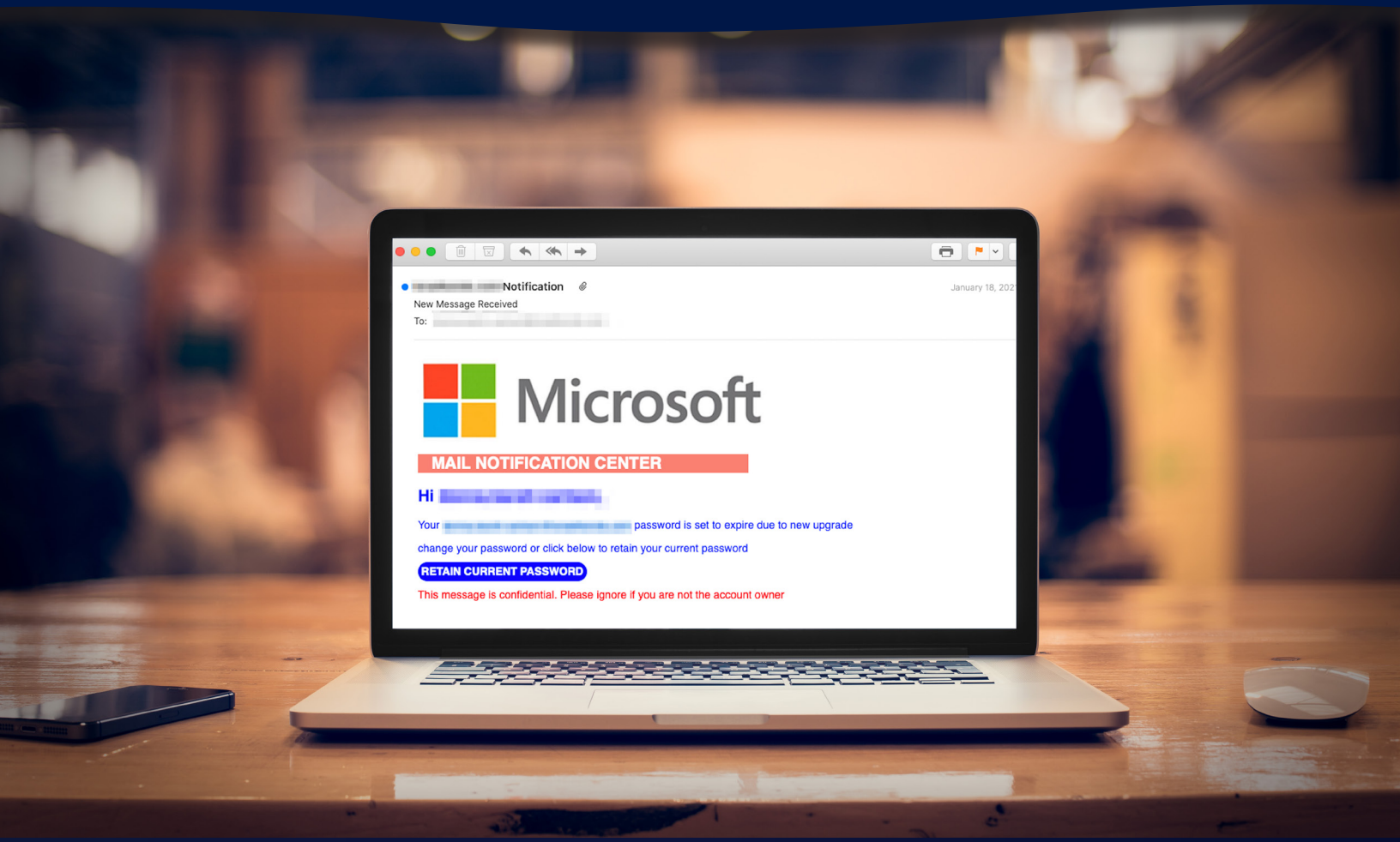
INKY®

REPORT

The Top 25 **Most Phished Brands**

As INKY protected customers' email accounts in 2020, the anti-phishing tool kept track of brand impersonations, detecting in all 40,906 unique campaigns. This report ranks these brand impersonations by frequency and details how they were used in attempts to breach targeted networks.



Introduction.

Well, folks, the stats are in, and we have them: the top 25 most-phished brands during 2020, picked up by our tool, INKY Phish Fence. It should be noted that we caught all these phish, and so stopped them from wreaking havoc on their intended targets — our customers.

Because of its broad footprint across many instances of business email compromise (BEC), Microsoft was unsurprisingly the most phished brand — by quite a stretch. Phishing campaigns impersonating one or more of the many Microsoft offerings accounted for nearly 70% of all brand impersonation phishing emails in 2020 (Table 1).

Table 1

Brand Name	Campaign Count	Sector	% of Brand Impersonations
Microsoft	28,536	Technology	69.77%
Zoom	3,803	Telecommunications	9.30%
Amazon	2,747	Retail	6.72%
Chase Bank	960	Finance	2.35%
RingCentral	807	Telecommunications	1.97%
eFax	542	Telecommunications	1.33%
Intuit	541	Finance	1.32%
CVS	541	Retail	1.32%
American Express	501	Finance	1.22%
Netflix	359	Technology	0.88%
PayPal	306	Finance	0.75%
Xerox	284	Telecommunications	0.69%
DocuSign	226	Technology	0.55%
AT&T	190	Telecommunications	0.46%
Sam's Club	115	Retail	0.28%
LinkedIn	109	Technology	0.27%
Walmart	86	Retail	0.21%
Apple	57	Technology	0.14%
USPS	50	Logistics	0.12%
Dropbox	41	Technology	0.10%
Citibank	32	Finance	0.08%
DHL	28	Logistics	0.07%
ADP	27	Technology	0.07%
FedEx	15	Logistics	0.04%
Bank of America	3	Finance	0.007%
Total	**40,906**		

INKY™

To put some context around these numbers, INKY processed 656,954,951 emails in 2020. In round numbers, that's two-thirds of a billion. Within this pool, our software found 4,874,096 phishing campaigns. Of those phishing campaigns, 591,293 of them were brand impersonations. Out of the brand-impersonation group, INKY found 40,906 unique campaigns, the total shown in Table 1. A single campaign is defined as being from the same sender domain and authentication source and having roughly the same text, links, and attachments.

One campaign can represent hundreds or even thousands of emails, which may be vanilla (only the recipient is varied) or dynamic (customized per target via clever software).

A drill-down into the top 10 shows Microsoft still in the lead by far, with other household names following at a distance (Figure 1).

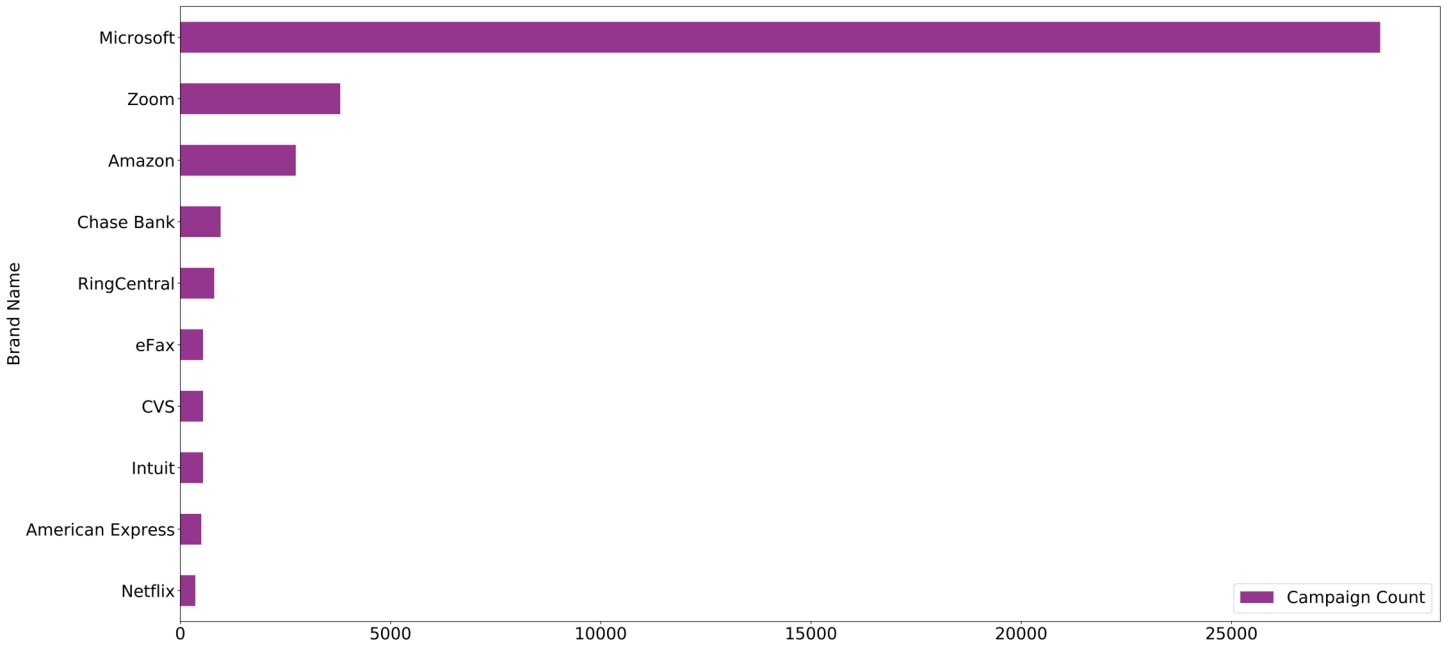


Figure 1

Sector Analysis.

A look at the domain-impersonation data by sector reveals Technology way in the lead, again virtue of Microsoft, with Telecommunications, Retail, Finance, and Logistics following in decreasing order (Figure 2).

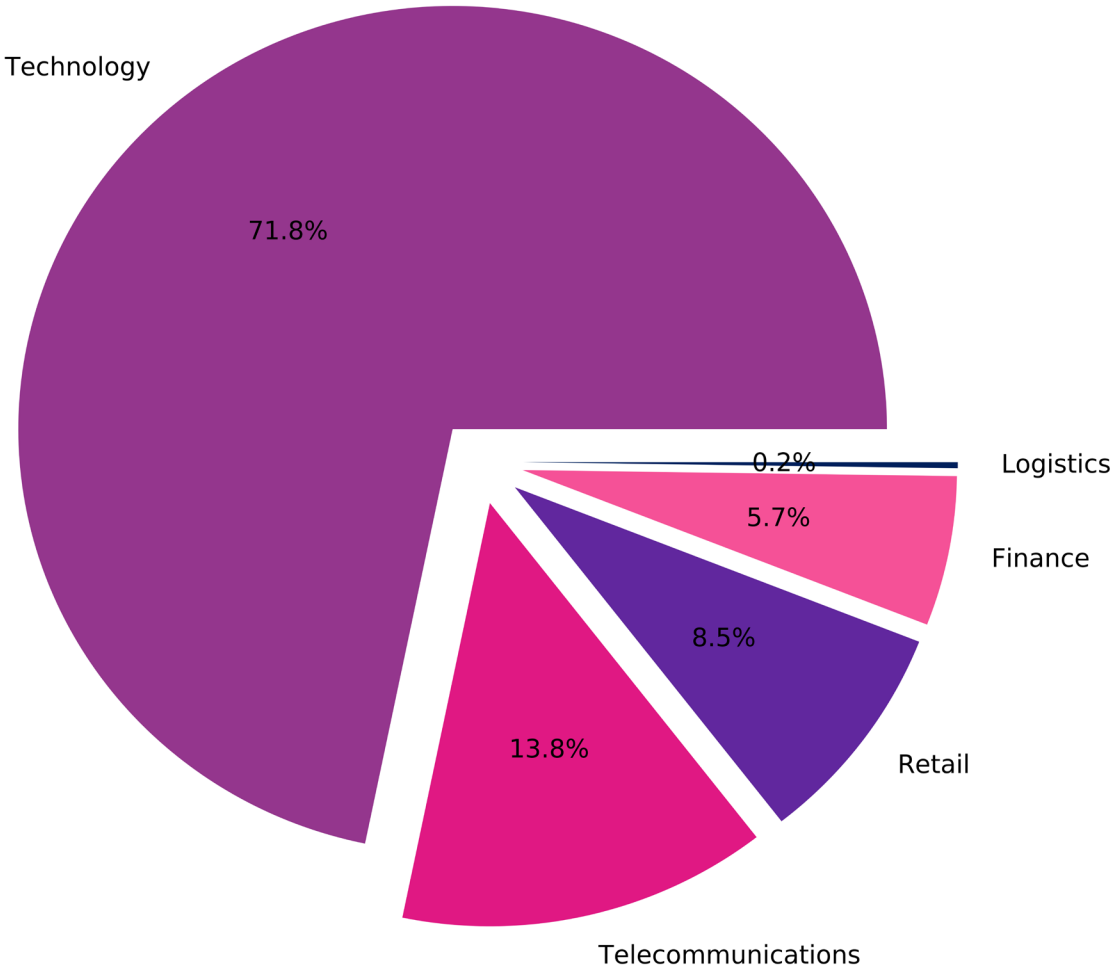


Figure 2

Technology.

Microsoft was by far the most impersonated brand in 2020. Microsoft credentials are extremely valuable for BEC attacks. Bad actors exfiltrate email data from compromised accounts to analyze and monitor buyer-supplier relationships. As they learn the details of an organization's supply chain, they lay in wait undetected for the perfect opportunity to intercept payments. Using stolen emails and data as context, they create look-alike domains or spoofed senders, tricking employees into sending money to the wrong recipient. Judging from the prevalence of Microsoft impersonations, it would not be too much of a stretch to assume that this is a great business.

One of the key methods used in this type of attack is to convince the recipient to "log in" to their account, where the login page is actually a credential harvesting site that convincingly mimics Microsoft (Figure 3). In screenshots throughout this report, company-specific and personal details have been obscured for privacy reasons.

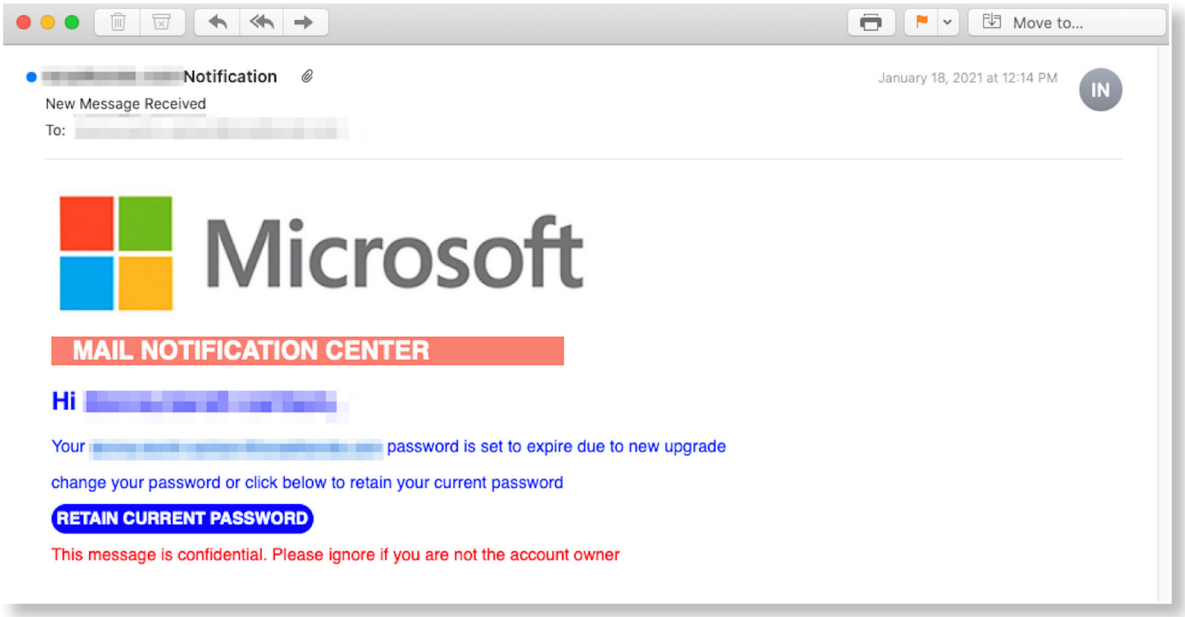


Figure 3

Other impersonated technology brands in the top 25 included, in descending order, Netflix, DocuSign, Dropbox, LinkedIn, Apple, Dropbox, and ADP. A tree map of these technology brands (minus Microsoft) shows the proportional representation of brand impersonations INKY caught in this sector in 2020 (Figure 4).

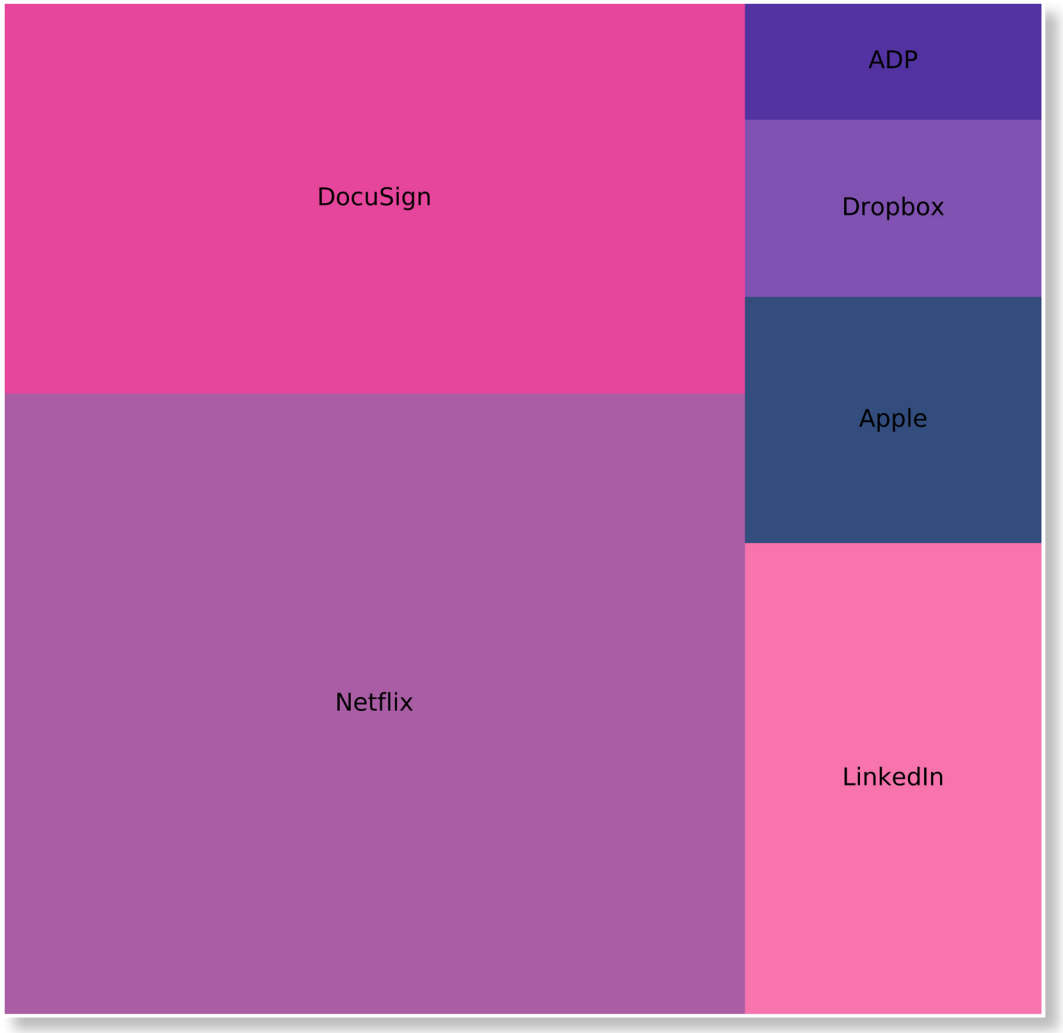


Figure 4

The second most-impersonated technology brand in 2020 was Netflix. People spent a lot of time at home, waiting out the pandemic while binge- or otherwise watching video entertainment on this most popular site. Naturally, the phishers were aware of this shift in behavior and targeted Netflix users as promising prey.

One type of attack aimed to harvest victims' bank credentials by asking them to update their billing information on a convincing-looking site (Figure 5).

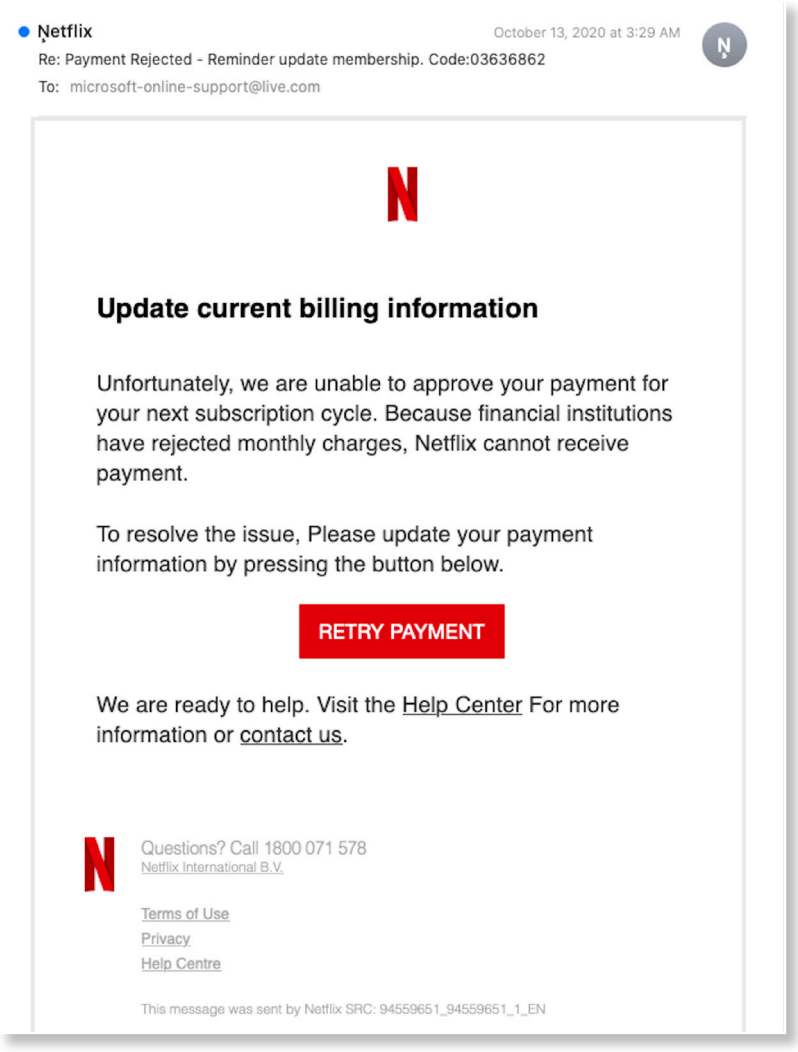


Figure 5

Next in frequency in the technology category was DocuSign. This electronic signature and digital transaction management company came into its own during the pandemic. The “wet” signature was the last piece of most transactions that had to be done in person, and DocuSign removed this final impediment to initiating, negoiating, and completing transactions remotely. As DocuSign grew in popularity, so did phishing attacks based on its highly recognizable branding elements (Figure 6).

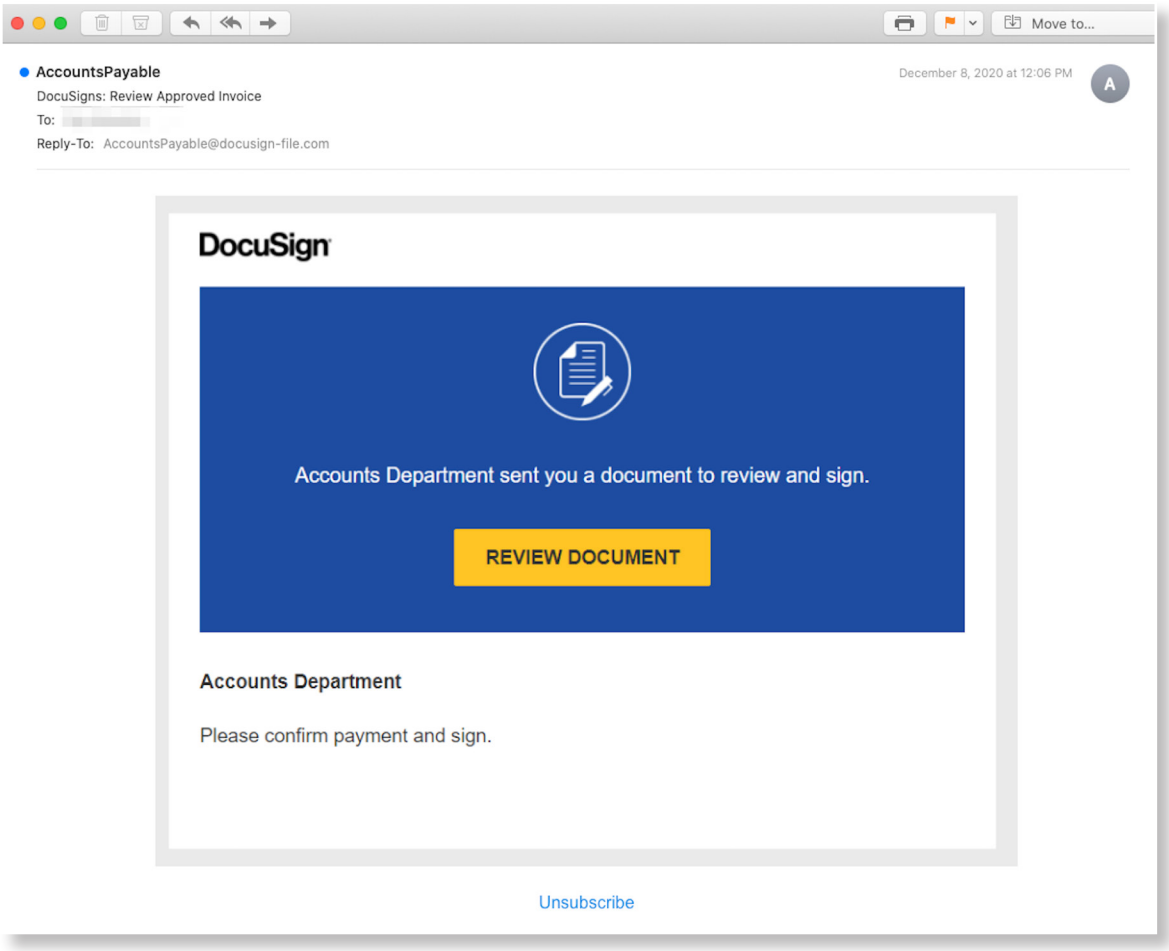


Figure 6

Telecommunications.

After technology, telecommunications was the second-most-impersonated sector in 2020 phishing attacks. Remote work, distance learning, and online socializing all drove people toward greater interaction with telecommunications brands for videoconferencing, online faxing, and VoIP. Of this group, Zoom was the most-impersonated, followed by RingCentral, eFax, Xerox, and AT&T (Figure 7).

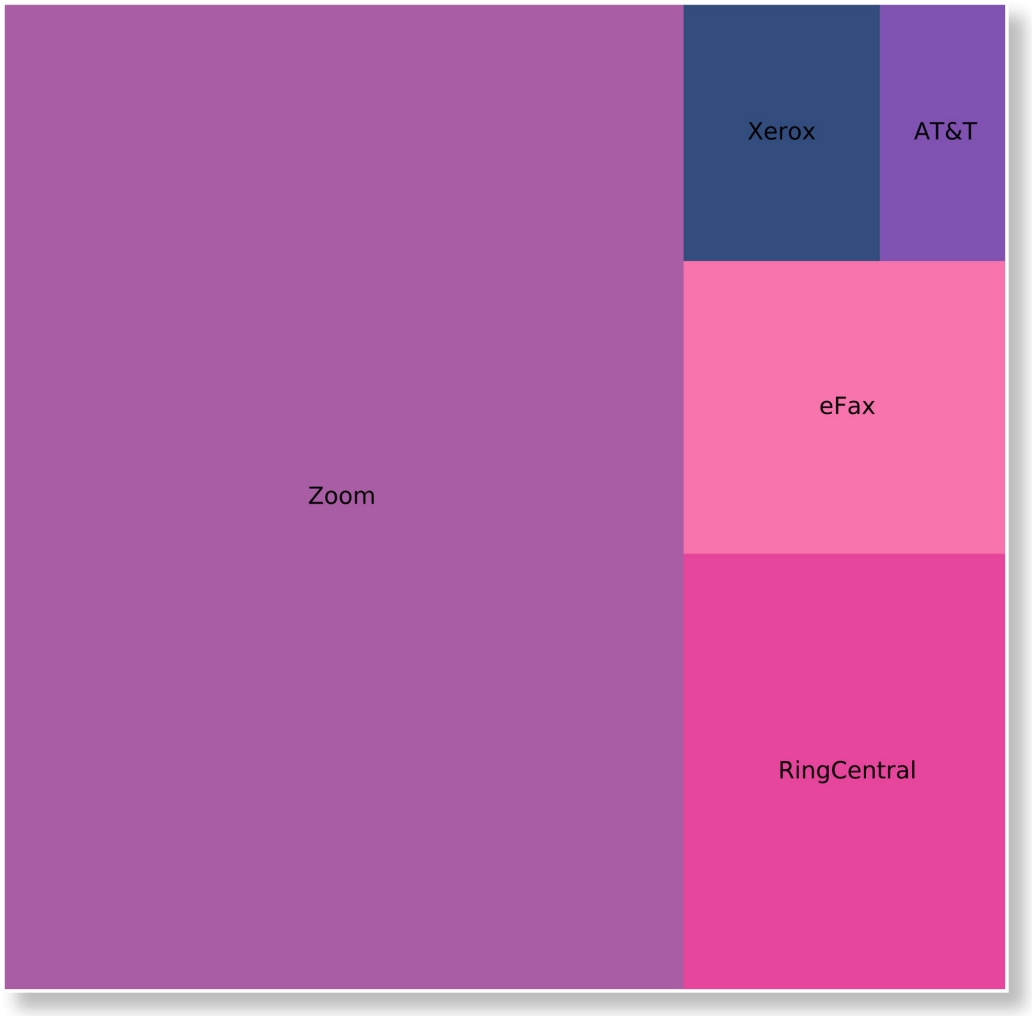


Figure 7

After technology, telecommunications was the second-most-impersonated sector in 2020 phishing attacks. Remote work, distance learning, and online socializing all drove people toward greater interaction with telecommunications brands for videoconferencing, online faxing, and VoIP. Of this group, Zoom was the most-impersonated, followed by RingCentral, eFax, Xerox, and AT&T (Figure 7).

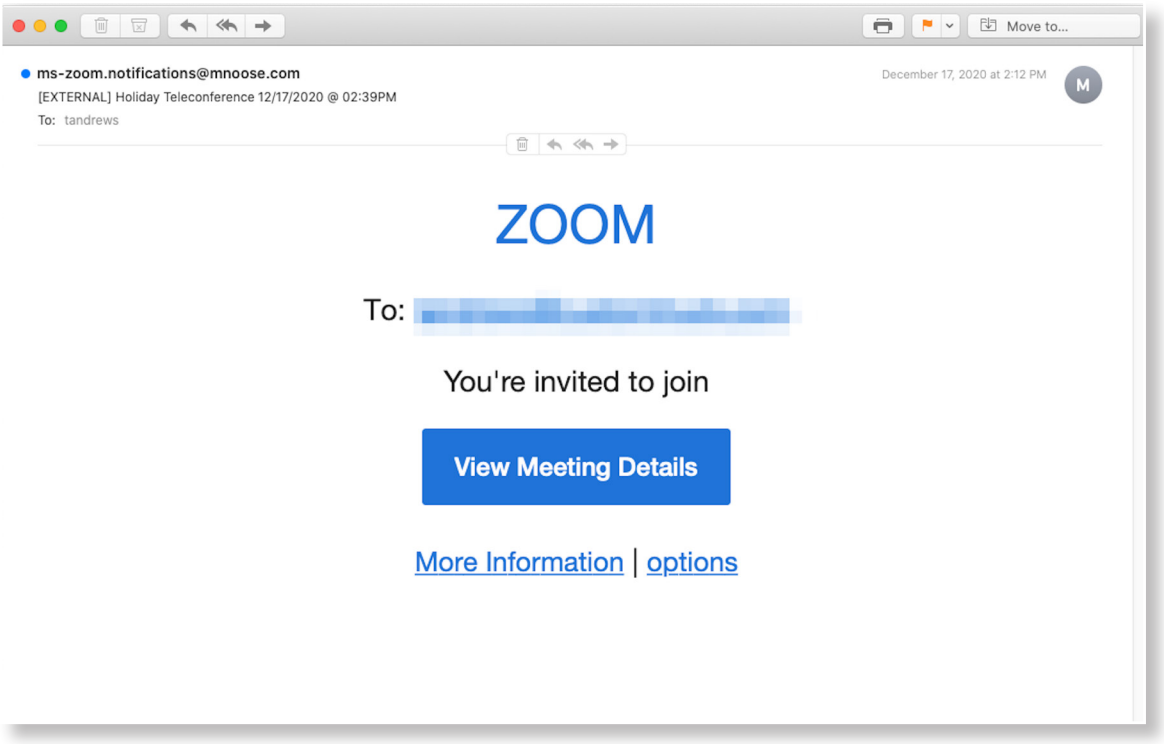


Figure 8

Another tactic phishers tried was sending a fake voicemail notification, purportedly from RingCentral (Figure 9). The cloud-based communications and collaboration company is well established among businesses of all sizes, many of which were coping most of the year with disrupted communications and anxious remote employees, any one of whom might become the perfect entry point for an attack against the larger organization.

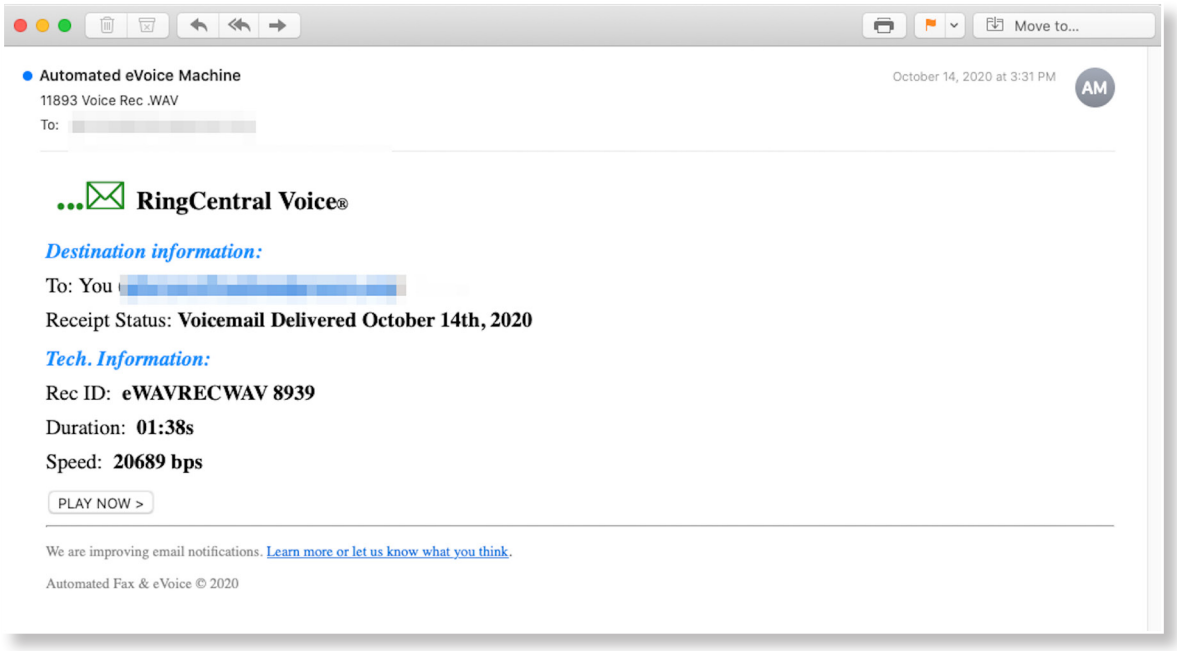


Figure 9

Although some of us might be forgiven for thinking that no one sends faxes anymore, in fact people do. Faxes are still the way some sectors do business and, while specialized terminals with heat paper are no longer in use, faxes sent from computers are fairly straightforward. INKY found more than 500 unique campaigns built around eFax, which offers an updated version of faxing with browser, app, and cloud components. A typical phishing attempt involved a branded eFax notification by email, inviting the recipient to click the big blue Preview Fax button (Figure 10)

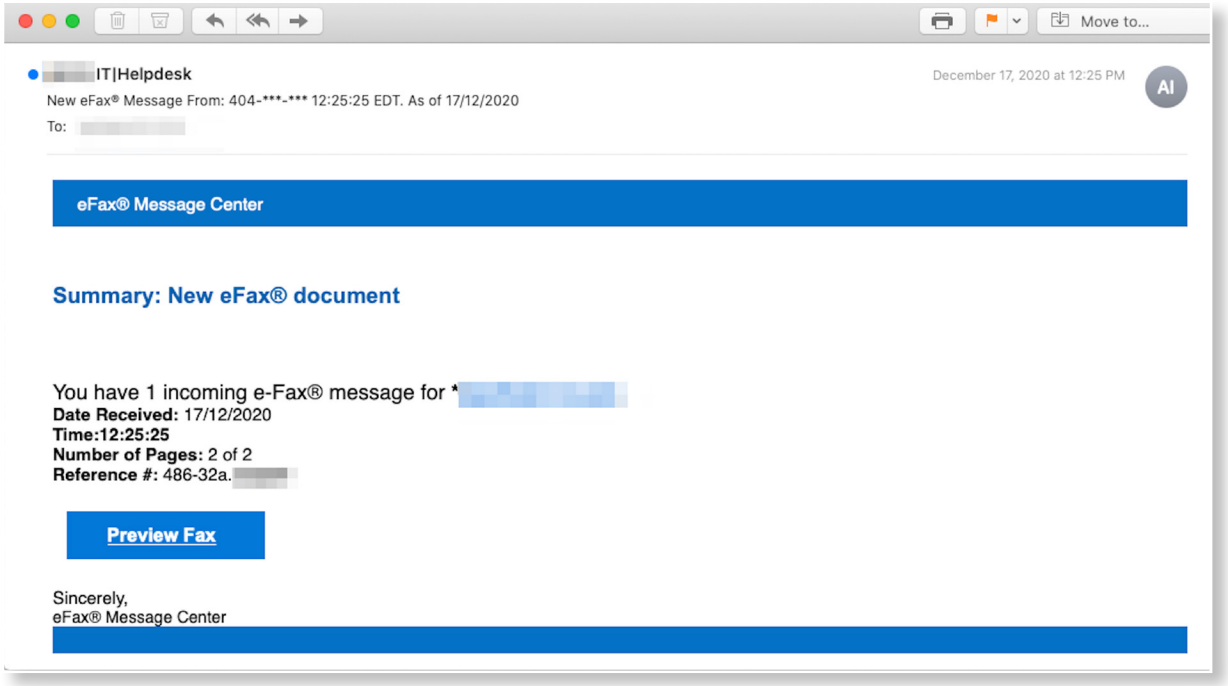


Figure 10

Retail.

In 2020, a lot of people turned to buying stuff online. Not too surprisingly, Amazon was both the largest beneficiary of this increased buying volume and phishers' favorite site to mimic in the retail sector (Figure 11).

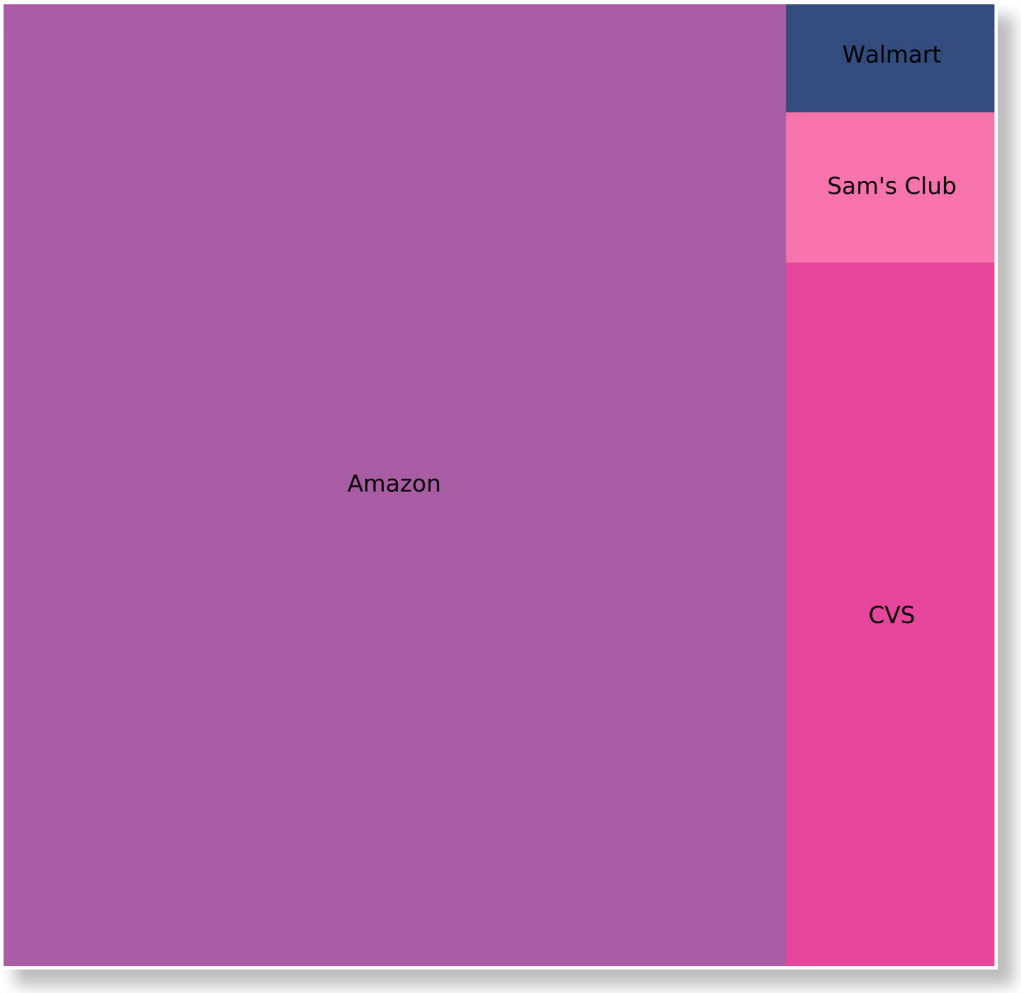


Figure 11

This good-looking impersonation of an Amazon shipment notification (Figure 12) is an example of a new wave of phish with no attachments or links. It simply offers a phone number, at the other end of which awaits, ready to ambush, a bad actor, who tries to get the victim to cough up login credentials and credit card information over the phone.

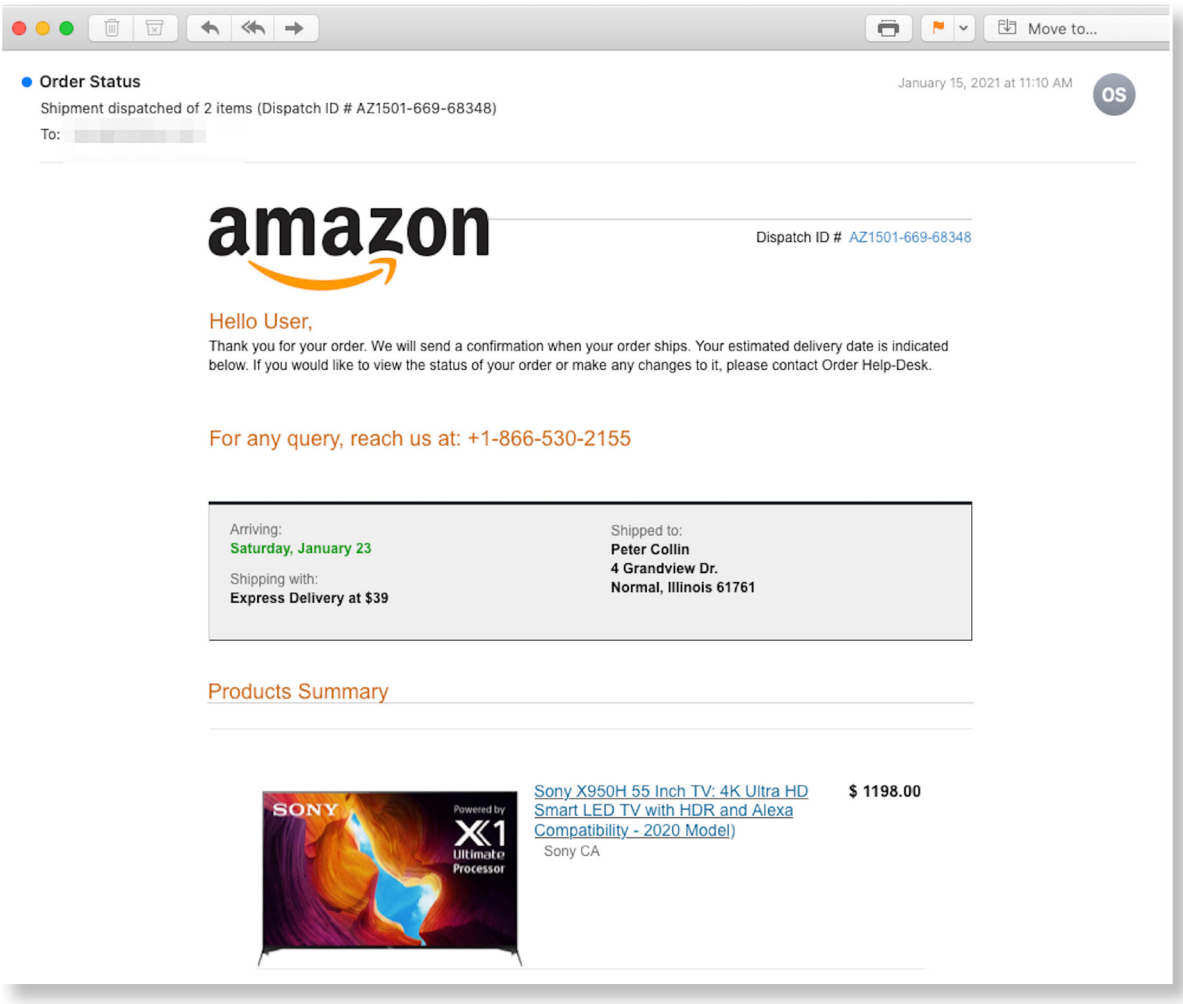


Figure 12

And, with illness and prevention thereof top of everyone's mind, online pharmacies were ripe for impersonation. Here's a fake CVS "survey" (Figure 13). The cynically malicious link here is the blue "We have a surprise for CVS Customers" text at the top. Boy, do they ever!

The link goes to a fake CVS survey site designed to harvest personal and credit card information. For taking the survey, the black hats promise a "free" gift, but, to receive it, the victim must pay for shipping. Once they collect the relevant personal and card details, they promptly don't send the gift, and the victim is out a lot more than shipping.

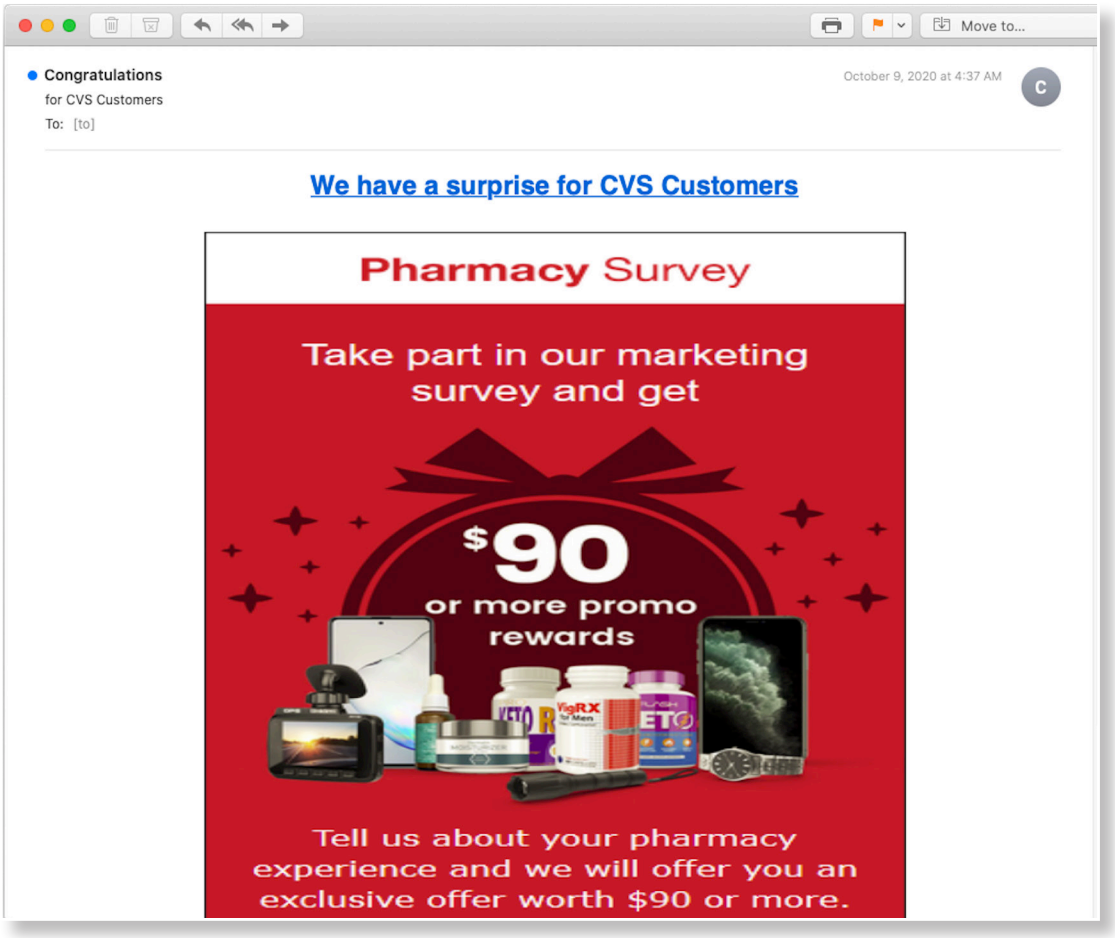


Figure 13

Finance.

And, of course, the “Willie Sutton rule” applies to phishers as well. He robbed banks because that’s where the money was, and they impersonate banks because that’s where the money is. Plenty of financial organizations, both traditional and cloud-native, made it into the top 25, including Chase Bank, Intuit, American Express, PayPal and Citibank (Figure 14)

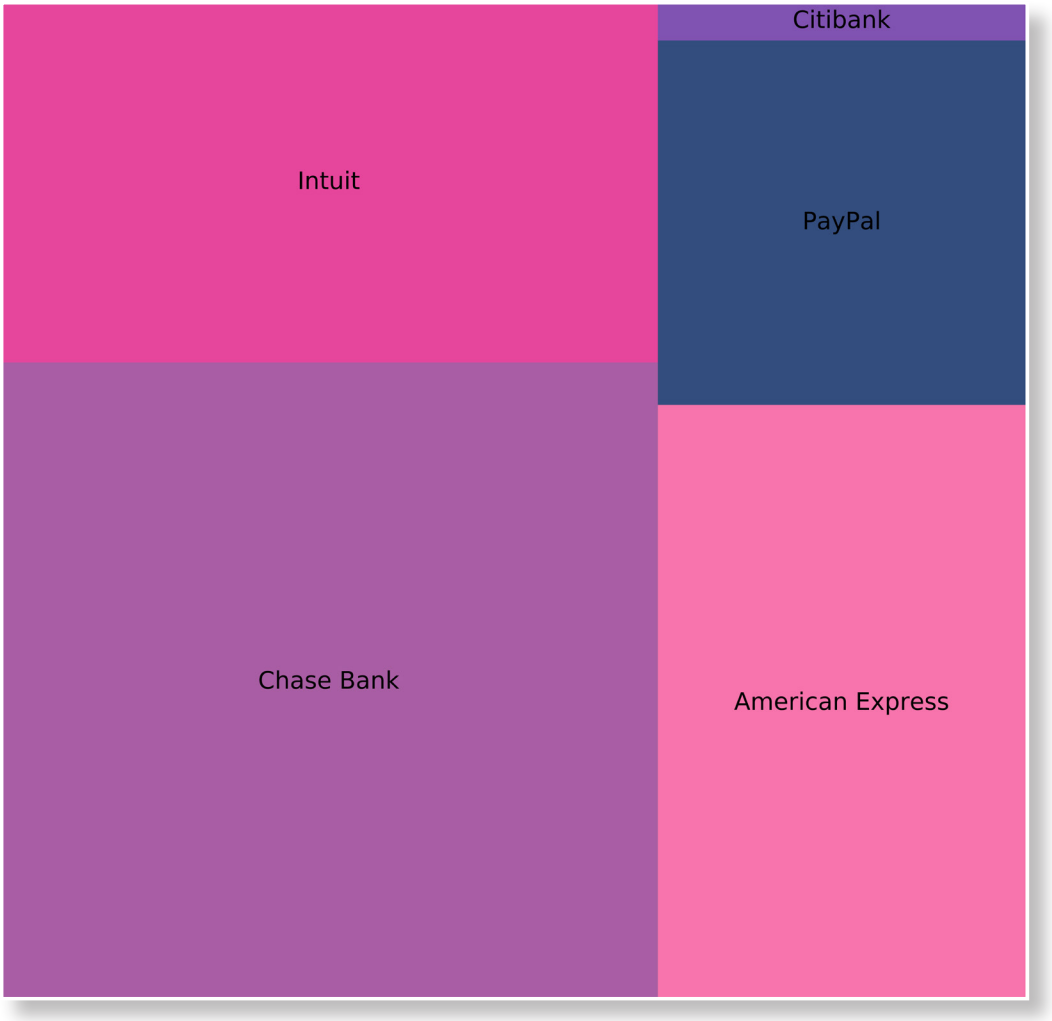


Figure 14

Chase Bank, the consumer division of JPMorgan Chase, has nearly 5,000 branches and 16,000 automated teller machines (ATMs) in the United States. With more than $2 trillion in deposits and almost $3 trillion in assets, the bank serves nearly half of the country's households. Thus, it is not at all surprising to find Chase was the most impersonated of the financials in 2020 (Figure 15). The casual reader might not notice that the sender is "No Sender," but the logo and other branding elements look about right.

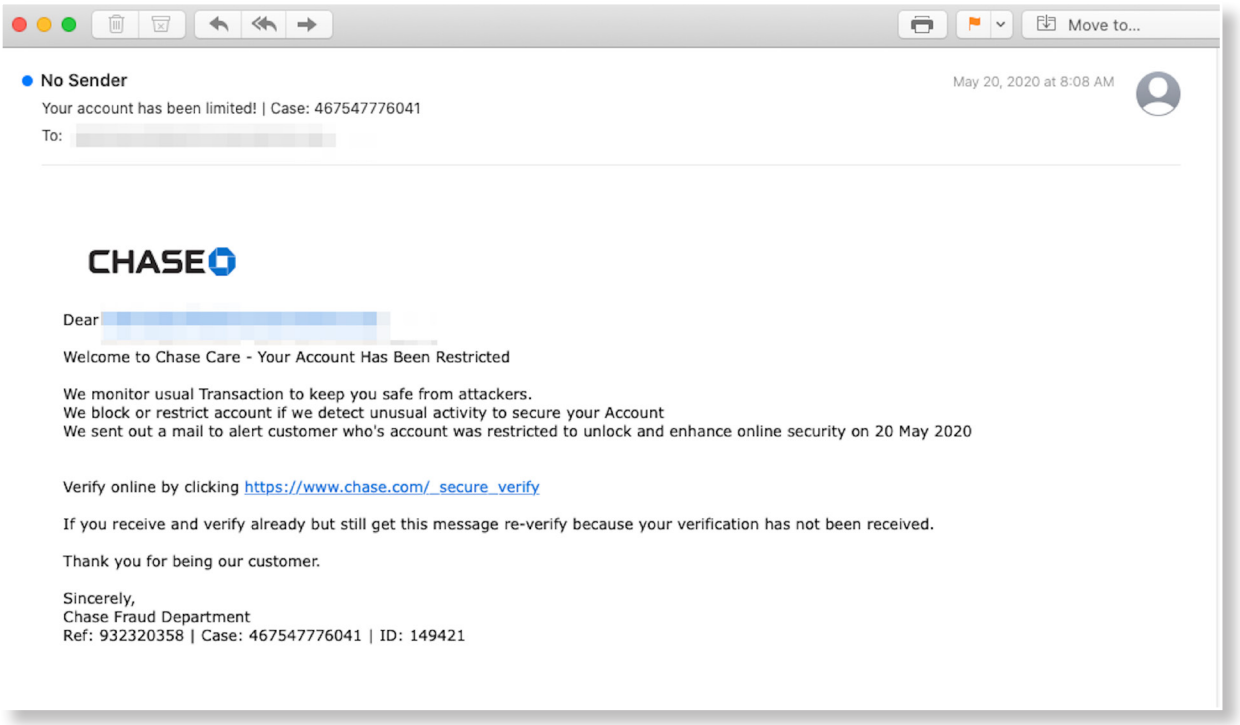


Figure 15

Right after the big retail bank, the next most impersonated financial firm in 2020 was Intuit, a fully cloud native service. Intuit's main product, QuickBooks Online, has made accounting easier for a vast array of businesses. With 200,000 professional accountants linked via QuickBooks to 2 million customers worldwide, there could hardly be a more perfect hole to phish in. Here's a notice from a generic "Accounts Payable Executive," who seems to think you owe $1,700 (Figure 16). But don't touch that big black "Pay Invoice" button! You'll be plucked clean on a credential-harvesting site.

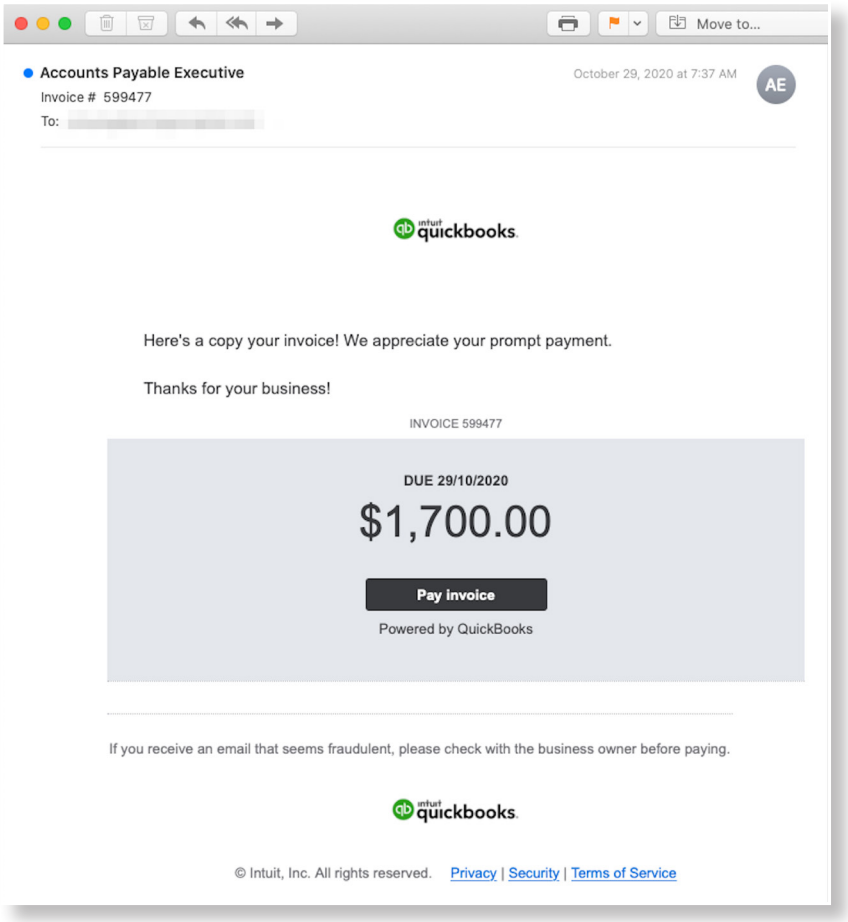


Figure 16

American Express is a classy bank, if not quite among the very largest in the United States. Nonetheless, its old-timey fiduciary vibe tends to calm potentially nervous customers. It was founded in 1850 and has adapted to changing times enough to remain a solid name in banking. Which makes it a lovely brand for an impersonation that funnels all that trust into a credential harvesting scheme (Figure 17).

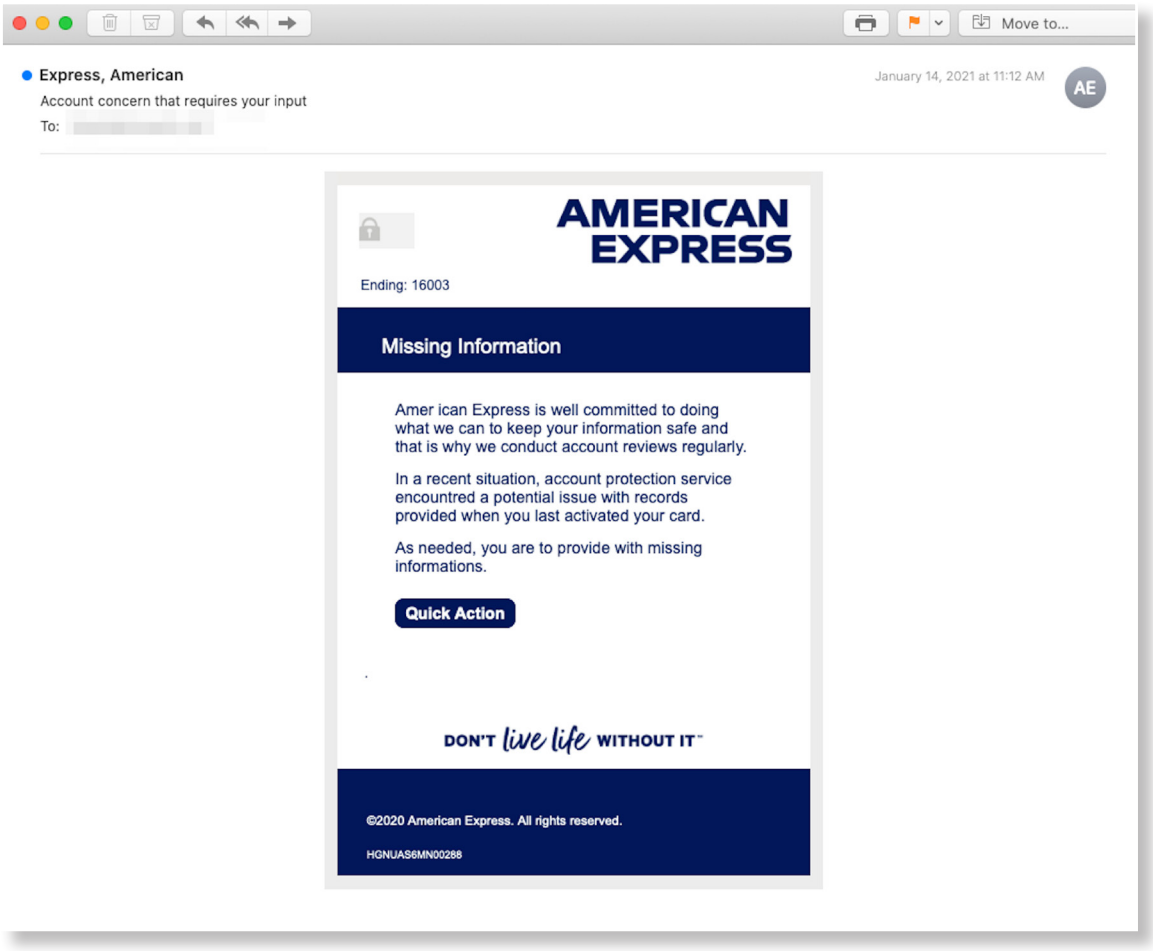


Figure 17

Logistics.

The other side of eCommerce is logistics, and, in fact, Amazon is a giant in both. But the dedicated logistics companies also saw a tremendous rise in shipping activity as the pandemic settled over the country in 2020. Everyone who bought something online had it delivered someplace, mostly to their homes. The top three logistics companies impersonated during the year were the U.S. Post Office, DHL, and FedEx (Figure 18).

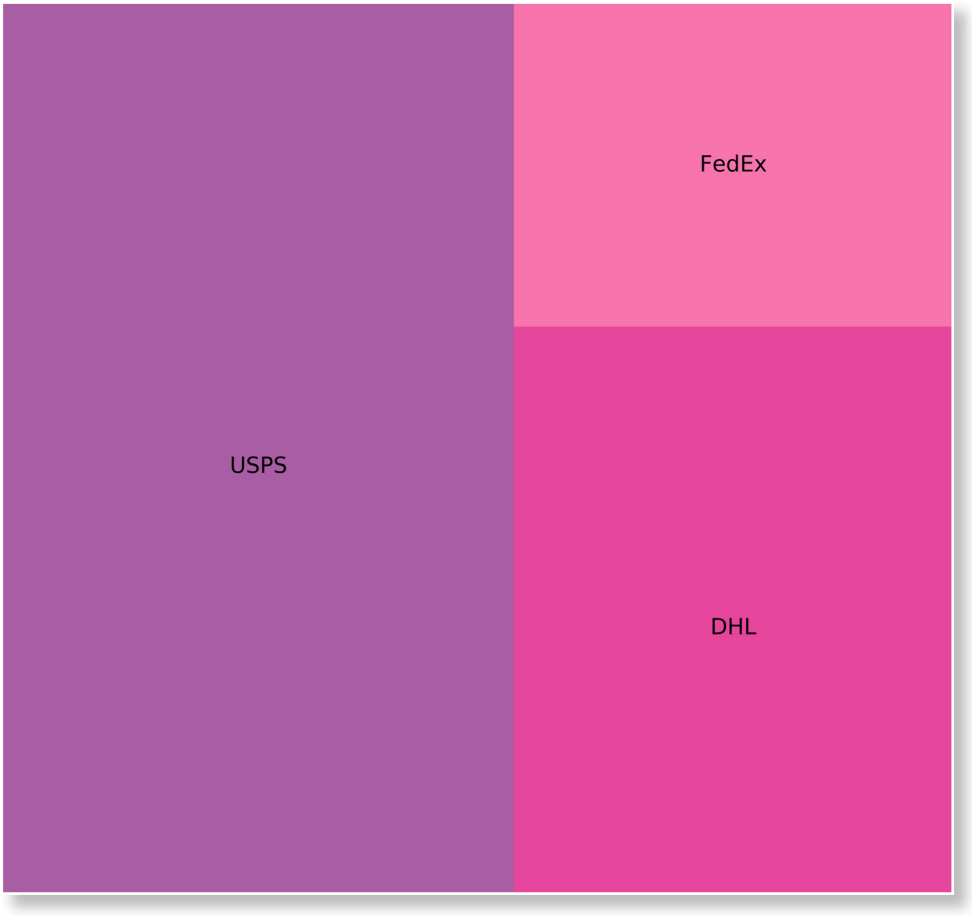


Figure 18

This U.S. Post Office impersonation is interesting in that it uses confusable text — or homographs, as the pros call them (Figure 19). Note the link address in the big white button. The domain, instead of being **`www.usps.com`** is **`www.uspŝ.com`**, a subtle difference, perhaps, but one that could take the recipient anywhere. For good measure, the hacker has made the word "address" in the URL "addre55," perhaps to fool any pattern-matching software that might be looking for keywords.

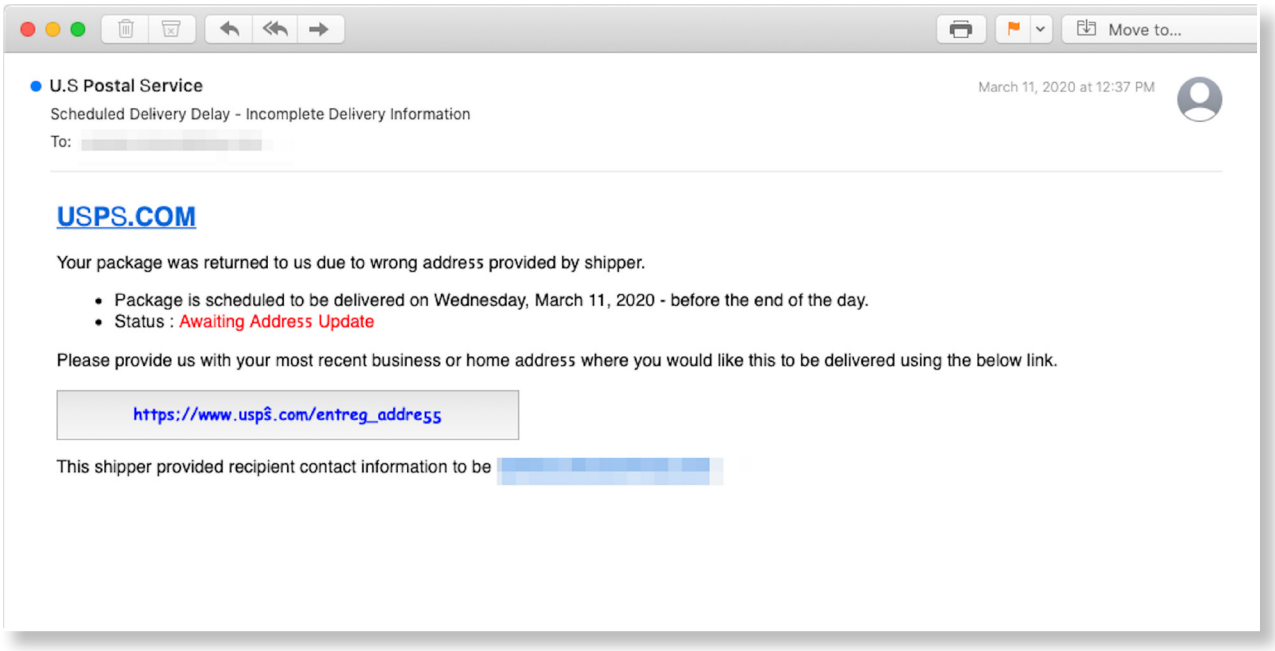


Figure 19

Although DHL is only one-tenth the size of FedEx, the German shipping company was spoofed far more often in 2020, with almost double the number of unique phishing campaigns. As with many of these attempts, this one has a note of urgency about it: take some action quickly (click the button) to avert a bad outcome (having the package returned or "abandoned"). Perhaps DHL is more popular among phishers because the company's actual branding elements are the alarming colors of red and yellow, increasing the sense that emergency action is required (Figure 20).

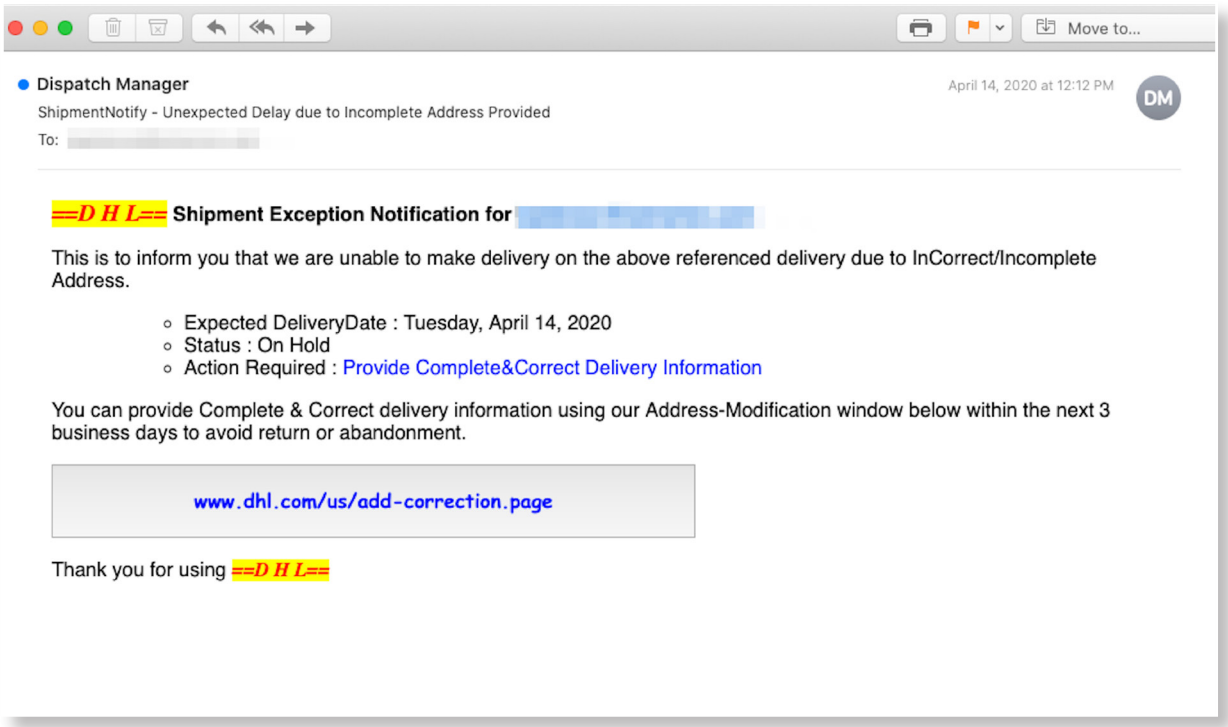


Figure 20

Another emergency of a similar sort, this FedEx impersonation informs the recipient that their address is “invalid” (Figure 21). If the recipient tries to open the attachment, the supposed “address form” to correct their address, malware is launched that contains a key-logger, ransomware, or a remote-access-tool installer.

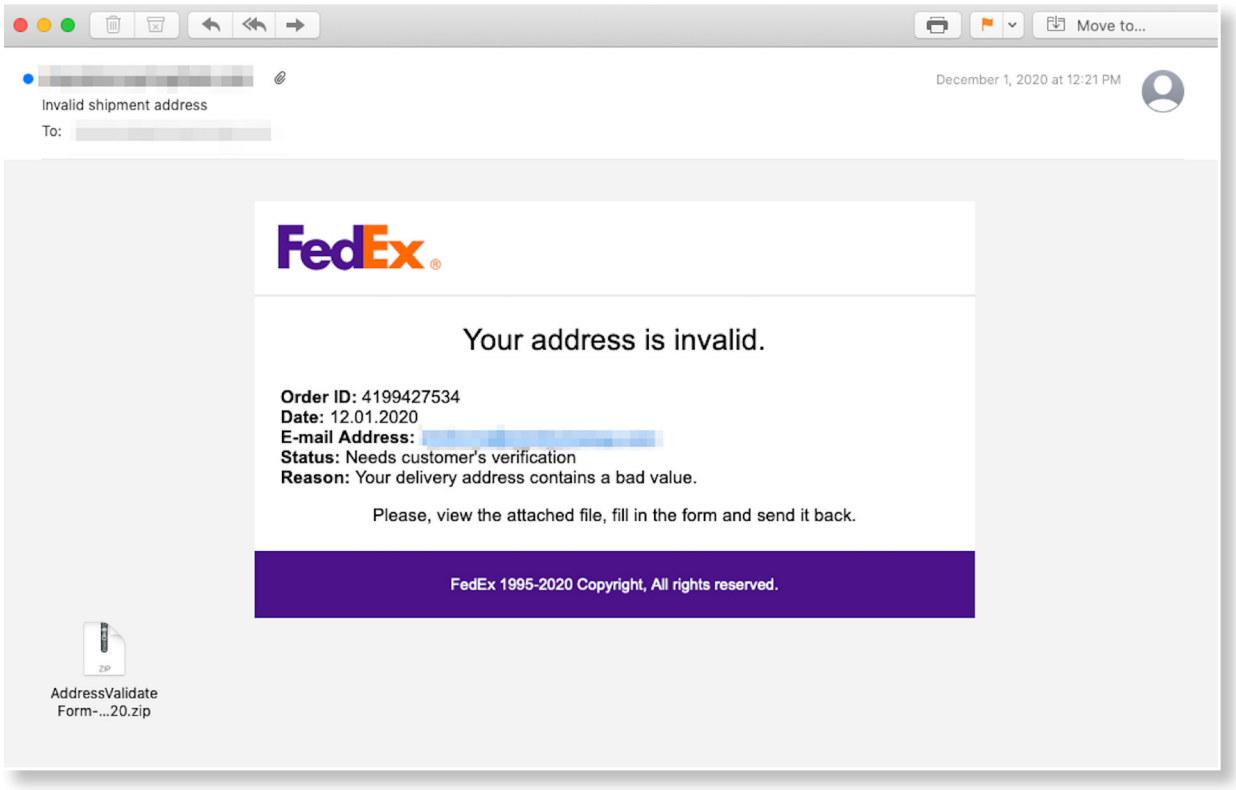


Figure 21

INKY™

Sticking With the Phish You Know Doesn't Work.

In 2020, phishing attacks geared up dramatically, driven by the social disruption stirred up during the pandemic. These attacks came from many angles, all probing at technical weaknesses in the infrastructure and blind spots in the human mind. At a high level, the nature of these phishing attempts and successful exploits was predictable. Phishers aimed at areas of both great importance and high anxiety: undelivered packages, missing payments, health information updates, meeting notices, social invitations.

But many of these assays were never seen before. Most anti-phishing products on the market today rely on some sort of Bayesian analysis; that is, on a model of the threat landscape based on prior examples, adjusted as new examples come in. These products can find a phish similar to ones they've already seen.

But since INKY assesses email based on first principles, it catches phish no one has ever seen. It's not enough to match a potential phish against others in a known pool, most importantly, because the difference between a real email from Microsoft and the most realistic-looking impersonation is vanishingly small. Matching the latter against the known pool will yield a false negative. That is, the mail was tagged "not a phish" wrongly.

INKY examining an email doesn't care whether it looks like anything known. It only cares whether what the mail purports to be (a notice from Microsoft about passwords) matches with what it is (a beautiful HTML document sent from a machine shop in Kazakhstan).

Why INKY?

INKY provides the most comprehensive malware and email phishing protection available. To see INKY's anti-phishing solution in action, request a demo. Let us show you what a difference it can make.

INKY Phish Fence uses a proprietary blend of Machine Learning and Artificial Intelligence that blocks even the most sophisticated phishing attacks that get past other systems.

INKY Phish Fence uses proprietary technology and algorithms to "see" each email as the recipient would. Unlike a person, however, it can detect an email forgery and/or malicious or suspicious content. Once detected, it can redirect the email to a quarantine area or deliver it with disabled links and warnings.

Alerts show within the email itself, which allows it to be viewed on desktop or mobile. This is a significant difference from other systems, which display warnings in headers and may not render properly in mobile applications.

INKY Phish Fence sits on top of any email system, including Microsoft Office 365 and Google Suite.

INKY Phish Fence scans every sent and delivered email automatically and flags malicious emails.

A comprehensive dashboard allows admins to see both the bigger pictures and to drill down to specific attacks, individuals, and individual messages. A robust search allows for detailed reporting at the granular level.

It can be set up and ready to go in just a few hours.

We're passionate about email.

Ready to talk about an issue you're facing with email security at your organization?

www.inky.com