



HUNTRESS

2025 Cyber Threat Report: Phishing Schemes

Understanding modern
phishing tactics and how to
defend against them

Table of Contents

Introduction

Phishing is a threat that's always evolving.....	3
Most common phishing themes we observed throughout 2024	4

Phishing tactics

Impersonated brands.....	5
Voicemail luring	6
Image-based content	7
QR codes.....	8
Fake "threads" and reply chains	9
Living Off Trusted Sites (LoTS)	10
E-signature impersonation	11

About Huntress Managed SAT

Organizations are stronger with Huntress Managed SAT	12
What sets Managed SAT apart?.....	13

Conclusion

Phishing remains prevalent, but it doesn't have to be painful.....	14
--	----



Phishing is a threat that's always evolving



We've come a long way from the days of glaring typos and poor grammar. Phishing scams just aren't as obvious as they used to be. They've gotten a lot more advanced and are now one of the biggest risks for businesses of all sizes. Since phishing isn't going away anytime soon, turning your team into your organization's first line of defense is key. That's why Huntress created a system to spot and stop malicious emails from causing you harm.

This eBook highlights the most common phishing techniques we saw in the wild in 2024, explaining how they work, why they're effective, and how Huntress Managed Security Awareness Training (SAT) can help bolster your organization's defenses.

The most common phishing themes we observed throughout 2024 include:

- **Brand impersonations:** Relies on familiarity to lower your guard.
- **Voicemail luring:** Leverages urgency and curiosity to deceive.
- **Image-based content:** Avoids scanners with clever design tricks.
- **QR codes:** Takes advantage of unguarded mobile devices.
- **Fake threads & reply chains:** Mimics conversations to gain your trust.
- **Living Off Trusted Sites (LoTS):** Capitalizes on the credibility of well-known platforms.
- **E-signature impersonation:** Exploits trusted platforms to bypass detection.

By the end of this short guide, you'll be more informed about these prevalent threats and also understand how Managed SAT can transform your team from potential victims to vigilant defenders.

Notable Phishing Email Themes



Figure 47: Prevalent phishing themes in 2024

Impersonated brands

Some companies are household names for a reason. Attackers know this and exploit your trust in reputable brands like Microsoft, DocuSign, Dropbox, and Adobe.

Throughout 2024, Huntress found that Microsoft was the most commonly impersonated brand, making up 40% of observed attacks, with DocuSign close behind at 25%.

Spot the fakers

- Emails may appear legit without a closer inspection—teach your team how to spot slight differences in domain names or branding elements.
- Choose an SAT program with timely, relevant lessons tailored to address real-world threats effectively.

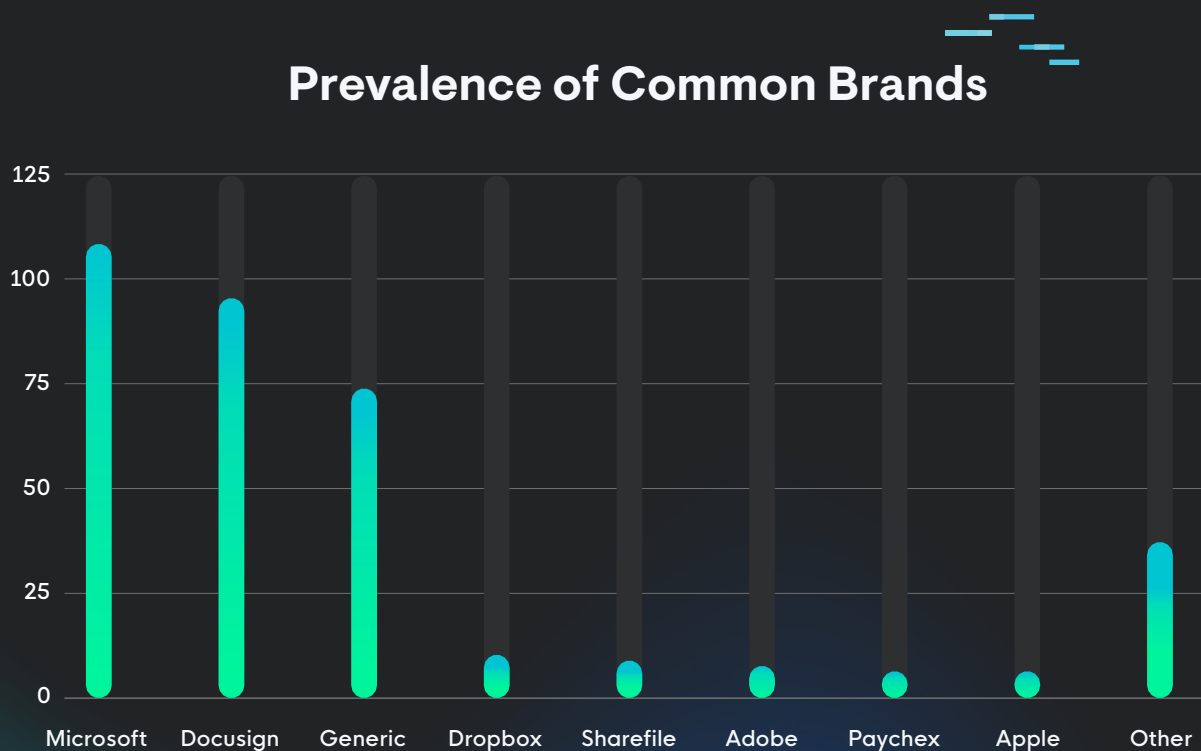


Figure 48: Prevalence of common brands impersonated during phishing incidents

Voicemail luring

If you haven't yet, it's likely you'll one day find an email claiming you've missed an important call. It'll say something like, "You've received a voicemail from [Unknown Caller]. Click here to listen now." Given how busy you might be, your urge to click will be strong, especially if it looks like the email came from your organization's phone system.

Attackers love to exploit this sense of urgency. These emails often link to malicious websites designed to steal your login credentials or deliver malware. What's worse, the websites you're redirected to will look *just real enough* to trick you if you don't look closely.

How to protect yourself against voicemail lures

1. **Slow down:** If an email demands quick action, think twice. Take a moment to verify its legitimacy.
2. **Inspect links:** Hover over any link before clicking to see where it leads. If the link is suspicious, leave it alone.
3. **Leverage training:** An effective, memorable SAT program can help you and your team spot and tackle these sneaky tactics head-on.

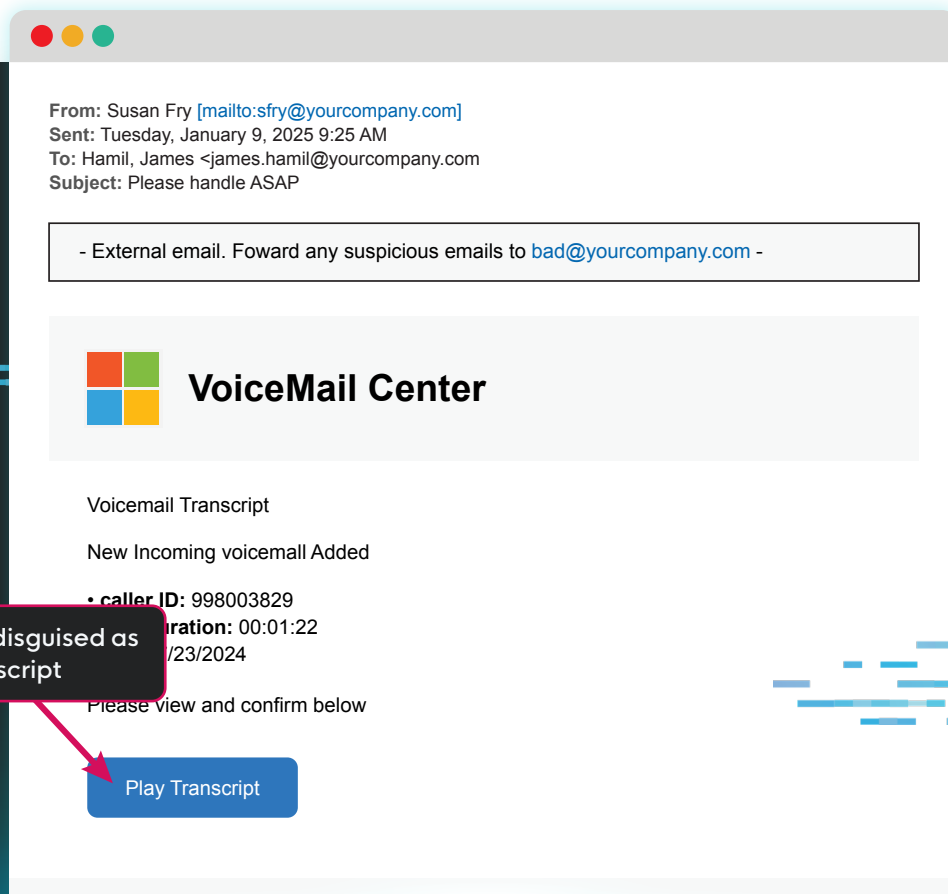


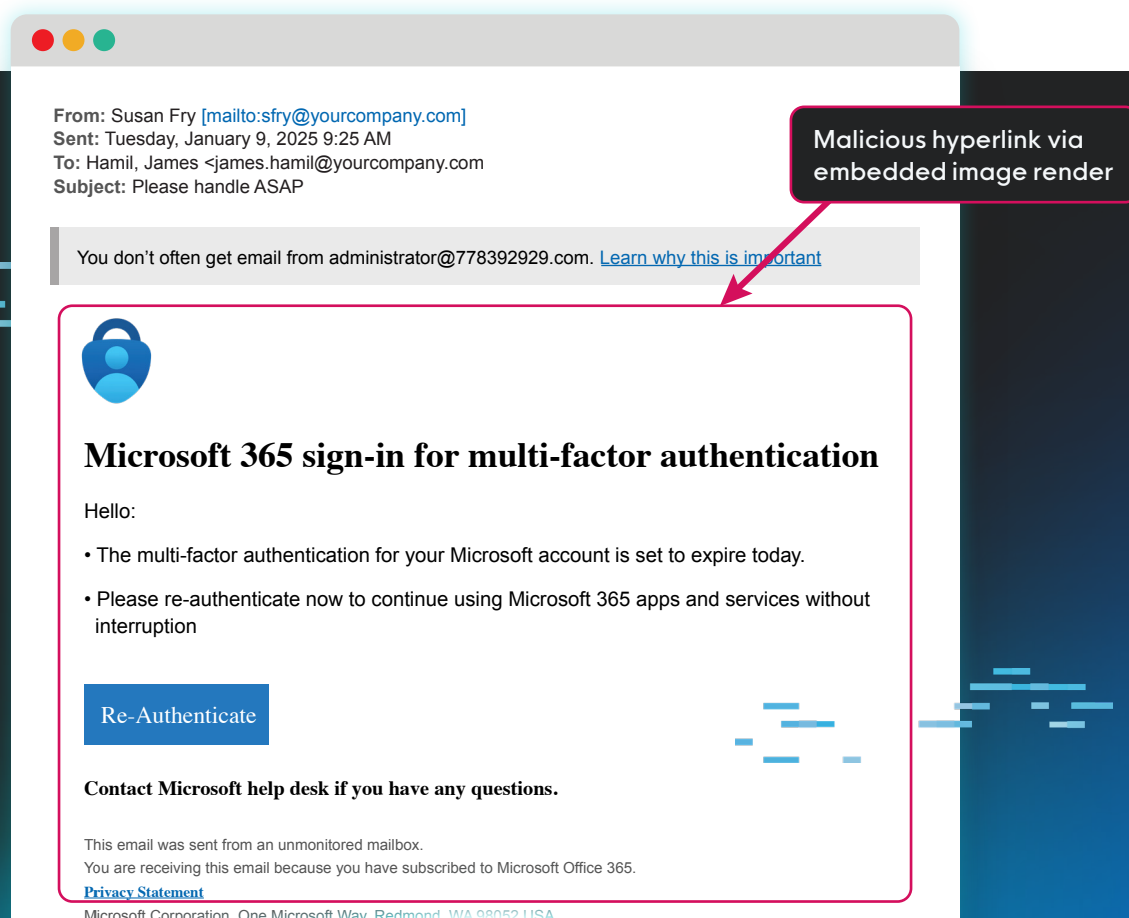
Image-based content

Gone are the days when phishing emails were built entirely with text. Attackers now embed content in hyperlinked images, sidestepping text-based email filters. The email might look simple, but its sole purpose is to bait you into clicking the image and landing on a malicious site.

Although email security scanners have come a long way, attackers keep innovating by tweaking designs and using images in crafty ways to bypass detection.

Stay safe against phishing attacks disguised as images

- **Learn to identify them:** Emails with a single image and little else should set off alarm bells.
- **Think before you click:** Always navigate to the site directly instead of clicking links embedded in emails.
- **Reduce risks proactively:** Run simulated phishing tests with your team through a trusted SAT program to mimic modern attack methods. This is a safe way to strengthen your defenses.



An example of an image-based phishing email attempt

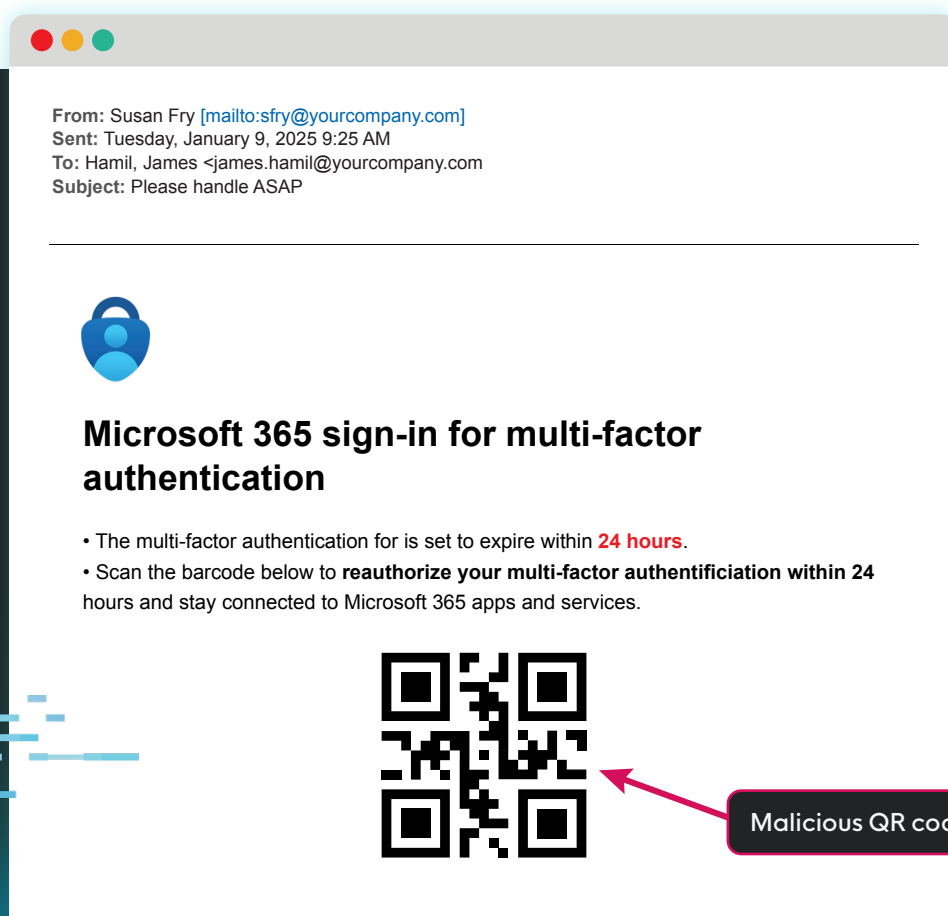
QR codes

No longer confined to marketing campaigns and restaurant menus, QR codes are now part of phishing attacks. Hackers embed them in emails to get around link detection systems. These codes often lead users to malicious websites that steal your credentials or distribute malware.

The issue gets even trickier if you scan these codes on your personal devices, which usually don't have the same security protections as company-issued equipment.

Avoid QR-based phishing attacks

- **Be skeptical:** Treat QR codes in unexpected emails with the same caution you'd reserve for unfamiliar links.
- **Mind every click:** QR codes often lead to landing pages, typically associated with familiar brands. Stay cautious, as hackers can spoof sites that closely mimic legitimate ones. If you're not sure, it's safer to visit the brand's official website directly.
- **Educate through experience:** Use memorable, engaging SAT programs and phishing simulations that focus on modern email tactics, so your team knows what to expect.

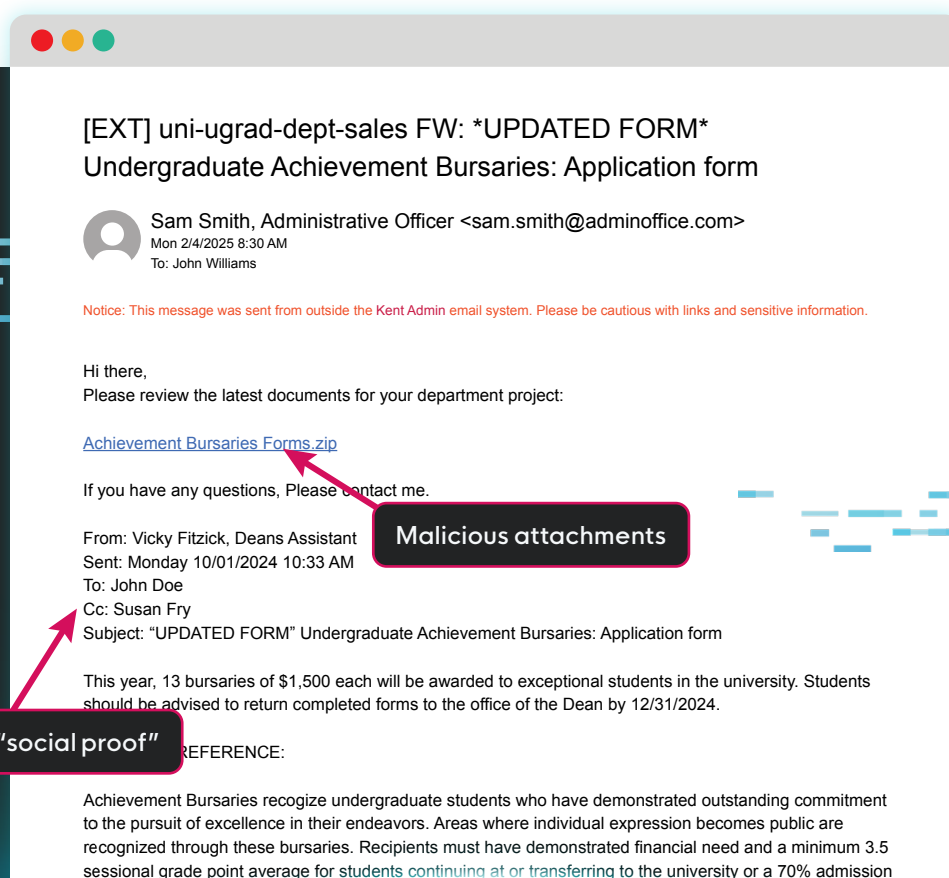


Fake “threads” and reply chains

Attempting to build trust through “social proof,” attackers craft convincing email chains that appear to involve multiple parties. These fake conversations are hard to ignore because they feel personal and urgent. Often, these emails include harmful attachments designed to deploy malware that can steal your sensitive data.

Don’t fall for fake threads and replies

- **Pay attention to details:** Encourage your team to question unexpected reply-all emails.
- **Get expert guidance:** Phishing defense coaching from real cybersecurity practitioners can give you the know-how to identify red flags you might’ve otherwise overlooked in a real phishing attack.



An example of a malicious fake thread email phishing attempt

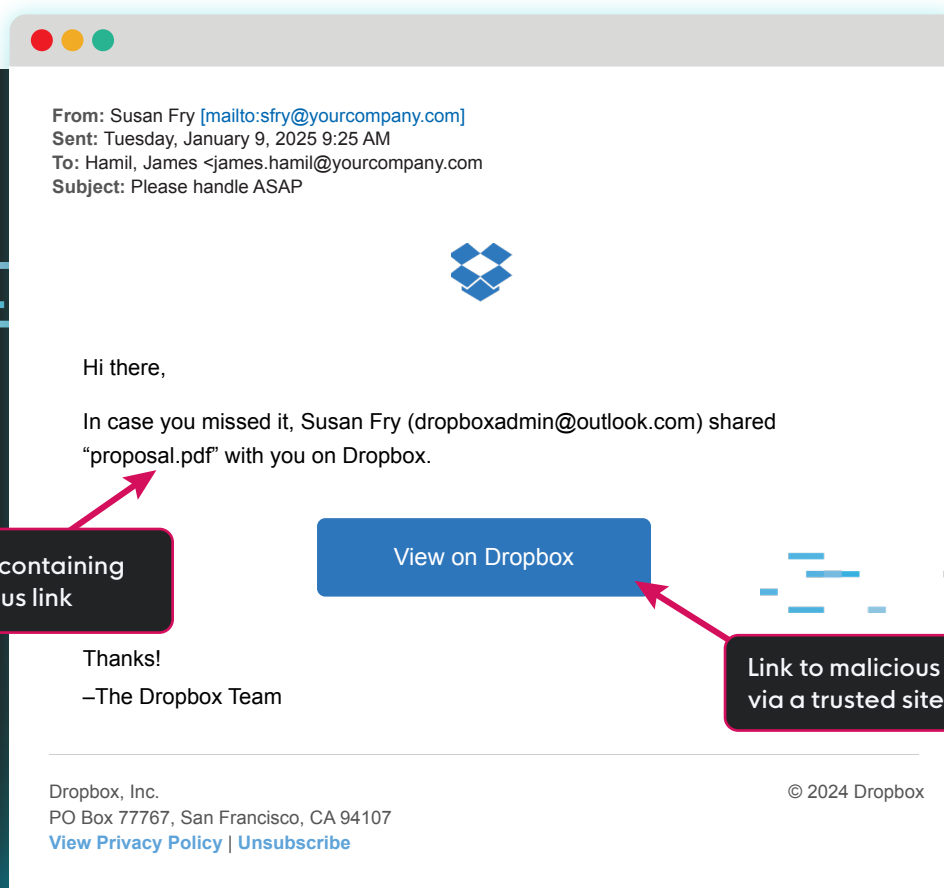
Living Off Trusted Sites (LoTS)

Malicious hackers are adapting by taking cover under the credibility of trusted platforms like Google Drive or Dropbox. They upload malicious content to free or trial accounts, then send you a direct link to the trusted platform. Or they'll send you a link to the trusted site but ask you to click another link that takes you to a site designed to steal your credentials. Because the initial email is technically "clean," it sneaks past most email filters.

This technique capitalizes on the fact that people generally drop their guard when using trusted third-party platforms.

Minimize your exposure to harmful LoTS tactics.

- **Don't be too trusting:** Remember that not everything shared via reputable platforms is safe. And be skeptical of links that redirect you to other sites.
- **Question relevance:** Why is someone sending you these documents? Were you even expecting them? If something feels off, it probably is.
- **Practice, practice, practice:** Phishing simulation exercises and defense coaching from expert-led SAT programs can expose your team to LoTS attacks in a safe, controlled environment.



An example of a LoTS phishing email attempt

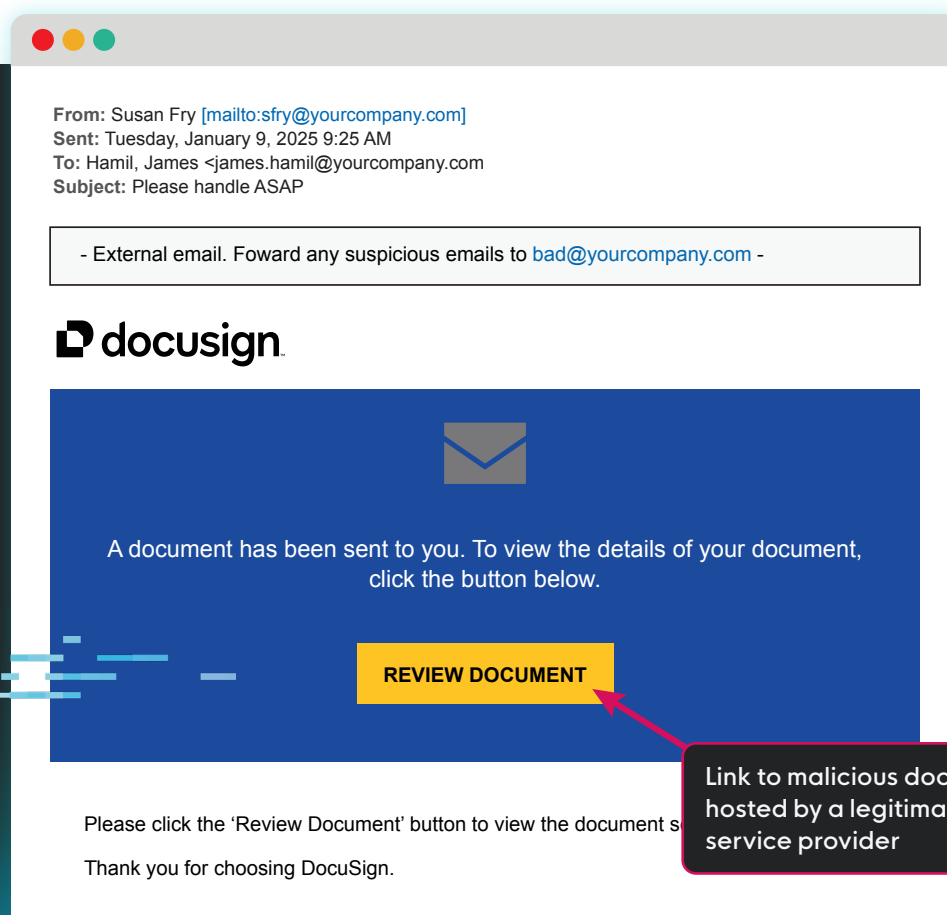
E-signature impersonation

E-signature tools like DocuSign and Adobe are critical for modern workflows, which makes them prime targets for threat actors. Impersonation attacks are a style of LoTS phishing that usually follows one of two patterns:

1. **Spoofted emails:** Hackers are now creating emails that look nearly identical to official messages from trusted e-signature platforms. Unprepared recipients often fall for them without second-guessing.
2. **Malicious files on legitimate platforms:** Some hackers go straight to the e-signature platform itself. Because the message originates from a trusted service, it's much harder to detect. They'll use legitimate accounts to send you a document that'll ask you to click a link. Not surprisingly, you're redirected to a new web page designed to steal your credentials or deploy malware.

Defend your org from e-signature impersonation

- Familiarize yourself and your team with what authentic e-signature emails should look like.
- Use phishing simulation exercises to test how you and your team would respond to this threat.




An example of a DocuSign phishing email attempt



Organizations are stronger with Huntress Managed SAT

Traditional SAT solutions are built by generalists with little visibility into modern phishing threats. Huntress Managed SAT, however, is backed by cybersecurity experts who know exactly what attackers are up to.



Our team keeps your training fresh with emerging phishing tactics, real-world examples, and behavior-based assignments that focus on your riskiest users. Managed SAT gives you:

- **Proven engagement:** Memorable, relatable content keeps learners invested.
- **Real behavior change:** Gamification and hands-on simulations help your team retain knowledge and build habits that protect your business.
- **Lower human risk:** Address risky behaviors in the wild with tailored, just-in-time training.
- **No admin headaches:** Get fully managed learning plans, plus robust reporting, integrations, and automated features that make your job easier.

When you use Managed SAT, your security awareness program becomes more than just a compliance checkbox. It creates a security-centric culture that actively reduces risks for your organization, keeps you safe, and stops phishing scams before they start.

What sets Managed SAT apart?

Built on real-world data

Huntress security experts analyze real attack data from the millions of endpoints and identities they manage. They identify the tactics threat actors are actively using, and they shape episodes and phishing scenarios to mirror the threats your users are most likely to face.

Story-driven training episodes

Our security experts and Emmy Award-winning animation teams collaborate to deliver fresh, memorable content. These engaging, consumable episodes adhere to adult-learning frameworks to ensure they'll truly resonate with your team.

Realistic phishing simulations

Your team will face realistic phishing simulations crafted by our cybersecurity experts. These scenarios replicate the latest tactics used by attackers, helping your team develop a hacker's mindset. By understanding how attackers think, they'll become stronger, more effective defenders.

Phishing Defense Coaching

Someone on your team fall for a phishing scenario? No problem. Our personalized coaching breaks down what went wrong and highlights what to watch for next time. Phishing Defense Coaching delivers just-in-time, context-specific training while the experience is still fresh, ensuring employees learn effectively from their mistakes.

Fully managed by experts

You probably don't have time to babysit a SAT program. That's why Huntress handles the management, from creating and scheduling monthly lessons to curating monthly phishing campaigns. Set it and forget it—we'll handle the training so you can focus on your priorities.



Phishing remains prevalent, but it doesn't have to be painful.

Phishing tactics are always evolving, changing constantly in the hopes of catching you off guard. But if you know how to identify nasty tricks like voicemail luring, image-based phishing, and impersonated branding, you're already leaps ahead of attackers.

Pair this awareness with a solution like Huntress Managed SAT, and you can turn your employees into an unbreakable line of defense against cyber threats. With engaging story-driven lessons, real-world simulations, and expert coaching, Managed SAT helps build vigilance and awareness across your entire team.

Now's the time to prepare your team to not only identify phishing scams but prevent them altogether. When your people know better, they defend better. And with Managed SAT by your side, they will.

Start your free trial of Managed SAT today.



About Huntress



Huntress is the enterprise-grade, people-powered cybersecurity solution for all businesses, not just the 1%. With fully owned technology developed by and for its industry-defining team of security analysts, engineers, and researchers, Huntress elevates underresourced tech teams whether they work within outsourced IT environments or in-house IT and security teams.

The 24/7 industry-leading Huntress Security Operations Center (SOC) covers cyber threats for outsourced IT and in-house teams through remediation with a false-positive rate of less than 1%. With a mission to break down barriers to enterprise-level security and always give back more than it takes, Huntress is often the first to respond to major hacks and threats while protecting its partners and shares tradecraft analysis and threat advisories with the community as they happen.

**As long as hackers keep hacking,
Huntress keeps hunting.**

Join the hunt at www.huntress.com and follow us on X, Instagram, Facebook, and LinkedIn.

[Learn More](#)

X in  

