?

What many people don't realize is that these seemingly random details are all criminals need to know to target you, your loved ones, and even your physical belongings online and in the real world. Avoid posting names, phone numbers, addresses, school and work locations, and other sensitive information (whether it's in the text or in the photo you took). Disable geotagging, which allows anyone to see where you are—and where you aren't—at any given time.

**Phishing - Play hard to get with strangers.**
Cyber criminals cast wide nets with phishing tactics, hoping to drag in victims. Seemingly real emails from known institutions or personal contacts may ask for financial or personal information.

Cyber criminals will often offer a financial reward, threaten you if you don't engage, or claim that someone is in need of help. Don't fall for it! Keep your personal information as private as possible. If they have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.

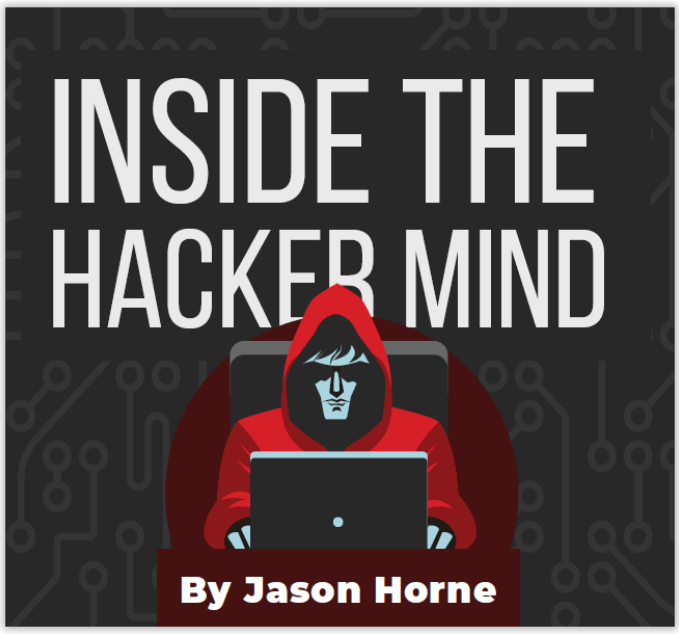
If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments found in that email. Always avoid sending sensitive information via email.

**Passwords - Shake up your password protocol.**
Gone are the days when you needed to come up with a frustrating mixture of letters, numbers, and symbols. According to NIST guidance, you should consider using the longest password or passphrase permissible. NCCIC guidance suggests 16-64 characters. Some sites even allow for spaces. Easy-peasy!

It's important to mix things up—get creative with easy-to-remember ways to customize your standard password for different sites. Having different passwords for various accounts can help prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Always keep your passwords on the down-low. Every time you share or reuse a password, it chips away at your security by opening up more avenues in which it could be misused or stolen.

*Source: https://www.dhs.gov/*

# Our CEO Is A Published Author




Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

# Socktober Is Here!

**Help make this a warmer winter for our neighbors in need! We are collecting NEW socks of all colors, sizes, and patterns the whole month of October and donating them to the Fort Wayne Community Schools Clothing Bank.**

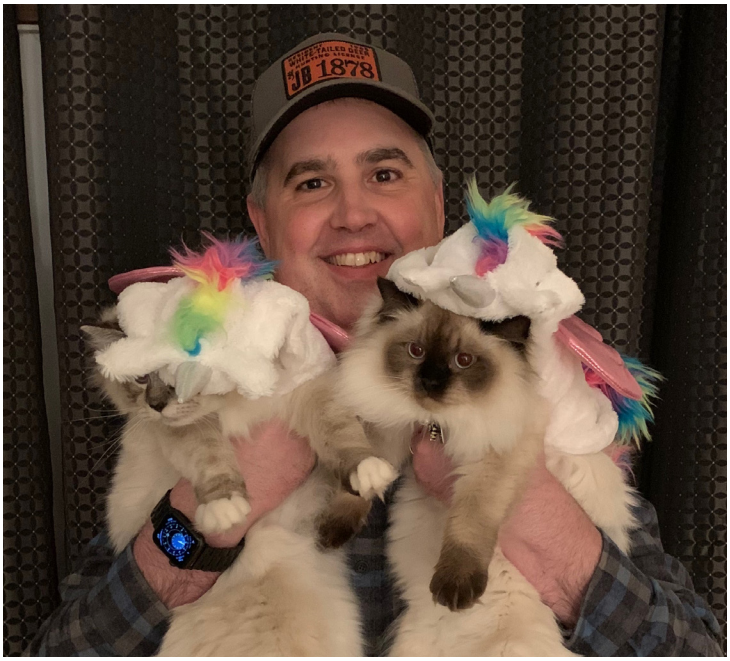
**Socks are the most needed and least donated articles of clothing given, so help us do our part for the community.**

**We need socks for men, women, and kids! If you would like to do a little more we are also accepting hats, gloves, and scarves!**

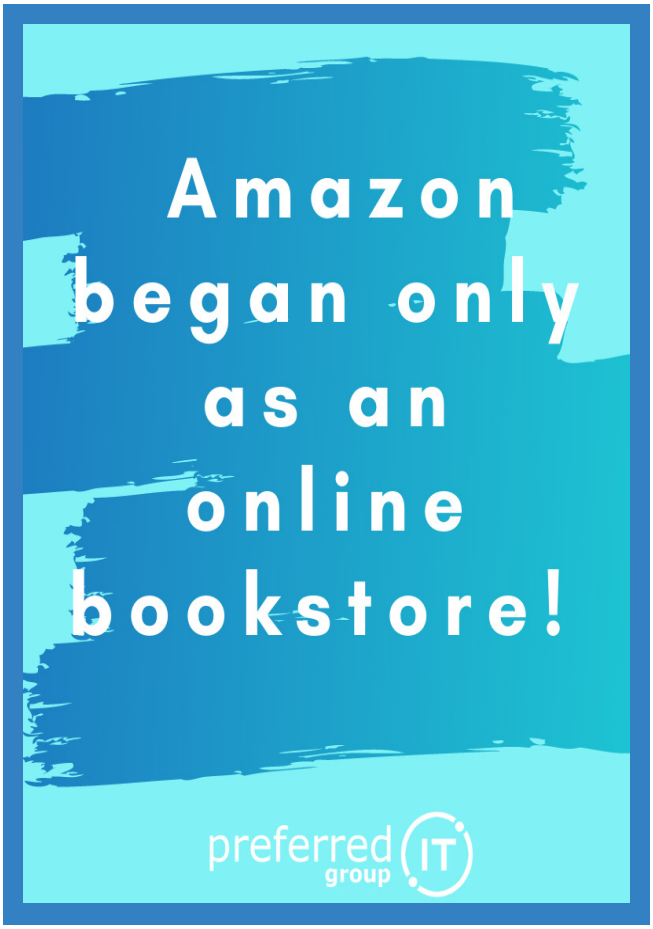
# Three Cheers For 7 Years!

***Happy 7 Years with Preferred IT Group!***

***Thank you for all that you do!***



FUN FACT!




preferred IT group

## CONTACT US

Fort Wayne
260.440.7377

Warsaw
574.306.4288

Columbia City
260.213.4266

Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.