How Users Can Identify Email Cyberthreats

PART II IN A THREE-PART SERIES FOCUSED ON CYBERSECURITY

Michele Vayle | RENOVODATA

IN THE SEPTEMBER issue of *3PL Perspectives,* we discussed some of the most prevalent types of email cyberthreats, with emphasis on the particular risks faced by 3PL and trucking companies. This article will feature a description of best practices for protecting businesses from these attacks.

As discussed in the first article, the leading entry point for cyberattacks is email, and even strong security systems can allow some fraudulent emails to break through. When that happens, users themselves form the first line of defense. Only a small percentage of users fully understand how to identify such threats, but, as shown here, it is not hard to learn.

These emails seek to fool recipients into taking unwise actions, and resistance to such provocations is absolutely essential. This is especially critical for 3PL and trucking companies because of the volume of email involved in day-to-day business and the speed with which users must process it.

Fortunately, an effective way to neutralize such cyberattacks is to teach employees how to quickly and accurately identify malicious emails. Here are the key steps:

1 – Always err on the side of caution. Even if an email contains the appearance of authentic-looking elements such as believable addresses, page designs, or specialized terminology, it still may feel a little off. This may be because of some subtle, difficult-to-spot peculiarity in appearance, or language. So take a closer look, and trust your instincts.

2 – Start with the salutation. Most business correspondence is sent to you by name, and not "Dear Manager" or "Valued Client." Be suspicious of any email with such a greeting, because it is likely to signal a phishing expedition.

3 – Look at the email address. If it is obviously fake, pull the plug. If it is similar to the real thing, however, it just might be on the up and up and worth evaluating, as in the case of a new business unit within the company. An easy test is to open a new window, type in the website address, and peek behind the scenes.

Also, do not fail to verify domain names. Fakes may differ from real ones by only a few characters. These are easy to overlook, so careful attention is necessary.

4 – Beware of spelling and grammar errors. Although we all make mistakes in written language, real companies strive to avoid them, especially in boilerplate text. Luckily, some otherwise-clever cyber-criminals weren't geniuses in English class and can make glaring mistakes.

5 – Take note of file formats. If an email purports to come from a trusted source, the file formats in the correspondence should match those normally used by the company and be compatible with your own. Careful examination can reveal if the sender's formats are suspect.

6 – Pay attention to the distribution group. The absence of one is a bad sign, as is one you don't know. Some scammers go to the trouble of hijacking real distribution group lists, so an authentic one does not prove the email to be legitimate. If the email turns out to be crooked, be sure to let everyone in the group know, since they may also be targets.

7 – Examine signatures and contact info. Who signed the email? How can the person be reached? When these questions arise, a bit of online sleuthing can usually uncover falsehoods because it is all but impossible for a masquerade to withstand scrutiny.

Hazy contact information inevitably smells of phish, since real companies want to publicize their contact details clearly. If the company and signer are on the level, there should be a website that can verify their legitimacy.

8 – Sender not available to be reached? No thanks. Any statement to this effect within the email is a dead giveaway that fraud is afoot. There is no good reason for any email, other than auto-generated notifications where the company's identity is well-known to the recipient, to omit direct-contact information.

SFIO CRACHO/SHUTTERSTOCK.COM

9 – Never click on hyperlinks in dubious emails. If you happen to open an iffy email, you should be safe, but if you open a link within it, you could put your company in severe jeopardy. When in doubt, don't click.

10 – Never divulge confidential information. Emails from law-abiding organizations do not ask for private, sensitive, or protected data or credentials via email, Facebook, Twitter, LinkedIn, or any other online medium. Such requests tell you a scam is in the works.

11 – Never respond to "immediate action required" demands. They are designed to provoke panicky, impulsive reactions that will lead to disaster. This is a traditional phishing tactic to which 3PL and trucking company employees, with their high-speed work environments, can be susceptible.

Such messages play on our Chicken Little impulses by fictitiously citing an overdue payment, a penalty levied, or some illicit act your company has supposedly committed, with promises of dire consequences from account suspension to legal action if demands are not met.

Fearsome phrases like "Account suspended" or "Unauthorized login attempt detected" usually appear in the subject line, with further intimidation packed into the body text. Direct threats to IT systems lead with statements such as, "Your system has been compromised."

Phishing threats of this kind are dangerous and fighting them requires no deep knowledge. All you need to know is that legitimate organizations simply do not behave in this way.

12 – Never click on attachments you don't know to be legitimate. They can carry any of the malware types, from password theft to data destruction to ransomware, that were described in the first article of this series. Generally speaking, you will normally be aware in advance of any attachments you receive.

Training should be ongoing, and every user should be brought up to speed quickly. Be aware that checking out the authenticity of emails can take time, which is always in short supply for 3PL and trucking company employees. Everyone should understand that no matter how much time it takes to avoid phishing scams, it is imperative for the safety of the company.

While you can be sure that the criminals who design malicious emails never stop thinking up new schemes, the companies that fight them with constantly evolving security devices and defense methods are always on the job and always moving forward.

The next article in this series will discuss best practices for defending your business against email phishing attacks.

Michele Vayle is Marketing and Sales Director for RenovoData in Atlanta, GA. She may be reached at 877-834-3684 or mvayle@RenovoData.com. For a wider range of information on cyber security, go to http://www.renovodata.com/blog.

INDEX TO ADVERTISERS