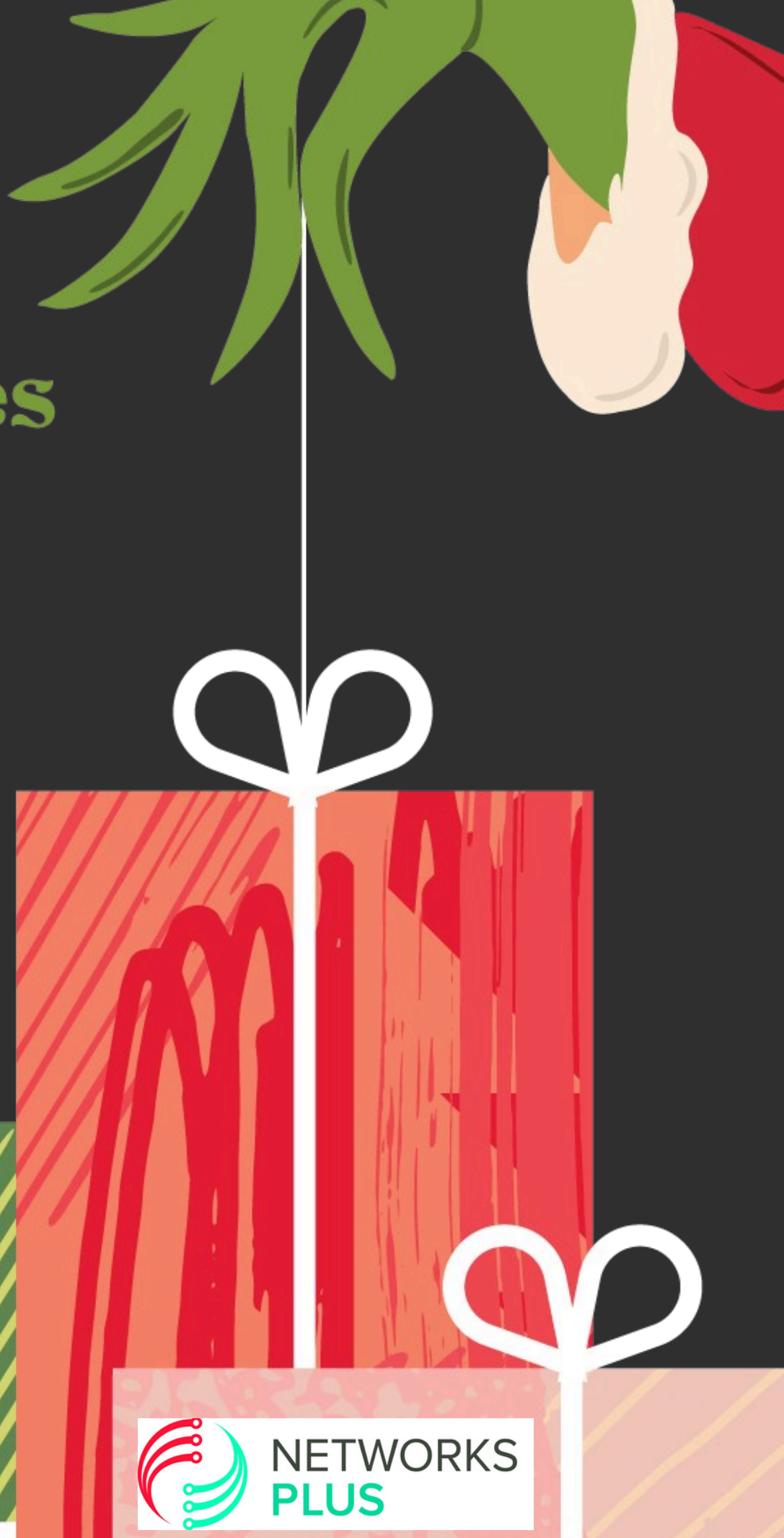
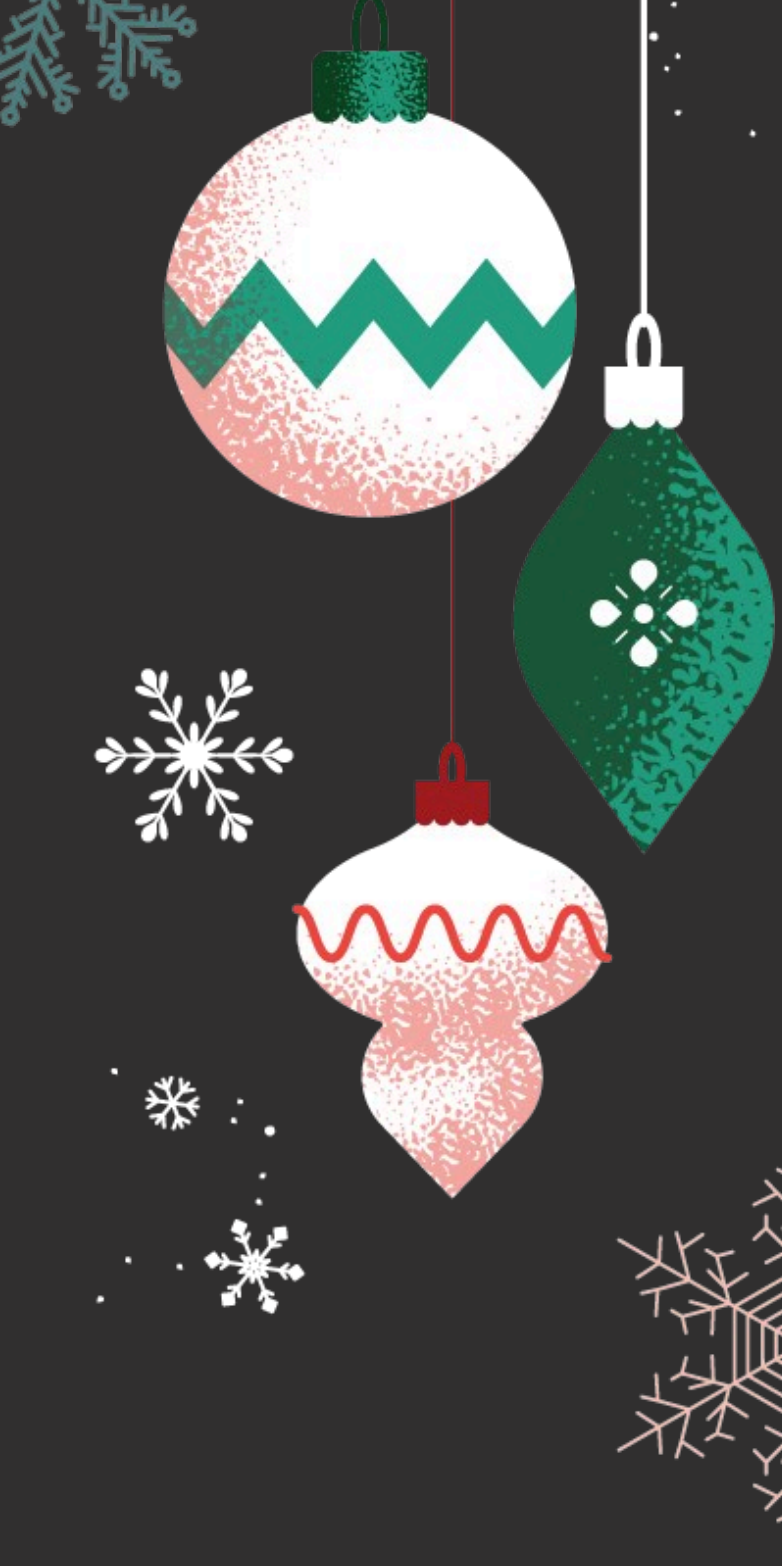
Don't Let Cyber Grinches Steal Your Holiday Joy!

12 Tips to Follow



NETWORKS PLUS

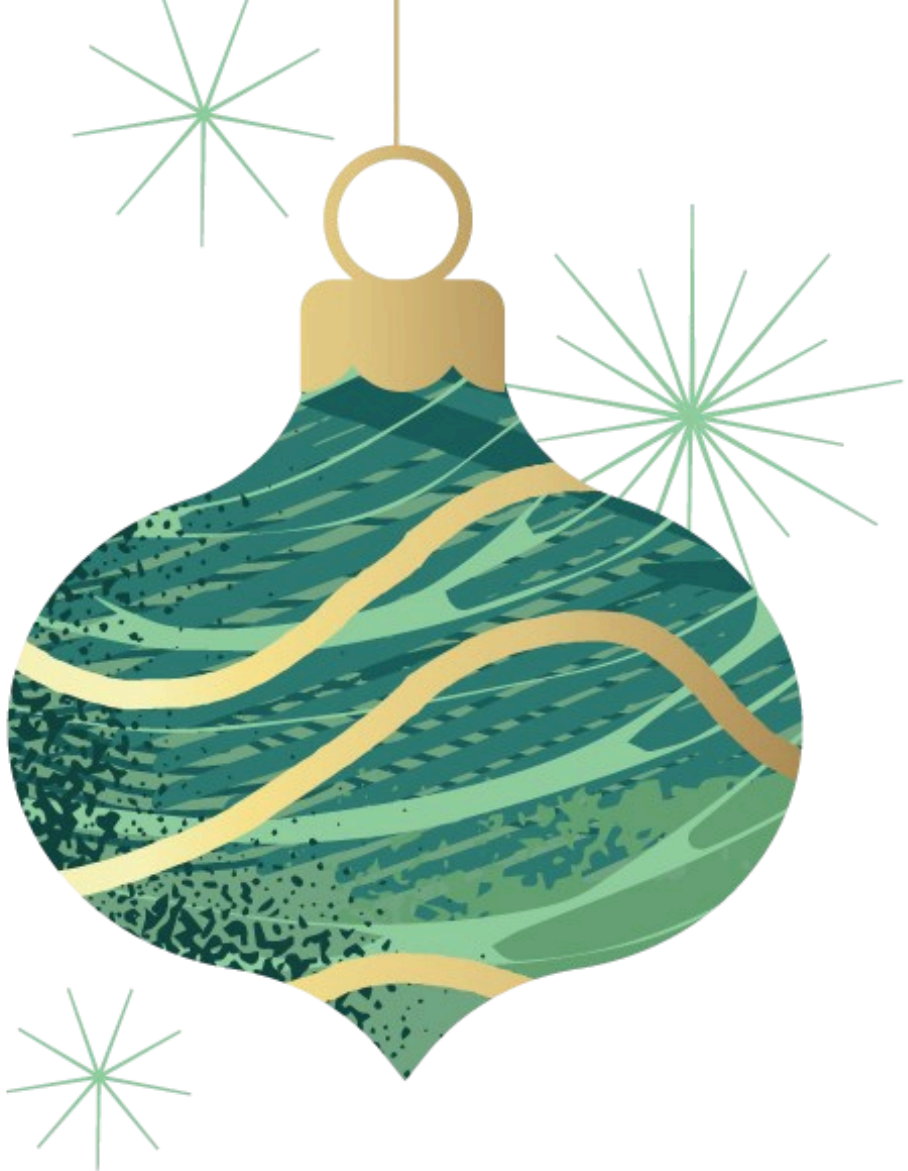


Protect Your Business from Holiday Cyber Grinches

While the holiday season brings joy, it also invites cybercriminals eager to exploit holiday distractions. Ransomware, phishing, and other threats often peak during this busy time, making it essential for businesses to be vigilant.

This guide offers 12 essential tips to help you strengthen your defenses and keep the holiday season cyber-grinch-free.

https://networksplus.com
consulting@networksplus.com 800.299.1704



Deck the Halls with Stronger Firewalls

1

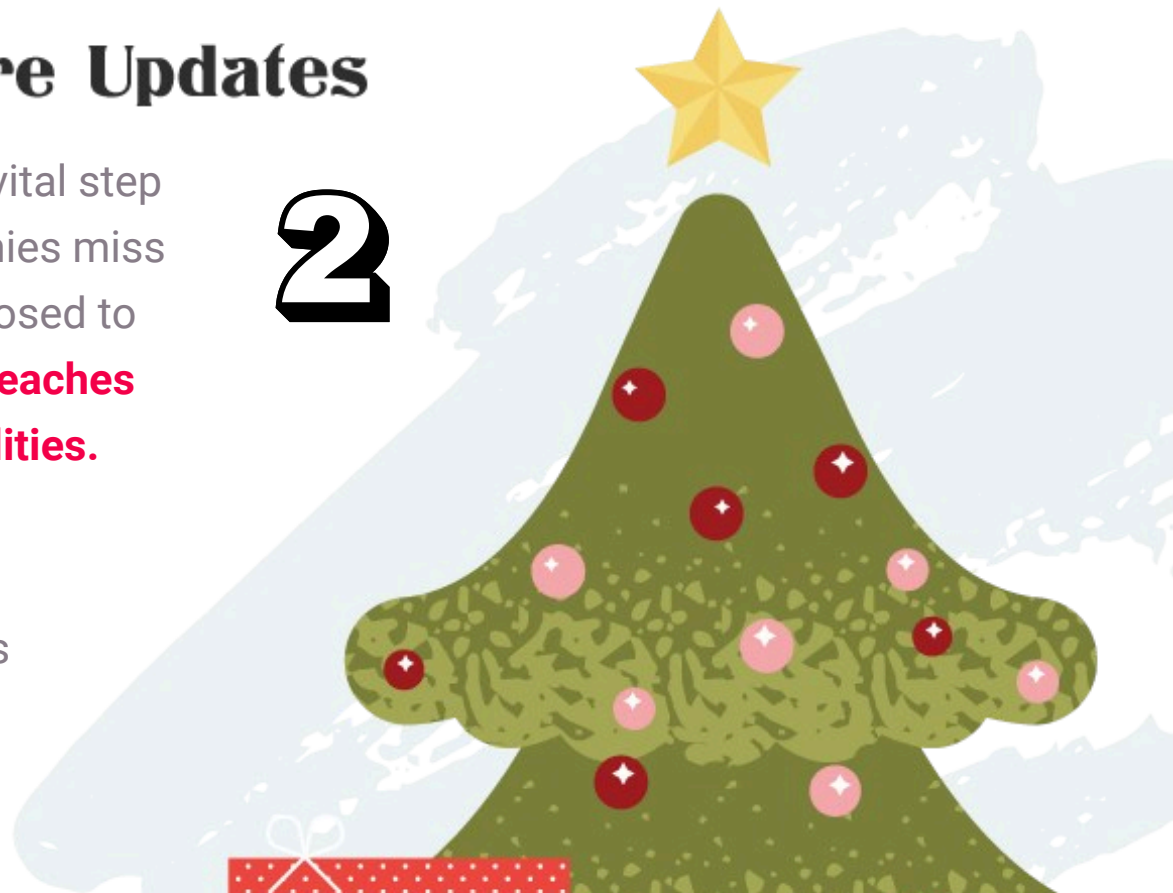
A strong firewall is your first line of defense against malicious traffic. Cybercriminals ramp up their efforts during high-traffic seasons like the holidays, so reinforce your network with firewalls that offer advanced intrusion detection. A report from Forbes notes that **43% of small businesses fall victim to attacks due to weak firewalls.** (Forbes)

“Unwrap” New Software Updates

2

Keeping software updated is a simple yet vital step to protecting your business. Many companies miss critical patches, leaving vulnerabilities exposed to cyberattacks. Studies show that **60% of breaches result from unpatched software vulnerabilities.** (AutoMox)

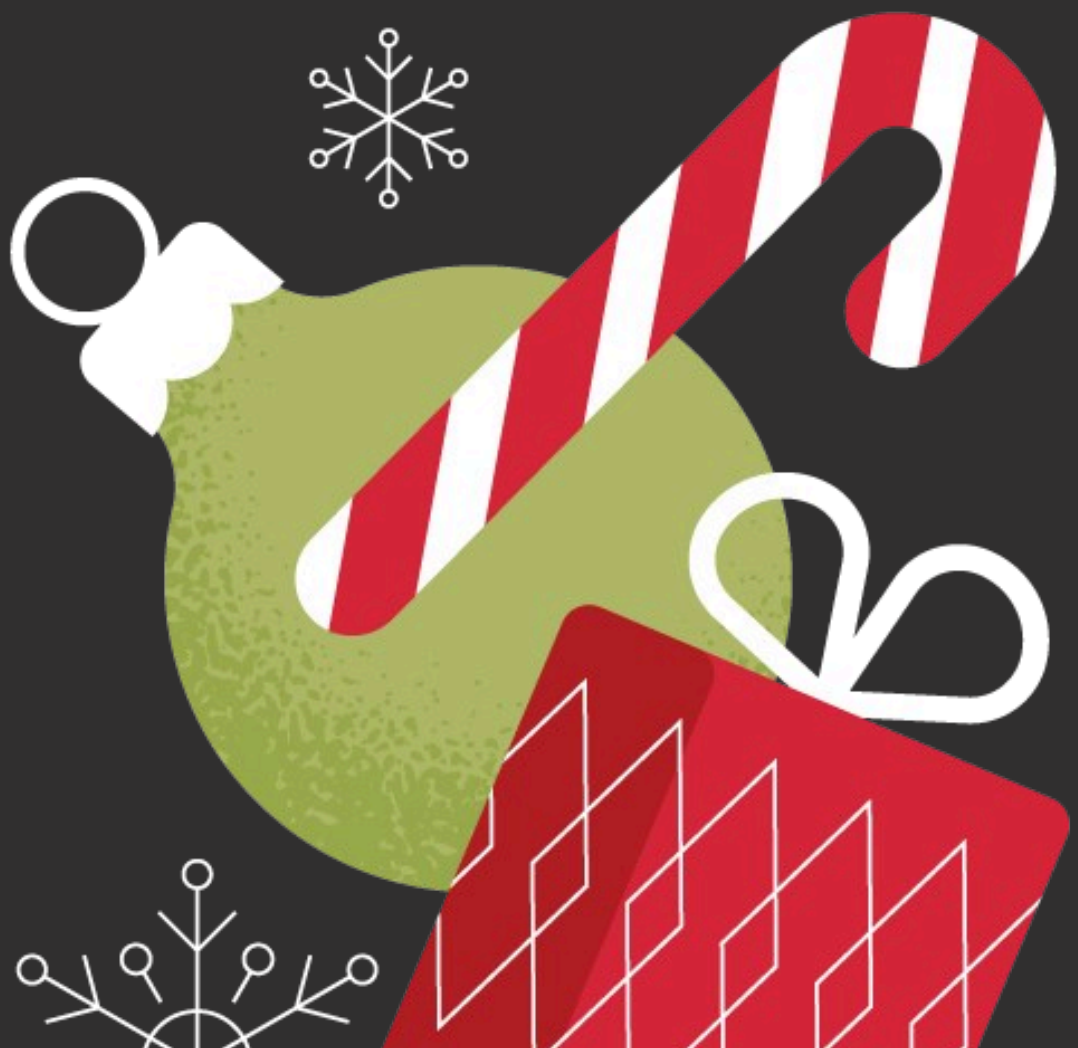
By regularly updating software, businesses can close gaps and fend off potential threats.



3 MFA is Twice as Nice

Multi-factor authentication (MFA) adds an extra layer of security to online accounts, helping prevent unauthorized access. With **phishing attacks increasing by 150% during the holidays,** according to studies (Check Point), enabling MFA is an easy and effective step to reduce the risk of compromised accounts.

"Wrap Up"



4 Data Backups Before the Holiday Break

Data backups are essential, especially during the holiday season when businesses may be operating with reduced teams. A recent study found that **businesses with consistent data backup practices recover over 97% faster from cyber incidents** than regular backups and store them securely offsite or in the cloud. (Invenio IT)

5 Avoid "Too-Good-To-Be-True" Emails

Phishing emails spike during holiday shopping seasons, using enticing offers or holiday greetings to lure unsuspecting suspects. According to Cybersecurity Ventures, **phishing costs businesses $17,700 every minute.** Educate your teams on identifying suspicious emails and encourage caution with unsolicited links or attachments as a cautionary preventative measure.

From fake promotions to charitable donation requests and package delivery issues, scammers will go to great lengths to convince their targets to click their link.

6 Beware of Social Engineering

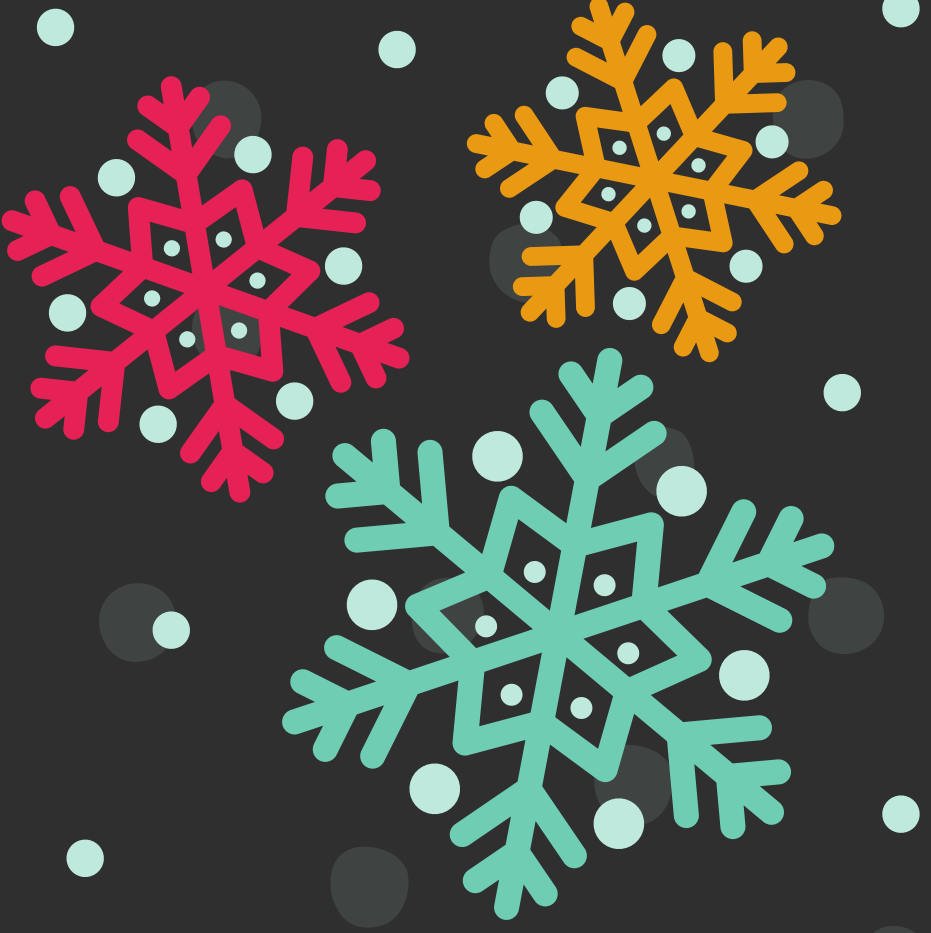
Social engineers are patient creatures. They sit back and study your email and communication patterns - analyzing your writing style, the people you interact with, and the frequency and timing of your activities, such as billing or invoicing. Once these grinches have collected everything they need, they will begin sending correspondence to your contacts disguised as you. Tricking your contacts into paying them, instead of you, is all part of their game.

Partnering with Networks Plus can help you monitor and watch for signs of these pesky creatures and slam the door in the faces before it's too late. **Be vigilant and don't let them steal your holiday cheer!**

7 Power in Strong Passwords & Passphrases

Weak or easy-to-guess passwords make you an easy target for hackers. By creating long, challenging, unique passwords or passphrases, you add an extra layer of security to your accounts.

All passwords and passphrases should include letters, numbers, special characters, as well as a combination of upper- and lower-case letters. Storing your credentials with a password manager is also highly recommended.



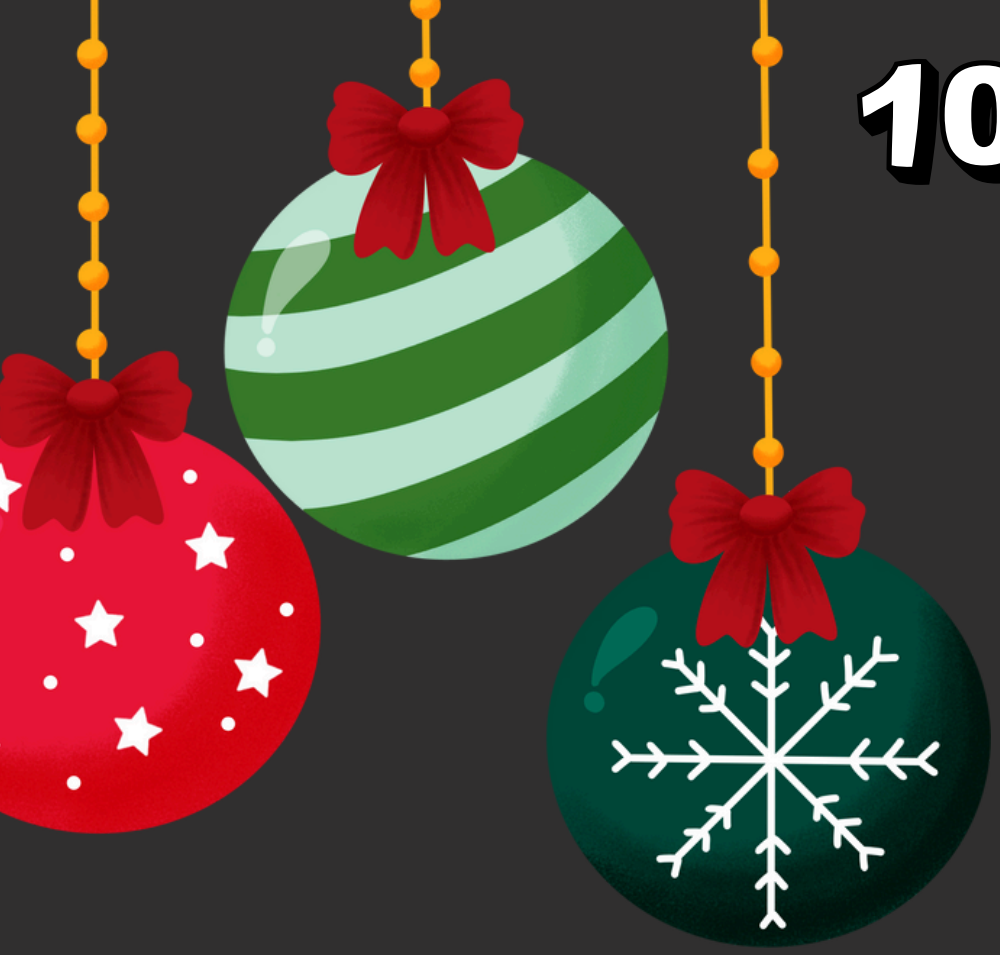
8 Watch Out on Public WiFi

Most everyone can appreciate free WiFi when it's offered at airports, hotels, restaurants, and other public places. However, these networks are often unsecured which can pose many risks to your devices and data. Should you choose to use free public WiFi, avoid entering sensitive information, such as login credentials or payment details, while connected.

If you must, we recommend using a Virtual Private Network (VPN) which can help encrypt your online activity and ensure safer browsing, even on public connections.

9 Secure Smart Devices

This holiday season will likely bring new gadgets into your home or office. If you are adding any new smart devices to your network, make sure to assign unique passwords to each of them. It's easy to overlook smart TVs, baby monitors, air purifiers, and video doorbells as threats, but if they are connected to your WiFi, they can provide a gateway into your network for hackers.



10 Check Financial Statements - Then Check Them Twice

Unauthorized charges on a bank statement might seem like an easy thing to spot. However, personal and professional spending tends to increase during the holiday season. Oftentimes orders placed online won't always match from the website to your statement. This can make catching mistakes difficult. While it's always best practice to monitor your financial accounts regularly, having someone watch extra closely for unauthorized transactions or unusual activity during the holidays is wise. **Many financial institutions allow you to set up alerts for any changes to your account so you can catch issues quickly**. Be sure to report any discrepancies to your bank promptly to help mitigate potential damage.

11 Don't be too Social on Social Media

Be diligent when making posts online. Double-check that your settings are not set to public view. Avoid sharing extremely detailed travel plans, pictures of expensive gifts, or any pictures that might show credit card numbers, bank statements, or other personal information. The more information you share, the easier you make it for social engineers to steal your identity.

12 Shop Trusted Websites Only

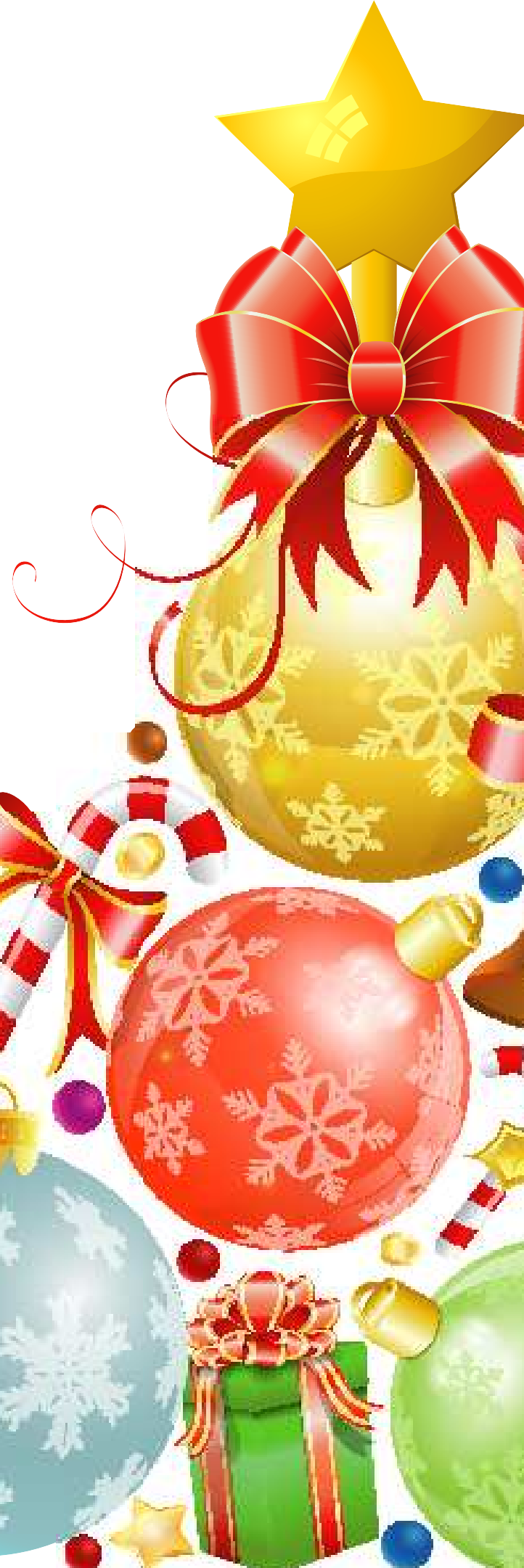
While online shopping is convenient, it does come with some risks. Eager shoppers may get ‘click happy’ and not realize they have entered a fake site. It is always recommended to choose reputable retailers. **You can ensure their websites are secure by checking for "https://" in the URL.**

Everyone loves a “good sale” but deals that seem too-good-to-be-true probably are. Additionally, using secure payment methods such as credit cards or platforms like PayPal can provide an added layer of protection. Debit cards are not protected like credit cards are and should be avoided for online purchases.

Staying Proactive During the Holiday Season

The holiday season is a time for joy and celebration, but it shouldn't come at the cost of your cybersecurity. Cyber threats ramp up during this time of year, targeting businesses at their most vulnerable.

By taking a proactive approach and following these essential steps, **you can keep your operations safe from holiday cyber grinch attacks.**



Want Peace of Mind Beyond the Holidays?

Cybersecurity doesn’t stop when the decorations come down. As your trusted MSP, we can offer more than just seasonal tips — we provide year-round protection, strategic IT solutions, and expert guidance to ensure your business stays ahead of evolving threats.

Don't let cyber grinches steal your peace of mind this season or any time of the year. Partner with us for a stress-free, secure holiday season and beyond.

Contact Us Today

to learn how we can help you enjoy not just a relaxed holiday but a **thriving, secure business all year long.**

NETWORKS
PLUS