Gone Phishing – Vigilance in the New Scam Era

Published by *Kattison Avenue* | Issue 12

Spring 2024

By Lauren Eiten

"Thank you for your order." "We tried delivering your package." We have all seen these subject lines in our inbox, but some are not so innocent. Business impersonation scams are not new, but some of their tricks are. These increasingly sophisticated scams not only present risks for individuals; they also risk harming a brand's goodwill if the business's name or marks are wrongfully used by bad actors.

According to the Federal Trade Commission (FTC), scammers are increasingly utilizing email and text messaging, rather than phone calls, to initiate the scam.[1] In 2020, 67 percent of business impersonation scams were initiated by phone.[2] In 2023, that number dropped to 32 percent. Over the same period, email scams rose from 10 to 26 percent.[3]

In this new scam era, both individuals and businesses need to be vigilant because business imposter scams are the FTC's most reported fraud.[4] Many of us check our emails on our phone on the way to work or while we wait to pick up our kids from soccer practice. On our phones, it is easy to miss the email address that is supposedly from DHL but contains every letter in the alphabet, or that the purported Norton LifeLock employee uses a Gmail account. Scammers also utilize urgency and scare tactics to spur their victims into action before they have a chance to think twice.

These traps can also catch attorneys' attention. I recently did a double take when I received an email thanking me for an order, although I had not made any purchases recently. Apparently, the reactivation of my Norton LifeLock had been completed for the cost of $699.96. Phony subscription renewals were the second most reported scam type last year, and it is easy to see why.[5] Even though the recipient is suspicious, no one wants to pay hundreds of dollars for a subscription they did not even know they had.

Today's scams are more complex. For instance, scammers now include a phone number for the customer to "verify" or "report the transaction." Once on the line, scammers convince the individual to allow them to connect to the individual's computer, either stating it is necessary to process the refund or for security reasons.

For instance, in my case, the "Norton LifeLock" invoice stated, "Contact us at +1(866) 362-0783 to report if this transaction was not authorized by you." Other red flags included that the payment method was "auto-debit," the salutation was to my email address rather than my name, and a quick google search for the phone number resulted in zero hits. Then to triple-check, I googled "Norton" and "impersonation scam." Sure enough, there was an example of my phishing email, so into the trash it went.

Unfortunately, in this day and age, individuals should be suspicious of any unexpected email. First, trust your instincts. If your first thought is to delete it, then you are probably right. Second, slow down. Check the sender's email address and the payment method, and look for typos. Third, never click on a link or call the number listed in the email. Instead, look up the company's website and use a phone number from that site to verify the email's authenticity. Lastly, report the scam to the FTC at ReportFraud.ftc.gov.[6]

The scam industry is a billion-dollar enterprise.[7] Scammers are good at what they do and are always evolving. If you paid a scammer, you may be able to get your money back by contacting the company you used to send the money and asking them to either cancel or reverse the payment.[8] If you gave a scammer personal information, such as your Social Security number, go to IdentityTheft.gov to make a recovery plan.[9] If you gave the scammer a password, create a new, strong password for all accounts that use that password. Better yet, create multiple new, strong passwords.[10] If the scammer has remote access to your computer, update your computer's security software and delete any identified issues.[11]

Businesses also need to be on the lookout. Scammers capitalize on businesses' goodwill, and as most readers know, goodwill does not come easy or cheap. Businesses should have monitoring practices in place to quickly identify new scams. Customer service representatives should flag and escalate any incoming questions or customer reports, and businesses should quickly add information to their website, either as a blog post or under the "Frequently Asked Questions" section.

On April 1, the FTC's new Rule on Impersonation of Government and Businesses went into effect.[12] The rule states that it is a violation to "materially and falsely pose as … a business or officer thereof," or to "materially misrepresent … affiliation with, including endorsement or sponsorship by, a business or officer thereof."[13] Because of the new rule, the FTC can more efficiently recover money for consumers under section 19(b) of the FTC Act and violators can be subject to civil penalties. The

new rule does not limit the rights or remedies available to trademark owners under the Lanham Act or the Anti-Cybersquatting Consumer Protection Act.[14]

Scammers are here to stay. It is on businesses and individuals to continue to stay one step ahead.

---

1 *Impersonation Scams: Not What They Used to Be*, Fed. Trade Comm'n (Apr. 1, 2024), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/04/impersonation-scams-not-what-they-used-be.

2 *Id*.

3 *Id*.

4 *Id*.

5 *Id*.

6 *Id*.

7 *Id*.

8 *What To Do if You Were Scammed*, Fed. Trade Comm'n (July 2022), https://consumer.ftc.gov/articles/what-do-if-you-were-scammed.

9 *Id*.

10 *Id*.

11 *Id*.

12 16 C.F.R. Part 461

13 16 C.F.R. Part § 461.3.

14 89 FR 15024.

To read *Kattison Avenue* | Issue 12, please click here.