TIR-20251125 Stay Vigilant - Top Cyber Scams to Watch During the Holiday Season

11/25/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

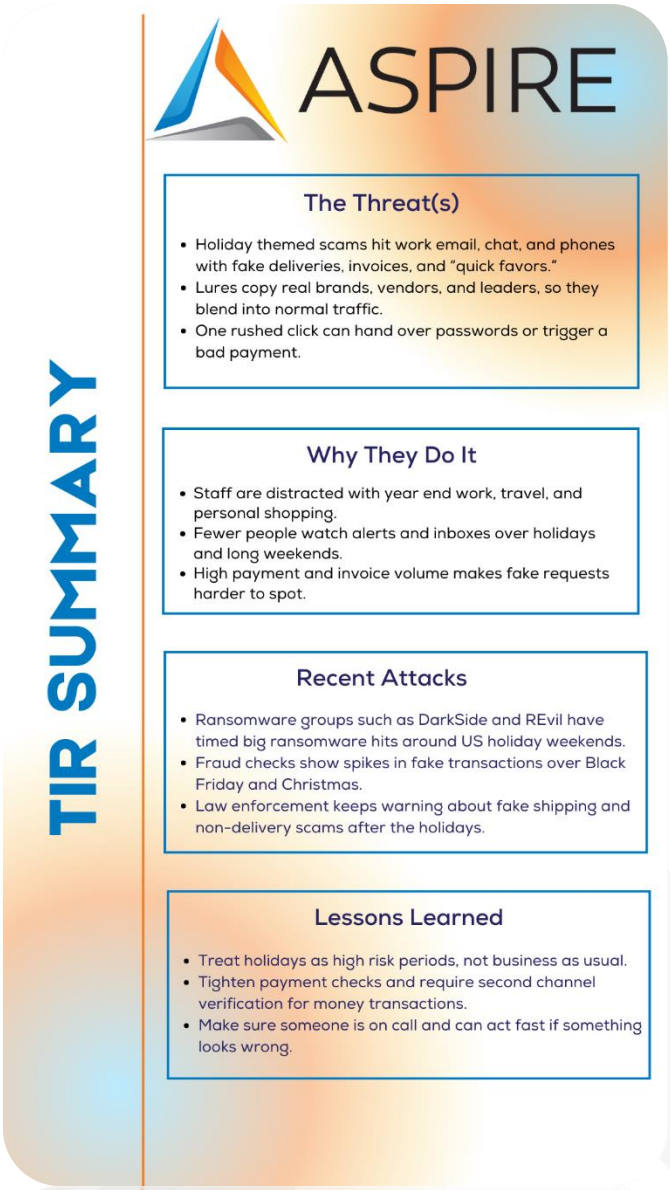
Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

Every year, the holiday rush stretches teams thin and blurs the line between personal and work activity. Staff juggle year-end invoices, travel plans, and online shopping, often from the same laptop and phone they use for business. Threat actors know this, and they plan around it. Government and industry reporting has shown steady spikes in fraud, phishing, and ransomware around Thanksgiving, Christmas, and long weekends, when organizations are running on skeleton crews and attention is split.

For many organizations, the front door is not a zero-day vulnerability, but an employee reacting quickly to a text/email about a “missed delivery,” a last-minute “invoice,” or a “holiday gift card” from a senior leader. Fake package alerts, gift card schemes, charity scams, targeted phishing and last minute finance emails all lean on the same weak spots. They sound urgent and borrow the names of trusted brands or leaders people trust, blending into the normal rush of holiday requests at work. When those lures hit a corporate inbox or device, they can lead to stolen credentials, unauthorized payments, or full ransomware incidents.



Aspire Technology Partners
(732) 847-9600
www.aspiretransforms.com

Companies and organizations cannot control how creative attackers get, but they can control how predictable their defenses are. Clear internal policies on gift cards and donations, strong verification steps for invoices and payment changes, and pre-holiday awareness notices go a long way. Basic blocking, multifactor authentication, strict controls on remote access, and someone on call over holidays who knows what “odd” looks like in your environment also help. The goal is not to scare staff away from celebrating, but to make sure one rushed click from November to December does not turn into an incident response call when everyone is enjoying their loved ones.

Why Attackers Target During the Holidays and Major Events

Holiday campaigns are not random; they are timed around human behavior and business operations. On the human side, people are busier and more distracted. Staff are checking personal and company orders from their work email, grabbing last-minute travel deals, and responding to texts between meetings. Attackers add a sense of urgency with alarming phrases like “delivery will be returned,” or “bonus expires today,” to push employees into acting before thinking. Behavioral studies and incident data both show that rushed users are more likely to click on links and approve payments without a second check.

Operationally, the calendar favors attackers. Long weekends and year-end breaks mean fewer eyes on what matters and slower response times. The Cybersecurity Infrastructure and Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have documented how ransomware groups timed several high-impact operations to Mother’s Day, Memorial Day, and Fourth of July weekends, including the DarkSide attack on Colonial Pipeline and REvil’s attacks on JBS and Kaseya’s customers. In each case, limited staffing made it harder to detect and contain the intrusion quickly, giving attackers more time to move laterally and data.

Major retail periods and events also provide cover (Black Friday, Cyber Monday, last minute Christmas deals). When fraud and transaction volume spikes, a single bogus invoice or payment instruction blends into the noise. TransUnion, for example, found

that over 5% of all digital transactions[1] over Thanksgiving through Cyber Monday 2024 were suspected fraud attempts, and bot-driven attacks on e-commerce sites surged during Black Friday and Christmas. Finance teams working through a backlog of order and refunds may not spot a slightly off vendor domain or an unusual change to banking details on a familiar logo.

Finally, holidays bring out generosity. Companies run charity drives or issue surprise bonuses. Attackers copy those patterns via fake donation appeals from "HR," spoofed emails from executives requesting urgent gift card purchases, and bonus notices that lead to credential-stealing login pages. The same good intentions that drive real workplace giving can be turned into leverage for fraud.

Fake Package Deliveries

During peak season, most offices see a constant flow of boxes and courier drop-offs. Attackers piggyback on that reality by sending fake shipping notifications directly to corporate email accounts and mobile numbers. Messages often claim a package "could not be delivered," that an address needs to be updated, or that a small fee is required to release a parcel. The link leads to a phishing site designed to steal credentials or payment details, or to install malware on the device. The U.S. Federal Trade Commission has warned about a rise in these fake delivery alerts, noting that they frequently aim to capture online banking and email logins.

In the workplace, these lures may reference common carriers (UPS, FedEx, USPS, DHL) or even internal mailrooms. Staff who routinely receive shipments (office managers, facilities teams, lab staff, retail locations) are at higher risk simply because delivery messages are part of their normal day. When those messages land on corporate phones or laptops, a single click can give an attacker valid credentials to email or VPNs. From there, they can pivot into invoice fraud, payroll changes, or full account takeover.

[1] Trailant.com

Image 1: Fake FedEx Text to an Employee

Gift Card Scams

Gift cards are a convenient way for companies to reward staff at the end of the year, and attackers have learned to fold them into social engineering. One pattern targets the organization's own purchasing. Threat actors will create fake gift card portals, lookalike vendor sites, or tamper with physical cards that carry no real balance when employees try to use them. Another pattern is more direct. This involves a text or email that looks like it came from the CEO, a department head, or HR, asking an employee to buy hundreds or thousands of dollars in cards "as a surprise for the team," then send back the numbers and PINs.

Attackers also spin up fake gift-card websites because they know many companies use legitimate multi-card platforms to buy rewards for staff. These scam sites look polished and offer the same range of brands you'd expect — Visa, Amazon, Target, restaurant cards, you name it. Once someone clicks a link from a spoofed email and lands on that fake checkout page, the attacker can grab payment details, corporate card numbers, or login credentials without raising suspicion. The whole setup works because it mimics a process businesses use all the time, making it harder for employees and executives to notice anything out of place.

These scams are popular because they are fast and hard to reverse. Once the codes are sent, the money is effectively gone, and there is no chargeback process the way there is with a credit card. Law-enforcement and consumer protection agencies have repeatedly warned that gift cards are a favorite payment method for fraud because of that one-way nature. From a business perspective, a company will receive backlash and potential fallout if the scam started from a compromised internal mailbox that now needs full incident response.

Image 2: Fake Gift Card Email

To Troy JanHorse

Subject You are the Bee's Knees!

Hey!

Are you free right now? Man, I need a favor. I am working on incentives for the SOC, and I want to surprise them with $1k each in VISA gift cards. There are quite a few people to purchase gift cards for, so I will need your help. Use the company card to make the purchase, I already approved it. Send me the pin numbers on all the cards so I know you bought them. And throw one in for yourself, you deserve it for all the hard work you do! Thanks so much for helping me out!

Cheers!

Leigh Gitimate
Director of the SOC at Not Even a Real Company, LLC

Charity Scams

Corporate giving ramps up in November and December. Many organizations coordinate food drives and donate to local non-profits. Although giving brings people joy, attackers will take advantage of that generosity. Fake fundraising emails, spoofed websites, and cloned versions of well-known charities appear with appeals tied to disasters or children's causes. Some impersonate HR or leadership and ask staff to donate through a link "so the company can track and match contributions."

The FBI and other agencies have noted that charity fraud often spikes after major events and around holidays, with criminals creating organizations that sound nearly identical to legitimate ones or using lookalike domains to capture donations and card details. In a workplace context, these scams can erode trust if employees believe the company endorsed a fake campaign. They can also become a foothold if the phishing site requests corporate email logins "to confirm employment" or "access the internal giving portal."

Spearphishing

Holiday spearphishing blends traditional business email compromise (BEC) attacks with seasonal themes. Instead of a generic "payment request," the message might talk about year-end bonuses, updated travel itineraries on behalf of the CEO, or holiday party details. Attackers research the target company, then spoof real vendors or executives. Increasingly, they also rely on phishing-as-a-service platforms that automate a lot of the work, including redirecting security scanners to benign pages while sending real users to credential-harvesting sites.

For Microsoft 365 and Google Workspace environments, those stolen passwords are often just one factor away from full access to mailboxes, document libraries, and chat histories. Once an attacker controls a real internal account, they can forward conversations or request updated banking information from payroll under the victim's name. During the holiday window, when staff may be approving payments from home or working odd hours, unusual requests can slip by without the usual scrutiny.

END-OF-YEAR FINANCE SCAMS

December is chaotic for finance and accounting teams. There are budget true-ups, vendor renewals, expiring discounts, and tax planning. Attackers take advantage of that pressure by sending fraudulent invoices or payment change requests that fit into expected workflows. Messages may reference genuine projects or suppliers, pulled from prior compromises or social media. The hook is usually something along the lines of “please settle before year-end” or “new remittance instructions due to audit.”

Image 3: Fake Finance Email with Malicious PDF Attachment

To Pat Ching

Subject URGENT - Need Vendor Paid

Good Afternoon Pat,

Accounting is wrapping up the end of the year and we realized that we still haven’t paid the vendor, ZeroTrust for the work they did on the paigeload project. The balance is in the pdf I attached to this email. I need you to authorize payment since you were the lead on this project and can account for their hours. The link will take you to Docusign where you include your signature. Need to get these folks paid, ASAP!

Thanks!

Bree Chdetector
CFO at Not Your Company But a Scammer, LLC

The FBI’s Internet Crime Complaint Center data shows that non-payment/non-delivery and credit card fraud together cost victims close to a billion dollars in a recent year, with many scams centered on online commerce and invoice manipulation. In a business setting, a single large fraudulent wire can overshadow the impact of a typical consumer scam. Because the messages often look like routine vendor communication, technical controls alone are not enough; organizations need clear internal rules for verifying payment changes and large transfers, especially in the last weeks of the year.

WHAT TO DO IF SOMETHING FEELS SUSPICIOUS

When people are not sure what to do, small habits matter more than fancy tools. Give employees simple steps they can follow instead of vague reminders to be careful.

- **Fake Package Deliveries**
  - Check tracking only in the carrier app or a saved bookmark. Ignore links in unexpected texts or emails.
  - Never enter work logins or card numbers from a shipping message.
- **Gift Card Scams**
  - Set a hard rule that no one asks for gift cards by email or text.
  - Confirm any gift card request by phone or in person.
  - Buy cards only through approved channels and never pay outside vendors with gift cards.
- **Charity Scams**
  - Use a short, vetted list of charities for workplace giving. Check any new charity on sites like Charity Navigator or the Give.org.
  - Donate through official sites, not email links, and verify any “HR donation” message with the head of HR.
- **Spearphishing**
  - Treat any message about money, logins, or urgency as suspect, even if it looks internal.
  - Check the sender address and hover over links before clicking.
  - Confirm unusual requests by phone or chat and send suspicious messages to IT instead of quietly deleting them.
- **End-of-Year Finance Scams**
  - Call vendors back on known numbers before changing banking details or making out-of-cycle payments.
  - Use dual approval for large wires and keep a tight list of people allowed to approve “urgent” payments. If tone, logo, or domain feels off, stop and verify.

Across all of these, leaders should make it clear that no one will be blamed for asking questions. People are far more likely to speak up if they know they will be thanked, not criticized, for stopping a transaction to double-check.

Attacks and Holiday Campaigns

Mother's Day

Several well-known incidents show how attackers build around holidays and busy periods. In May 2021, the threat actor DarkSide hit Colonial Pipeline just before Mother's Day weekend, using stolen VPN credentials to access corporate systems and deploy ransomware. The outage disrupted fuel supplies across much of the U.S. East Coast and forced emergency measures from federal agencies.

Later that same month, REvil affiliates attacked meat processor JBS around Memorial Day, temporarily halting operations in North America and Australia and leading to an $11 million ransom payment.

Fourth of July

Over the Fourth of July weekend in 2021, REvil struck again through Kaseya's remote management software, affecting hundreds of downstream organizations – many of them small businesses that relied on managed service providers. CISA and the FBI later used these cases to warn that ransomware crews intentionally choose holiday windows to gain extra dwell time and leverage.

On the fraud and phishing side, regulators have documented repeated spikes in fake shipping notifications and non-delivery scams during holiday shopping season. The Federal Trade Commission says scammers are sending "missed delivery" texts and emails that lead to credential-stealing sites or malware. The FBI's IC3 also links non-payment and non-delivery scams to hundreds of millions of dollars in losses each year, and notes that complaints spike after the holidays when people realize their orders never showed up. Industry data also shows that suspected fraud increases sharply between Thanksgiving and Cyber Monday and stays elevated through December, with higher rates of bot-driven attacks on retail sites and malvertising campaigns pushing fake offers.

While not every case ties directly to one of the five scams covered here: attackers still time their work to the same peaks in shopping, travel, giving, and year-end processing that every business experiences.

CONCLUSION

Holidays and major events bring out the best in organizations – generosity, rewards for staff, and a push to close the year strong. They also bring out opportunists who watch for distraction and overload. Each of these scams uses the same basic tactic, just dressed up differently. Someone inside the business gets pushed to click, approve, or pay without the usual checks.

Technical defenses matter, but culture and process matter just as much. A workforce that knows what “normal” looks like during the season, understands the scams that are circulating, and feels comfortable questioning odd requests is far harder to exploit. With a modest amount of preparation now, such as clear policies and training, organizations can reduce the odds that a festive message or “urgent” year-end request turns into the incident everyone remembers in January.

RECOMMENDATIONS

You do not need fancy tools to stop most holiday scams. You do need clear rules that people can follow when things are busy.

- **Refreshers -** Send a short holiday reminder that walks through the five main scams with real examples. Set firm rules that no one asks for gift cards by email or text, no donations come from links in work email without vetting, and any request that moves money gets checked on a second channel.
- **MFA -** Turn on multifactor authentication for email, VPN, and remote access. Before the holidays, remove old accounts and trim admin rights, especially for seasonal staff.
- **Filter -** Tune filters to catch lookalike domains and holiday lures such as fake shipping or gift card messages. Use web filtering to block known phishing sites.

- **Finance -** Put simple payment rules in writing for year end. Use call backs on known numbers for banking changes and urgent payments and require a second approver for large wires.
- **Monitor -** Plan for low staffing on holidays. Assign on-call coverage, add alerts for odd logins and mailbox changes, and run a short practice walk-through for account takeover, ransomware, and fake payment cases.

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**

- The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Watch for Cyber Monday Scams

Holiday scams 2025: These common shopping habits make you the easiest target | Malwarebytes

12 Holiday Cyber Scams to Avoid | Terranova Security

'Tis the Season for the Wayward Package Phish – Krebs on Security

How the Cyber Grinch Stole Christmas: Managing Retailer Supply Chain Cyber Risk - Security Boulevard

Why company hacks like the REvil ransomware attack tend to happen over holiday weekends | Fortune

Holiday Cybersecurity Tips | NCDIT

Ransomware Awareness for Holidays and Weekends | CISA

Colonial Pipeline attack: Everything you need to know | ZDNET

Holiday Phishing Scams: How to Stay Cyber-Safe This Festive Season - AccessIT Group

Stay Cyber Safe: 5 Tips for Secure Holiday Shopping

Holiday Scams — FBI

Cybersecurity Risks to Watch This Holiday Season | Traliant

Scammers are delivering phishing messages this holiday season | Consumer Advice

12 Holiday Scams to Watch for at Work This Christmas

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.