September 2026

Think Before You Bite

By Richard Morrill

Recently at the help desk, we've seen an uptick in folks reaching out to us with uncertainty regarding an email they've received. We've all heard of classic scam emails, like the infamous "Nigerian Prince" who just needs a small wire fee to release a fortune, promising to pay us back tenfold. Historically, these types of scams were easy to spot, but today, with the advent of large language models and AI assisted tools generally, scammers are able to send out an estimated **3.4 billion phishing emails globally every single day**.

Many of these modern attempts look remarkably convincing, nearly indistinguishable from legitimate messages sent by the actual companies they pretend to be. Because up to **90% of cyberattacks begin with phishing**, it's never been more important to arm yourself with the knowledge needed to safely navigate the modern digital landscape. The good news? You don't need a degree in computer science to spot a fake email, you just need to know the hooks to look out for.

Spotting the Hooks

There are many potential ways a scammer may try to hook a mark and it's important to understand some of them because knowledge of them allows us to identify and keep ourselves safe from them. Here are some common methods used to trick people into falling victim.

The Sense of Urgency

"Think before you act" is a good rule in life because it allows you to evaluate your actions before you have to live with the consequences. Scammers want you to skip that entirely. A rushing potential mark can become a victim quickly. Phishing emails often demand immediate action with phrases like "Your account will be suspended in 24 hours," or "Your transaction for $478.22 has been approved, click here if you didn't authorize this," or "Pay this fine now to avoid legal action." Real emails on topics like these rarely give you an immediate deadline, precisely because the legitimate business doesn't want you to make a frantic mistake. If an email you receive makes your heart rate spike, take it as a sign that someone is trying to scare you into action before you've had time to process what's going on.

The Display Name Trap

Modern email clients opt for simplicity at the expense of accuracy and precision. Many of them, by default, only expose the "Display Name" field of an email sender. When first setting up an email account, you typically have to configure what display name you'd like to appear to folks when you send them a message. For real people, this is as simple as your first and last name, so that your friend Sarah knows that cool_fisherman@swcp.com is actually John Doe. Modern email clients will simply show "John Doe" in lieu of the email address itself. Scammers know and exploit this. They can make their first name *Amazon* and their last name *Customer Support* so that you see "Amazon Customer Support" as the "name" for the email. Meanwhile the underlying email address itself is something like john_doe1374@gmail.com, most assuredly not a customer service support email address for Amazon.

Thanks <valued customer name>

It used to be the case that many scam emails were full of typos and grammatical mistakes, but AI has allowed bad actors to leverage the wealth of human knowledge to better format their emails. They still, however, rely on being non-specific in their mass spam campaigns. You'll commonly see emails with phrasing like "Dear Valued Customer" as opposed to your name. This is due to the scam being sent to a myriad of recipients and not just you. Keep an eye out for things that seem too generic.

Deceptive Links and Attachments

Many scam emails rely on poisoned links or bogus attachments as their avenue of exploit. They'll send you a message saying your password is expired, telling you to click a link to reset it, but that link leads to the scammer's own site, designed to steal your information. This works much like the Display Name Trap from before, because a hypertext link can be formatted to say one thing, and do something different. What many people don't realize is that a link in an email or on a website is composed of two parts: what you see, like "click here for the full recipe", and a hidden destination. When you click the highlighted phrase, the underlying link might take you to the recipe, or perhaps someplace more sinister. Scammers can, and do, write their links as something like **go to "mp.swcp.com" to update your password**, but the link actually points to their scam site.

The way to tell where a link actually points is to hover your mouse over it (without clicking on it) to see the actual URL behind the link. If it doesn't match what the text appears to be, it's best to not click. A broader rule of thumb is to simply **never**

click links in an email. If it wants you to visit a real site like your bank, open a web browser and navigate to your bank's address directly, instead of relying on a link that might be hiding something nasty.

On Apple phones and tablets it's a little harder to see the link without clicking. First, try this on a known-safe link in the mail or Safari app: long-press a link, and it will show an preview of the page the link points to. At the top-right of the preview window click **Hide preview**. Not only will the preview go away, it will remember this setting and refrain from showing you previews when you long-press links in the future. This is good because displaying the preview could be just as dangerous as loading the link normally if it was a truly malicious page.

Dangerous Attachments

Likewise, attachments can be pretty dangerous to interact with. If you aren't expecting your friend George to send you a PDF, it's best to not open any attachments he sends without checking with him first. Many tricks are used for this, such as naming files in a misleading way. In the name of simplicity (like the Display Name from earlier), operating systems will hide common file types like a .exe (Executable Windows Program) from your view, so you simply see "PayPalInvoice", which you might assume is a PDF, when it's really "PayPalInvoice.exe". A ".exe" files is a program execute code on your device and do many potentially nefarious things. Your computer is full of .exe files and they are not inherently bad, but anyone who tries to trick you into running a .exe out of your email is up to no good. Again, if you don't know about an attachment heading your way, it's best to avoid interacting with them entirely. If you're in doubt about something that appears to come from a friend or trusted business, it never hurts to just reach out to that source and verify before interacting.

Sometimes, the Bait is the Real Thing

Given the increase in frequency of scams and the convoluted tactics employed by scammers, you may be feeling ready to just write off email entirely. The problem with that, of course, is that we still receive valid, important, and even time-sensitive communications via email. What is a responsible citizen to do, then, when faced with the veritable minefield that is modern email? If you receive an email that doesn't have these telltale signs and looks to you to be real, what should you do? You should absolutely confirm with the individuals directly, as referenced previously. Consider an email that purports to be from PayPal about an outstanding invoice. If you don't use PayPal, ignore it, but if you do have a PayPal account, how can you be it's legitimate? Your next and only course of action should be to investigate PayPal directly. **Do not click a link or call a number in the email.** That information source is suspect! Instead, head to **paypal.com** directly and either log in to your account and see if you can find a relevant document in your portal, or use PayPal's "Contact Us" section to give them a call and ask about the Invoice. The same goes for an email that purports to be from your bank: **contact your bank directly** to inquire about it, using trusted methods to uncover contact information, like finding the telephone number from your last account statement, or by visiting their website. It's worth noting that the same strategies also apply to individuals. Take the time to make the call to your loved one before you wire them bail money to help them get out of the prison they "**found themselves in while on vacation**."

We Can Help

While this month's newsletter paints a somewhat bleak picture of the future of phishing emails and the weight of responsibility they place on you to protect yourself, I believe the key takeaway is that a little bit of knowledge and healthy skepticism mixed with a dose of patience can go a long way to helping mitigate many of these common tactics. It's also important to remember that you don't have to be alone in identifying bogus emails. Those of us here at the help desk welcome opportunities to uncover the bad emails and help you navigate safely through your inbox. For those who may be interested, I'll be doing a deeper dive in to the "how" of identifying phishing emails in a subsequent blog post on our web site. It will include screenshots and step by step directions on how to identify key components of an email, like how to make the modern email client tell you the real email address behind the message and how to uncover the true target behind the apparent link.

This Month in Ideas & Coffee

We have a full schedule of free talks and classes this month!

- **September 15 6pm - 7:30pm –** *WordPress Work Along* – Answers to your pressing WordPress questions. Bring your laptop!
- **September 16 6pm – 8pm** – Basic Computer Proficiency – email, browsers, and staying safe online.
- **September 23 6pm - 8pm –** Introduction to WordPress
- **October 7 6pm - 7:30pm** – More on the new AI features in WordPress

Watch the **Ideas & Coffee** event calendar at **https://swcp.com/calendar** for future info.

Southwest Cyberport – swcp.com

New Mexico's Expert Internet Service Provider since 1994

505-232-7992 | Support: help@swcp.com

5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

Click on bold blue type in browser for links.