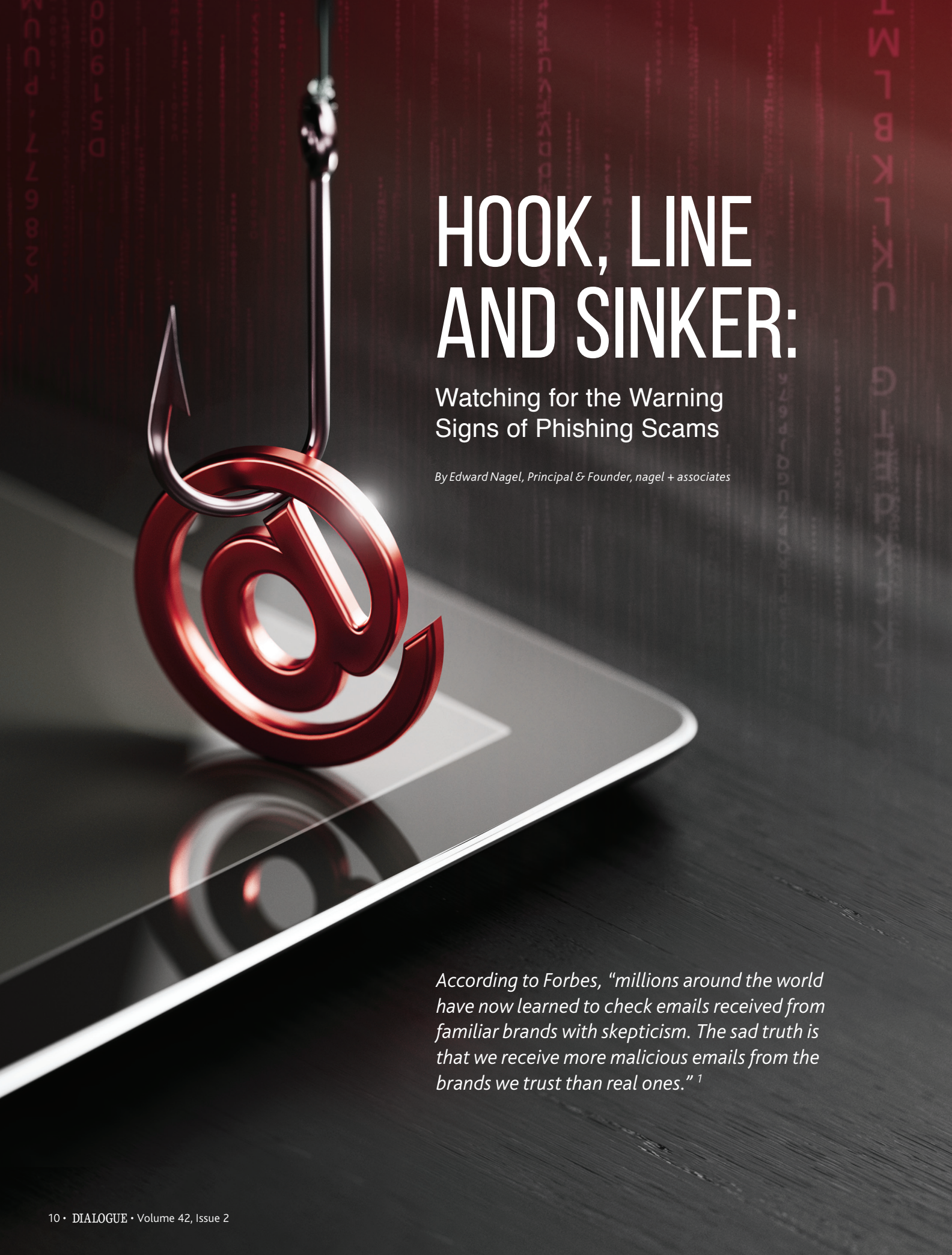

HOOK, LINE AND SINKER:

Watching for the Warning Signs of Phishing Scams

By Edward Nagel, Principal & Founder, nagel + associates

According to Forbes, "millions around the world have now learned to check emails received from familiar brands with skepticism. The sad truth is that we receive more malicious emails from the brands we trust than real ones." [1]

PHISHING: A TYPE OF CYBERCRIME

Broadly defined, phishing is a type of online scam that falls within the category of cybercrime, the intent of which is to extract confidential information and eventually money from you.

On the surface, a phishing email, text message or phone call seems real. Phishing scammers often provide you with a seemingly legitimate reason to click on a link or visit a website. Once on the scammer's website, they ask you to enter your login information, account details and other confidential information, such as a social insurance number and password—all of which arm the scammers with enough information to unleash financial havoc on you or your organization.

EVEN HOLLYWOOD IS NOT IMMUNE

It seems that even the most sophisticated businesspeople are not immune to being victimized by phishing scams. According to an article published by CBC News, Barbara Corcoran, investor on ABC's Shark Tank and founder of real estate brokerage firm The Corcoran Group, admitted she was recently the victim of an email phishing scam. "I lost the $388,700 as a result of a fake email chain sent to my company.... The scammer disappeared and I'm told that it's common practice, and I won't be getting the money back."[2] Another article covering the story published by Global News goes on to explain that "it was an invoice supposedly sent by [her] assistant to [her] bookkeeper approving the payment for a real estate renovation. There was no reason to be suspicious as [she invests] in much real estate."[3] Apparently, the bookkeeper continued to communicate with the person who she thought was Corcoran's assistant and sent a wire payment for a renovation.

Several weeks after the initial news of the Corcoran phishing scam circulated, in an unexpected twist, CNN published an article stating that the German-based bank the bookkeeper used to wire the money froze the transfer before it was deposited into the scammer's bank account in China, enabling Corcoran to recover the stolen funds[4]—a highly unusual but positive ending to the story.

Most victims are not as fortunate as Corcoran. Quick action was undoubtedly critical to her ability to recover the stolen funds.

TYPES OF SCAMS

In my two-plus decades of investigating corporate fraud, I have found that while there are a variety of ways that phishing scams can be carried out, their objective is generally the same: obtain access to the victim's personal/confidential information with the ultimate objective of stealing their money.

Although the method is only limited by the creativity of the fraudster, here are the most common types of these scams:

- **Deceptive phishing:** Deceptive phishing scams, arguably one of the most common scams of its type, typically involve perpetrators impersonating a legitimate organization, such as Facebook or Microsoft. Very often, these communications set out a situation that demands urgency, appealing to your anxiety, such as you will not be able to log into Netflix later that day, thereby minimizing how much time you have to think about it.
- **Spear phishing:** Spear-phishing schemes are often carried out through social media and are typically targeted. The communication is tailored to you to make you believe that they know you, which makes it difficult to catch (sort of like Barbara Corcoran's bookkeeper). These scammers try to convince you to do something, such as click on a link, visit a site, download a file or pay an invoice. While the email looks legitimate, the URL is invariably not, typically leading you to a site controlled by the scammers.
- **C-Suite phishing:** This type of phishing scam targets senior management to obtain login information and impersonate them. Once fraudsters have access to a high-level account, they use that information to influence another employee to perform a specific function, such as paying an invoice. Like other phishing schemes, this one targets unsuspecting employees who are less likely to question a request when it purportedly comes from senior management.
- **Vishing schemes:** This type of phishing scheme typically uses Voice over Internet Protocol (VoIP), a category of hardware and software that enables people to use the internet as the transmission medium for telephone calls. The person on the phone is impersonating someone at an organization that you may routinely deal with, which makes it seem legitimate.
- **Smishing schemes:** This type of phishing scheme is typically carried out by text message or SMS. Similar to the ones carried out by email or phone, the fraudsters target individuals, asking them to visit a website or click on a link, which is invariably controlled by the scammer or the entities with which they are associated. Once you have clicked on the link or visited the site, the information you provide them is used to access your corporate or personal accounts, and is generally accompanied by some kind of financial loss.
- **Pharming schemes:** Given that consumers and organizations have become more aware of the traditional baiting emails, phishing scammers have had to become more creative. These schemes are cyberattacks intended to redirect a website's traffic to a fake or malicious website, typically controlled by a fraudster who is looking to extract information from you, access your server or accounts, and obtain access to your funds. Pharming can be conducted either by changing the host files on a victim's computer or exploiting a vulnerability in the Domain Name System (DNS), which is the internet's way of converting alphabetic names into numeric IP addresses.

---

[1] *https://www.forbes.com/sites/zakdoffman/2019/08/25/microsoft-paypal-facebook-warning-top-10-brands-impersonated-in-phishing-attacks-revealed/#48a7772e73d6*
[2] *https://www.cbsnews.com/news/barbara-corcoran-loses-388700-dollars-phishing-scam-shark-tank/*
[3] *https://globalnews.ca/news/6603601/barbara-corcoran-shark-tank-email-scam/*
[4] *https://www.cnn.com/2020/03/02/business/barbara-cocoran-email-hack-money-returned/index.html*

> "IF IT'S TOO GOOD TO BE TRUE, IT'S PROBABLY A SCAM—HOOK, LINE AND SINKER."

RED FLAGS

When comparing a legitimate email or text to a fictitious one, there are some indicators, or "red flags," that you need to be looking out for to detect a phishing email, including the following:

- **Suspicious sender:** On the surface, the email address looks legitimate. However, there is often an extra letter or character strategically placed so you do not initially see it. I have seen this in practice and it requires a few double takes before you see the typo.
- **Subject line expressing urgency:** One of the hallmark features of phishing emails is the sense of urgency. The language used in the subject line is meant to cause you to react quickly, reducing the likelihood you will question its veracity.
- **Typographical or grammar errors:** Phishing emails are usually replete with spelling and grammar issues. (For reasons unknown to me, these criminals have not been introduced to spellcheck.)
- **Unusual links:** If you hover your mouse over the link in a phishing email, you may notice some unique URLs or shortened links that hide information. This is usually a good indication that it is a fictitious email.
- **Suspicious attachments:** There is often an attachment, which frequently contains links, to a phishing email. Be leery of it. This is often done to avoid being caught by spam and other email filters.
- **Poor quality images:** In today's age of technology, an organization's logo and promotional materials are easily copied from the internet. Therefore, be on the lookout for pixelated logos, images or things that simply don't look right.

HOW HONEST ARE WE?

It has been suggested to me—and I would tend to concur—that 10 per cent of our society is inherently honest and 10 per cent is inherently dishonest, which leaves the remaining 80 per cent to be as honest as the situation dictates. Therefore, arguably, there is a large potential pool out there who could at some point "turn to the dark side."

Moreover, while the vast majority are trying to make an honest living, we need to be mindful that there are people who fill their days thinking about ways to enrich themselves at the expense of others, rather than being productive members of society. They prey on our complacency and lack of attentiveness in the hope that we will let our guards down just once to fall victim to their scams.

If it's too good to be true, it's probably a scam—hook, line and sinker. Watch out for those warning signs. ■

*Edward Nagel, CPA, CA*IFA, CFF, CBV, is a seasoned forensic accountant who, since 1998, has focused exclusively on providing forensic and investigative accounting services to corporations, individuals, and public sector and not-for-profit organizations and their legal advisors/boards, primarily in the area of corporate fraud. Edward is Principal and Founder of nagel + associates, a Toronto-based boutique forensic and investigative accounting firm that specializes exclusively in conducting forensic investigations, anti-fraud consulting, anti-fraud training and crypto advisory services. Contact him at* edward@nagel-forensics.com.