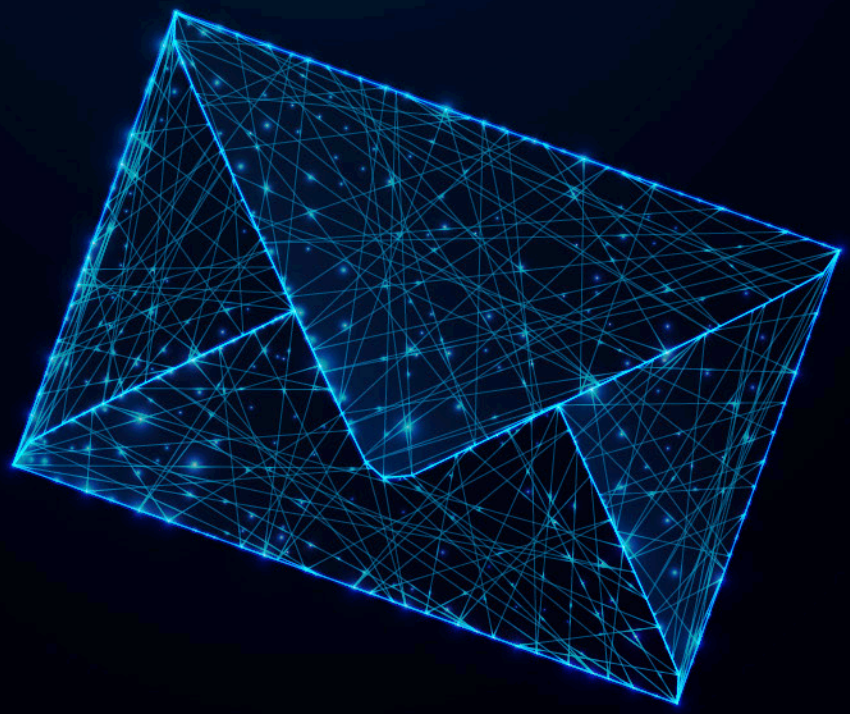
REPORT

INKY 2020

End of Year Phishing Report

An analysis and assessment of customer-reported phishing experiences. How attackers took advantage of the many disruptions to normal life, and how INKY defended against them. What to expect in the next year and decade as phishing technology and practices and their countermeasures become more sophisticated.



Introduction

Now that 2020 has closed out, I think we can safely say it was a banner year for the phishing industry. In some ways, the environment was perfect for nurturing phishing attacks: people were isolated by COVID-19 for much of the year, and they were dealing with unfamiliar situations, fear, and uncertainty. And they were more than ever reliant upon the infrastructure of the Internet, particularly email.

Email has been a lifeline, along with Zoom and various news sources, and so it is not surprising that the bad guys crafted throughout the year specialized attacks that keyed off important and anxiety-producing events in the news headlines: shutdown announcements, stimulus check updates, election news, and even Zoom invitations.

Between COVID-19, stimulus packages, remote work policies, unemployment benefits, and school statuses, there were plenty of themes for the hackers to choose from. People — impatiently sitting at home wondering what in the world could be next — craved information on all these topics, making them unusually susceptible to forged-brand attacks, account takeovers, and other forms of phishing. These attack emails appeared to come from reputable sources, such as government departments, public health organizations, and well-known corporations.

And once phished, work-from-home employees became wide-open attack vectors for black hats aiming at the digital assets of corporations, government at all levels, and non-profit institutions.

Phishing is not like spam. Vendors promising to catch 90% of phish, or even 99%, fail to recognize that the most convincing phish get through. The most sophisticated perpetrators — often state actors or well financed crime groups — are the best at choosing targets and crafting attacks. The most difficult to detect phish are also the most dangerous.

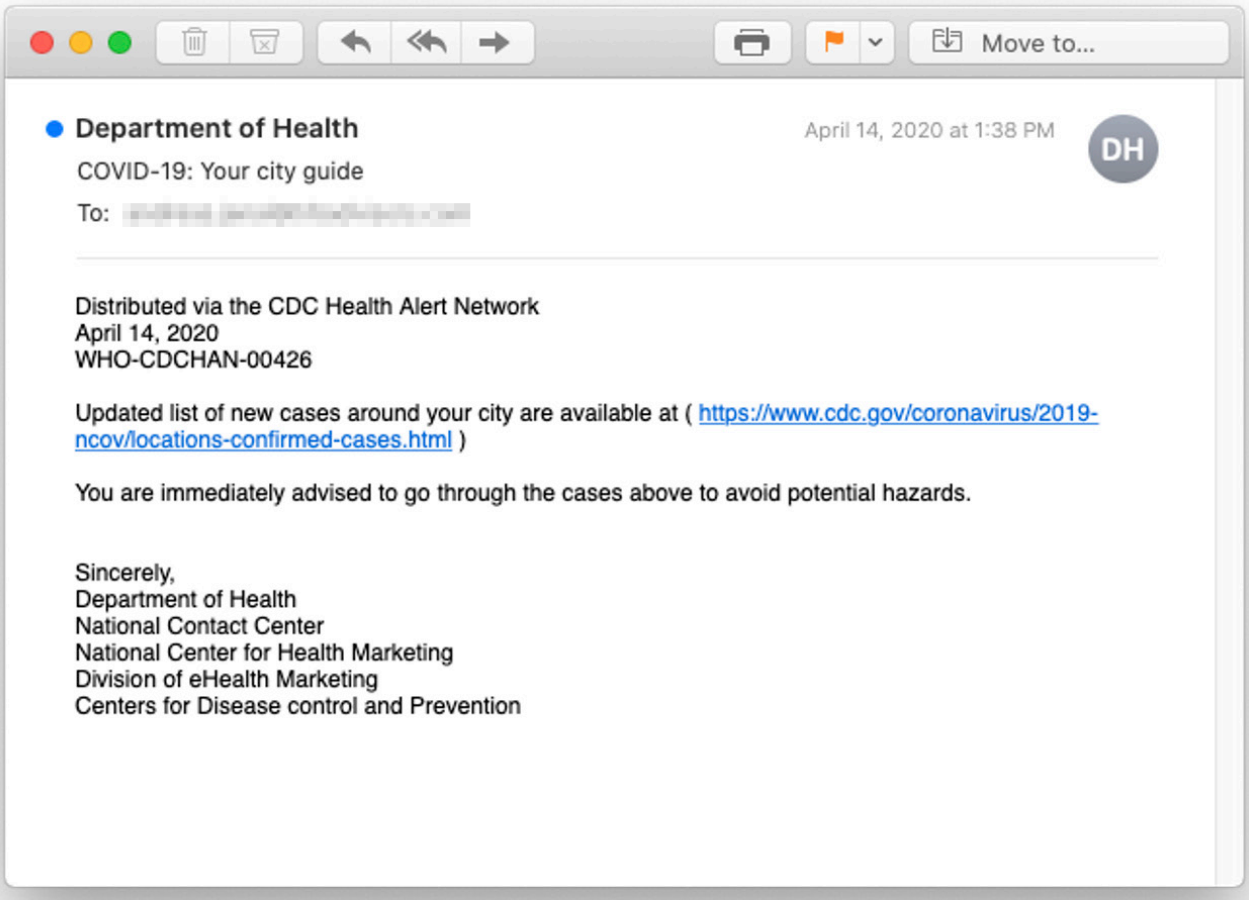
Deploying advanced anti-phishing technology against this changing threat landscape throughout the year, INKY Phish Fence caught a number of phish that others missed.

COVID-19

There were so many phishing attacks based on the COVID-19 threat in 2020 that they are nearly impossible to count. It's fair to say, a COVID-19 message was behind many phishing assays, even when they were built primarily around other themes. Several examples follow here.

This one, sent April 14, soon after the pandemic started, looks innocent enough: an email from the "Department of Health." A close examination might clue the astute reader to the fact that the huge address block contains a small error. The author seems to have missed the upper-case "C" in "Centers for Disease Control and Prevention." But otherwise, it looks like a perfectly fine alert from CDC about "new cases" of the disease in "your city."

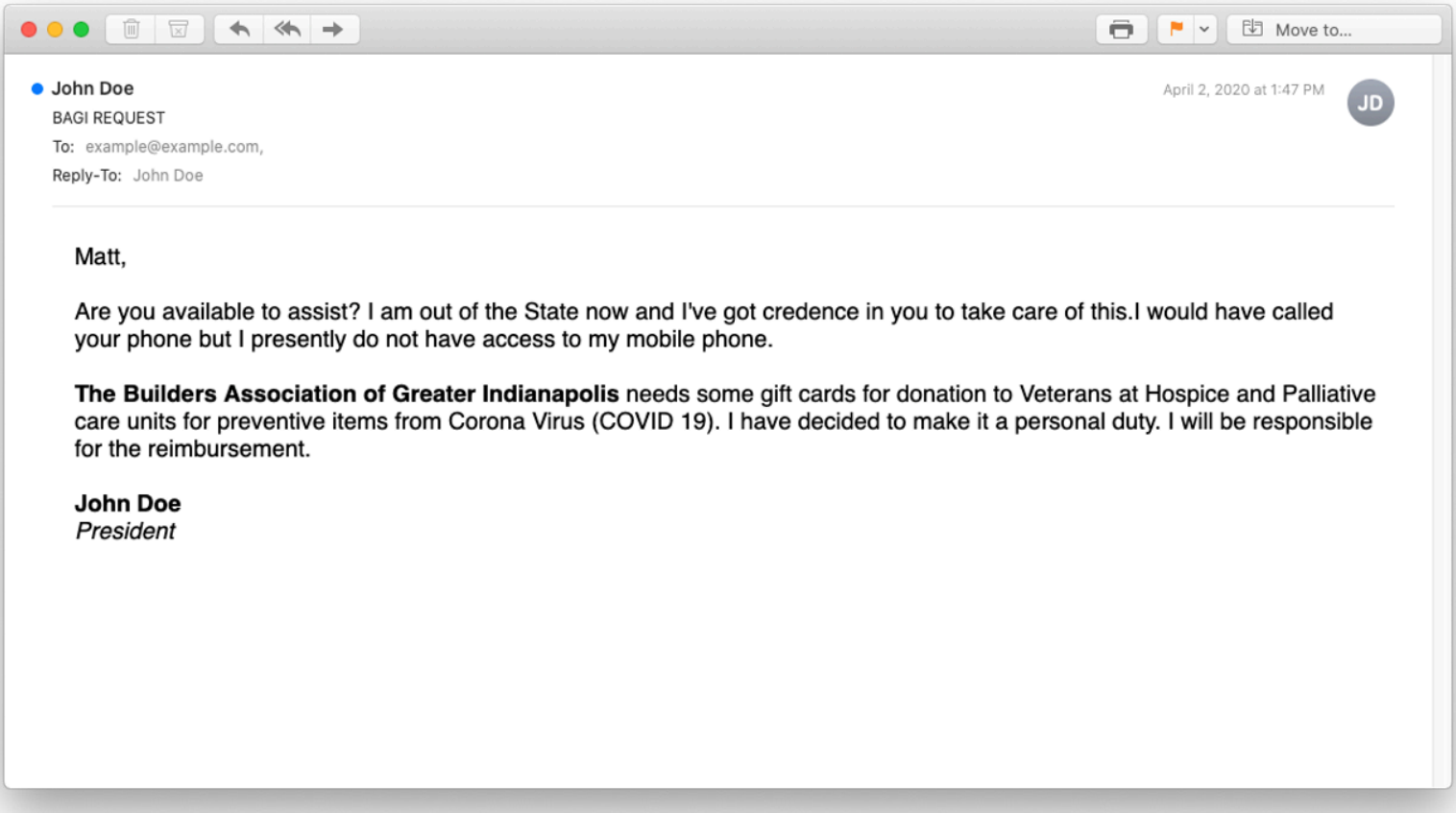
An anxious recipient could easily click on that link, which appears to lead to a real CDC site. Although the HTML <a> tag indicates a CDC site, the underlying code sent the recipient to a credential harvesting site, which presented a beautiful-looking Microsoft Office 365 log-in.



Although this next one has a COVID-19 angle (because why not?), it is mostly a CEO impersonation. INKY caught it on April 2 with its VIP list, a set of names of top executives in a company who might be spoofed to employees.

In the message, John Doe, the CEO, appears to be outside the usual communication sphere and is asking for gift cards for a worthy charitable cause. Even for the careful eye, there are few things wrong with it. “State” is spelled with an upper case. But, other than the strange request itself, there’s nothing off with this note. The sender’s address appears to be the real CEO’s email.

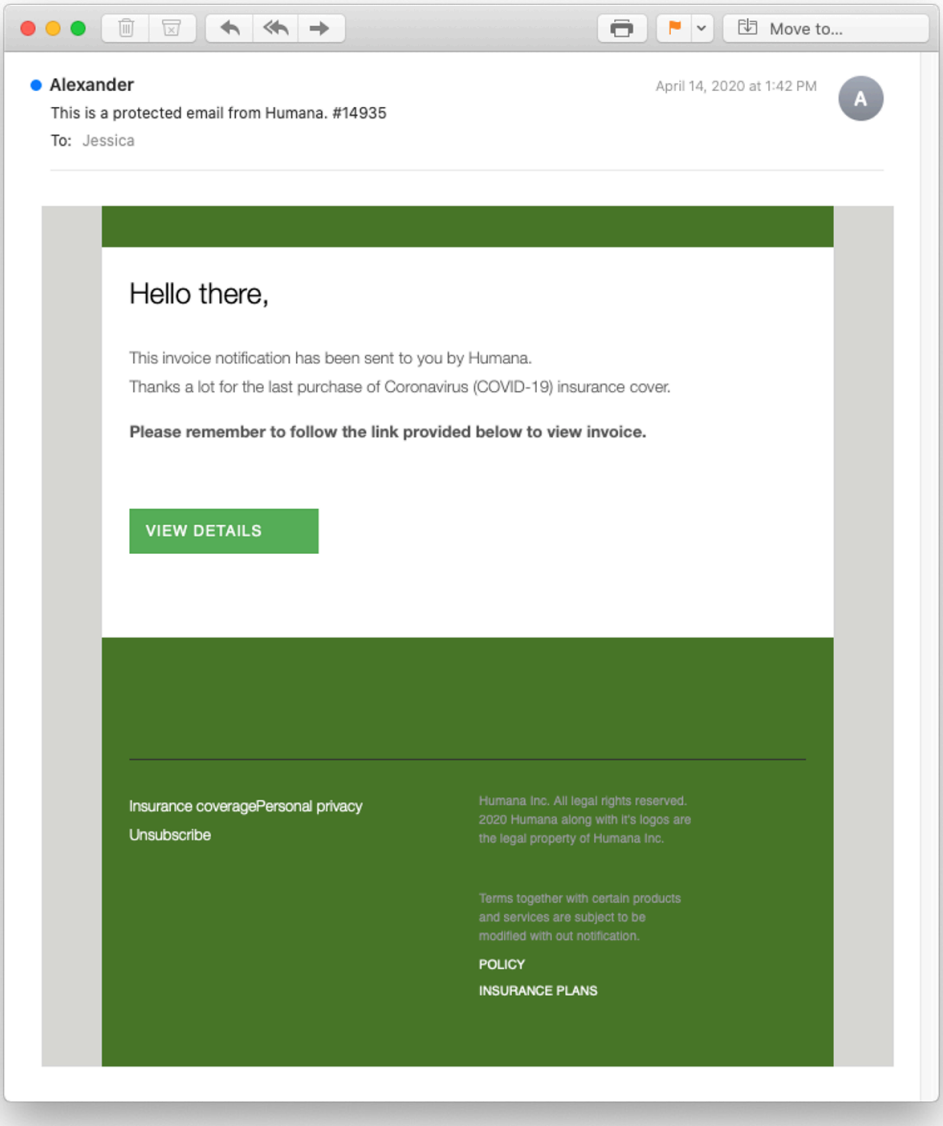
In practice, when the INKY team onboards a new customer, an admin can upload a VIP list as a spreadsheet with first and last names and email addresses of anyone who might be a spear-phishing target (e.g., the CEO, the CFO, finance department staff, the CIO).



One more COVID-19 phish, and we'll move on.

This one appears to be from Humana, a well-known insurance company based in Louisville, Kentucky. But it really came from Russia. If you happen to speak Russian, you might notice certain phrases like "... to view invoice." The Russian language has no articles (i.e., "a" and "the"). A native speaker might not know that in English we would say "... to view the invoice."

But other than that, there are few clues as to how poisonous this email really is. If the recipient were to click on the inviting green button that says "VIEW DETAILS" they would be directed to an apparently legit O365 login page, which is actually a credential harvesting site.



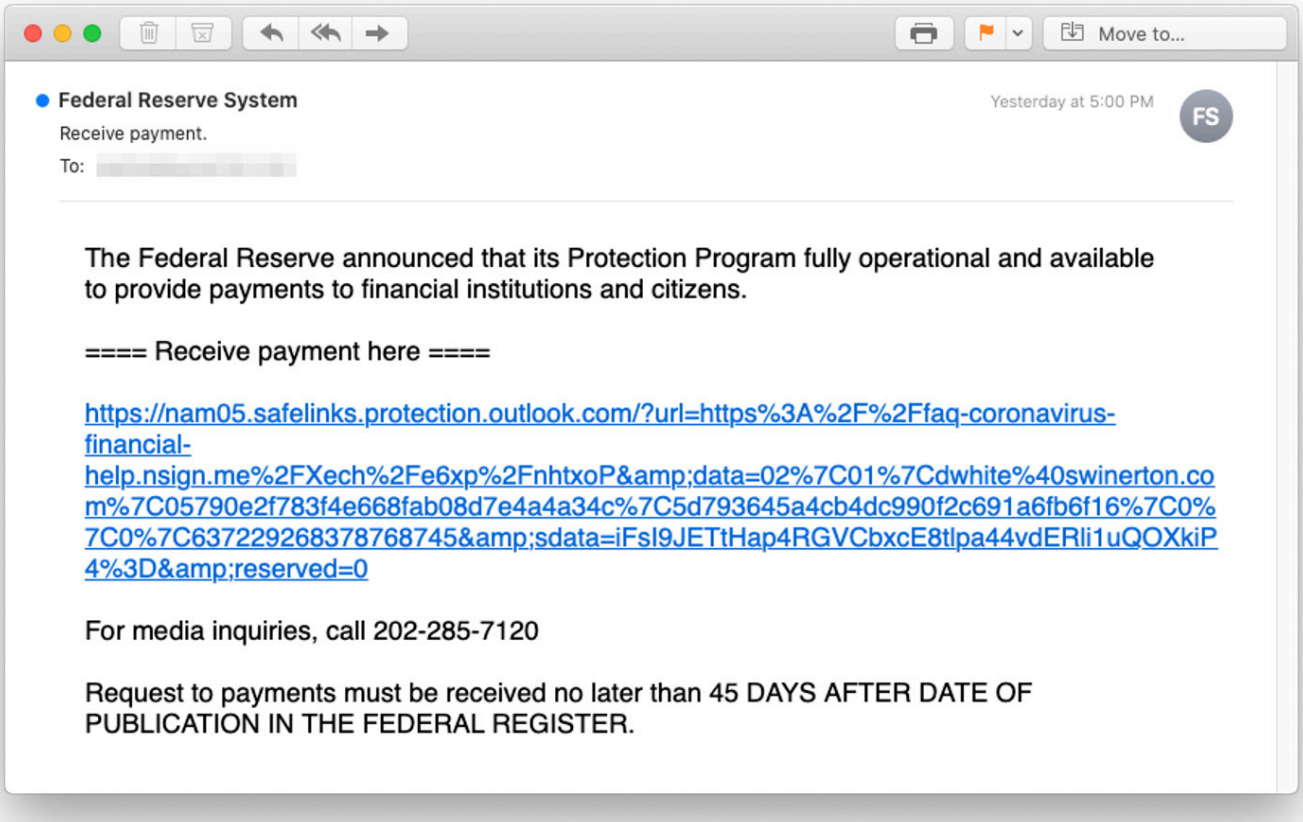
The target, Jessica, is an employee of a firm INKY was protecting with Phish Fence. This email got past all other measures the customer had in place.

Another fruitful area of phish-foolery in 2020 was centered around stimulus payments. Many people skated through 2020 on financial thin ice and perhaps even lost sleep at night wondering whether and when the government would send back some of their hard-earned tax money in the form of stimulus checks.

Given the anxiety around this issue, phishers gravitated toward strategies that would prey on people's hope that the bailout cavalry would arrive in the nick of time, just before their eviction, layoff, or repossession notice hit the mailbox.

Here's an example INKY Phish Fence snagged April 19. A customer reported it through the reporting tool.

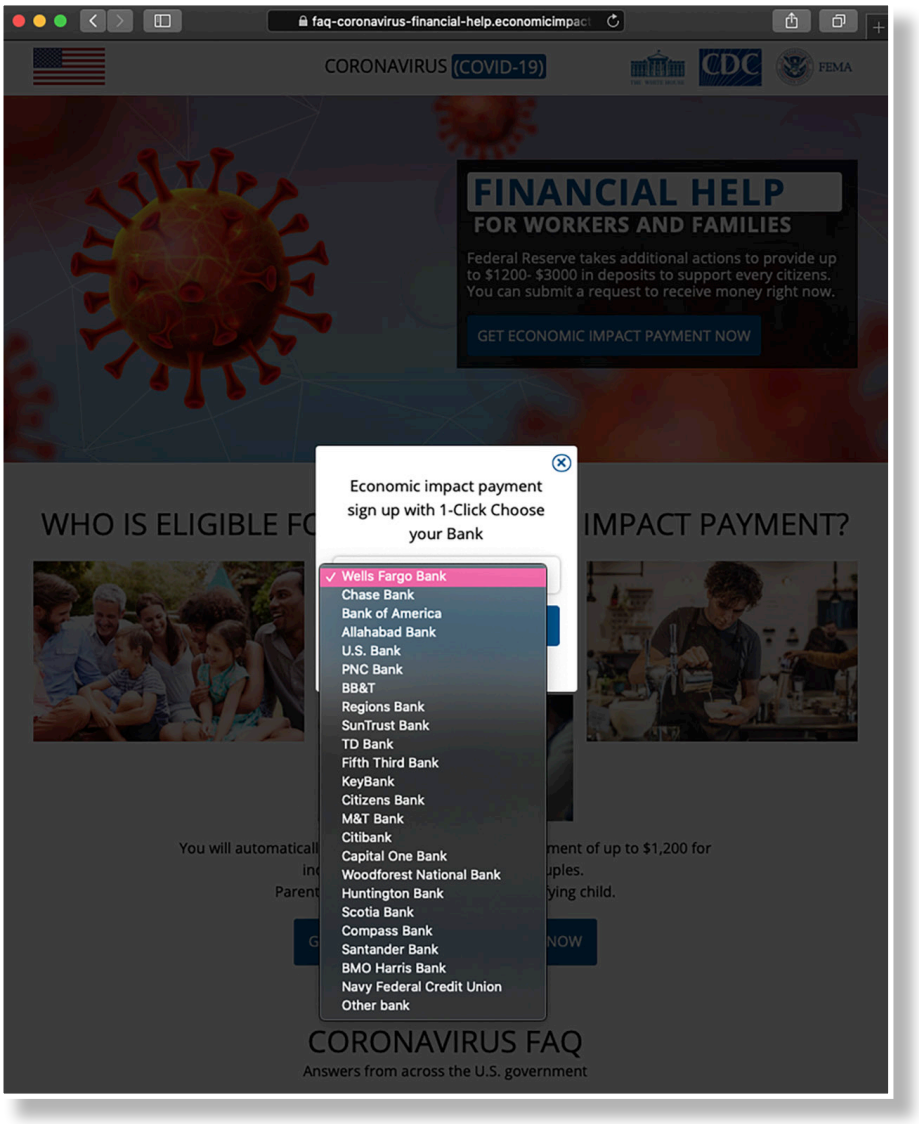
The message appears to come from the Federal Reserve System, which is what's shown in the display address. Never mind that the Fed is not the organization in charge of stimulus payments. That's Treasury (i.e., the Internal Revenue Service or IRS). But people in a state of high anxiety might not know that little fact or be willing to overlook it simply because they want so badly to will that payment into being.



Drilling down a bit, The malicious link in the email leads to **`https://faq-coronavirus-financial-help.economicimpactpayment.site/`** which might sound fine, but it turns out that the domain **`Economicimpactpayment.site`** was created with Namecheap, a "budget hosting provider" based in Phoenix, AZ, on April 16, 2020 — just days before it was put into service. This site was not created by some ancient, venerable government institution. It was only a shallow storefront set up for phishing purposes.

In addition to impersonating the U.S. government and offering fake economic impact payments, the site made use of logos for agencies (i.e., Federal Emergency Management Agency or FEMA and the Centers for Disease Control and Prevention or CDC) related to the COVID-19 pandemic — but not to economic payments.

However, the devil is in the details, and some of those details were particularly realistic. Anyone clicking the link in the email would be led to a page with nice pictures and soothing words about impact payment eligibility. Symbols like the American Flag and logos from the CDC and FEMA also helped make the page look reassuring.

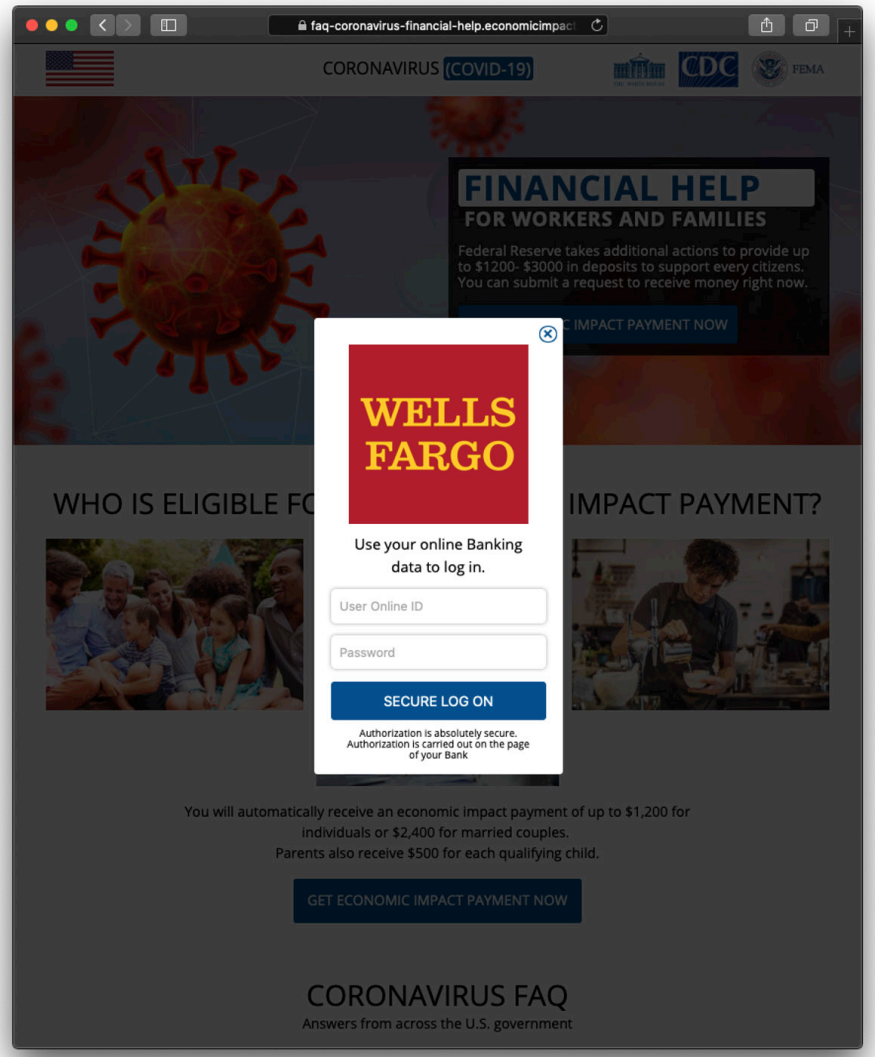


Once the recipient selected a bank and hit the “NEXT” button, a credential harvesting login would appear. The phishers took care to insert the correct logo of the selected bank (in this case, Wells Fargo).

In doing a deeper analysis of this particular phishing attempt, an INKY technician entered fake credentials on the “Wells Fargo” login. The site returned the error message “You entered the wrong data.” However, behind the scenes, the fake credentials were sent to the phisher’s email address. Obviously, if the phish were successful, the recipient’s real banking credentials would have been stolen.

A reverse image search on images revealed that the phisher used mainly stock images available on the Internet but fabricated some of the others.

Although the harvesting site was hosted by a domain in Arizona, the fake email pitch itself originated from a "good" (according to the SPF record) Italian IP address hijacked from a "legitimate" (according to the DKIM record) Italian domain. Most anti-phishing technology on the market today (with the exception of INKY) would consider "pass" tags on these two measures sufficient to judge the email safe. The key word back a few sentences is "hijacked." A bad person got a hold of a good email address and repurposed it to promote their own nefarious goals.



If the target managed to get all the way through the dialog — and gave up their banking credentials — they were then dumped ceremoniously onto an actual government page, an IRS FAQ (**`https://www.irs.gov/newsroom/economic-impact-payments-what-you-need-to-know`**).

You could click on that last link and no harm would come of it. But if you got there by way of Italy and Arizona, you might notice a decrementing bank balance in the following days.

Given the professionalism of the HTML and CSS used to compose the phishing site, the creator was likely someone with strong Web development skills. And they get a special tip of the hat for the fact that the drop-down menu displayed the correct logo for each selected bank.

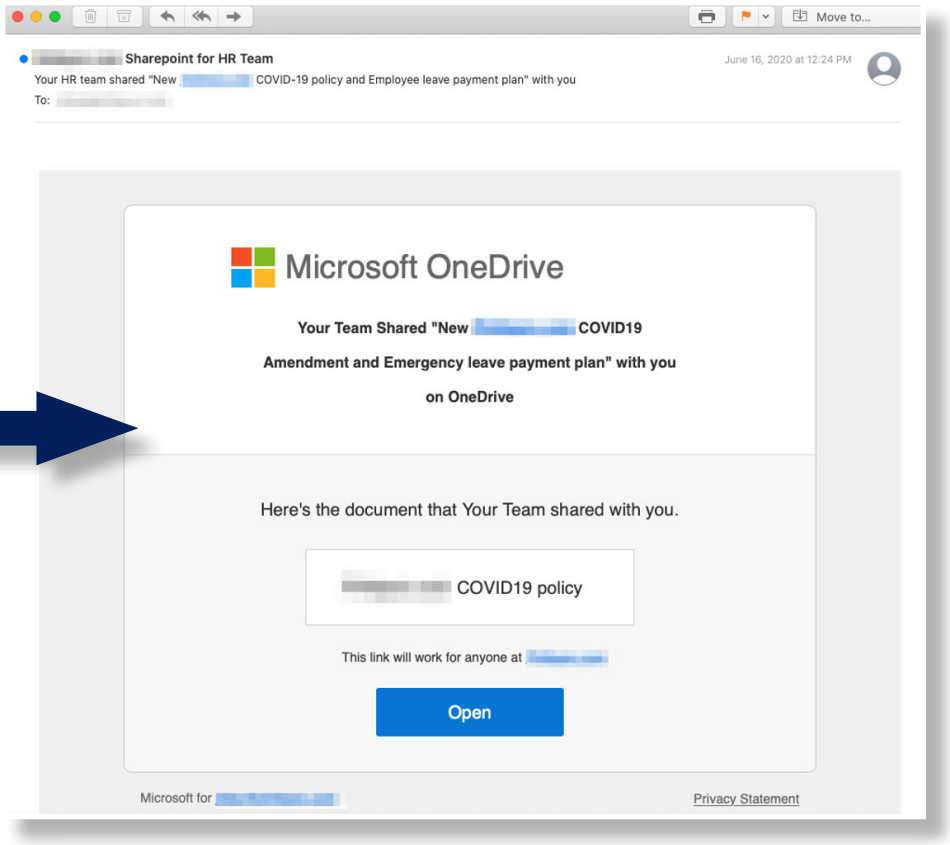
Many people formerly used to commuting to an office every day found themselves working from home in 2020, as companies endeavored to keep the lights on while not exposing their employees, customers, and suppliers to COVID-19.

One of the issues that came to the fore during this change in work circumstances was that employees were now working outside the corporate firewall. Often the IT department was unable to keep an eye on the digital traffic, and workers themselves were unused to how to manage their time and resources without colleagues nearby.

Cue the phisher-people.

What better target than someone confused, inexperienced, and isolated? Some of the better phishing attempts were aimed at this audience.

Here's a good example of a phish targeting remote employees:



Note the attention to detail here. Although the INKY team blocked out the personally identifiable information (PII) on this screenshot, the black hat who crafted this attack inserted the target company's name throughout the email. For now, we'll call the firm "Phishco."

The "from" display name is "Phishco Sharepoint for HR Team." The mail offers to share a file download called "New Phishco COVID19," supposedly policy guidance for employees. Three more specific company references follow. It's enough to lull the reader into complacency.

However, anyone clicking on the big blue "Open" button would have been taken to a credential harvesting site, where login particulars would be stolen. As a nice final touch, the sequence would drop the victim onto a real World Health Organization (WHO) page, which details precautions people can take to protect themselves against the virus.

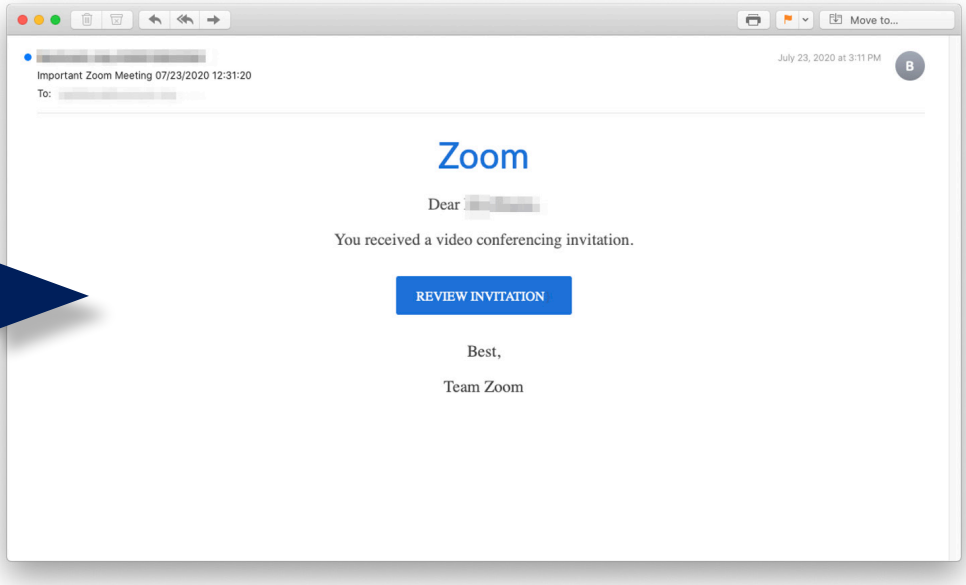
As workers and managers struggled to navigate the difficult terrain of 2020's new work circumstances, and individuals tried to remake their disrupted lives under quarantine and other restrictions, phishers took advantage people's trust in the Websites of companies and institutions that seemed to represent lifelines.

Some of these attempts probed IT infrastructure, like Zoom, Dropbox, and SharePoint. Others sought to find weaknesses in financial tools like PayPal and Quickbooks. Why those last two? As American bank robber Willie Sutton may or may not have said in response to a reporter's asking why he robbed banks, "Because that's where the money is." Phishers gravitate toward the money.

Zoom

Before the pandemic, the cloud videoconferencing provider Zoom was known to only a few people, mainly the company's small corporate customer base. During lockdown, Zoom's user base expanded from 10 million to more than 300 million daily users, opening a huge opportunity for phishers to target isolated people who lacked much in the way of context and experience using Zoom.

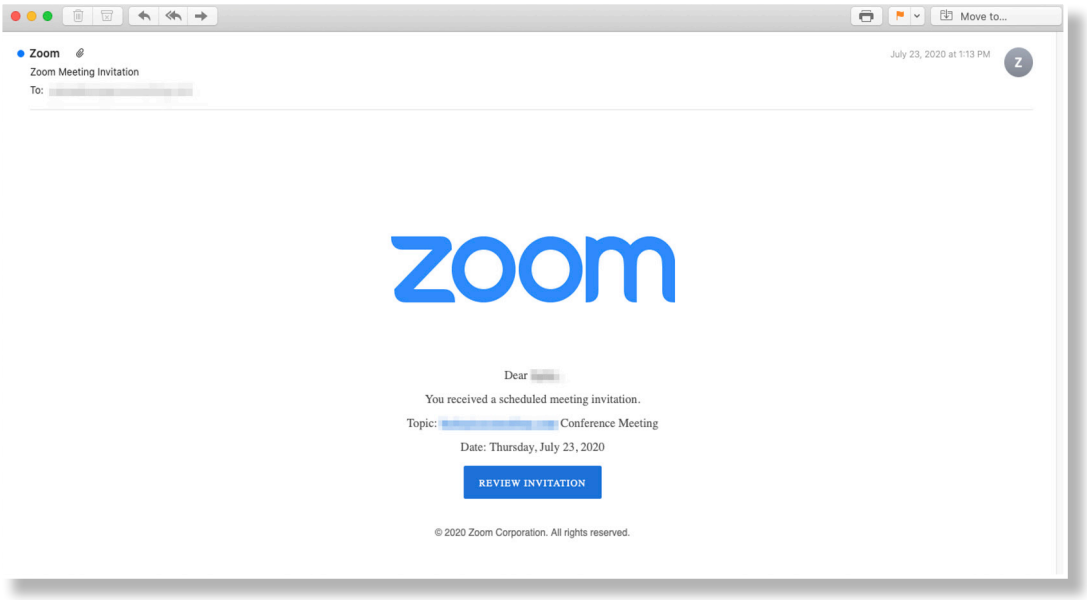
Everyone got a lot of Zoom meeting invitations. And phishers sent quite a few themselves. Here's an example, picked up by INKY Phish Fence:



Looks pretty good, right? Nice logo, simple layout, accurate recipient company name (blocked out for privacy), and real recipient (also blocked out). But clicking the "REVIEW INVITATION" button would lead to a Microsoft credential harvesting site. The Zoom logo is not an actual logo, but just some blue sans serif typeface that's been blown up to about the right size.

Here's another with a bit more realistic detail, including sender spoofing of Zoom itself and a copyright statement (All rights reserved. Ha!)

Note the better logo, inserted recipient's name, and even a nice topic description that includes the recipient's company's name.

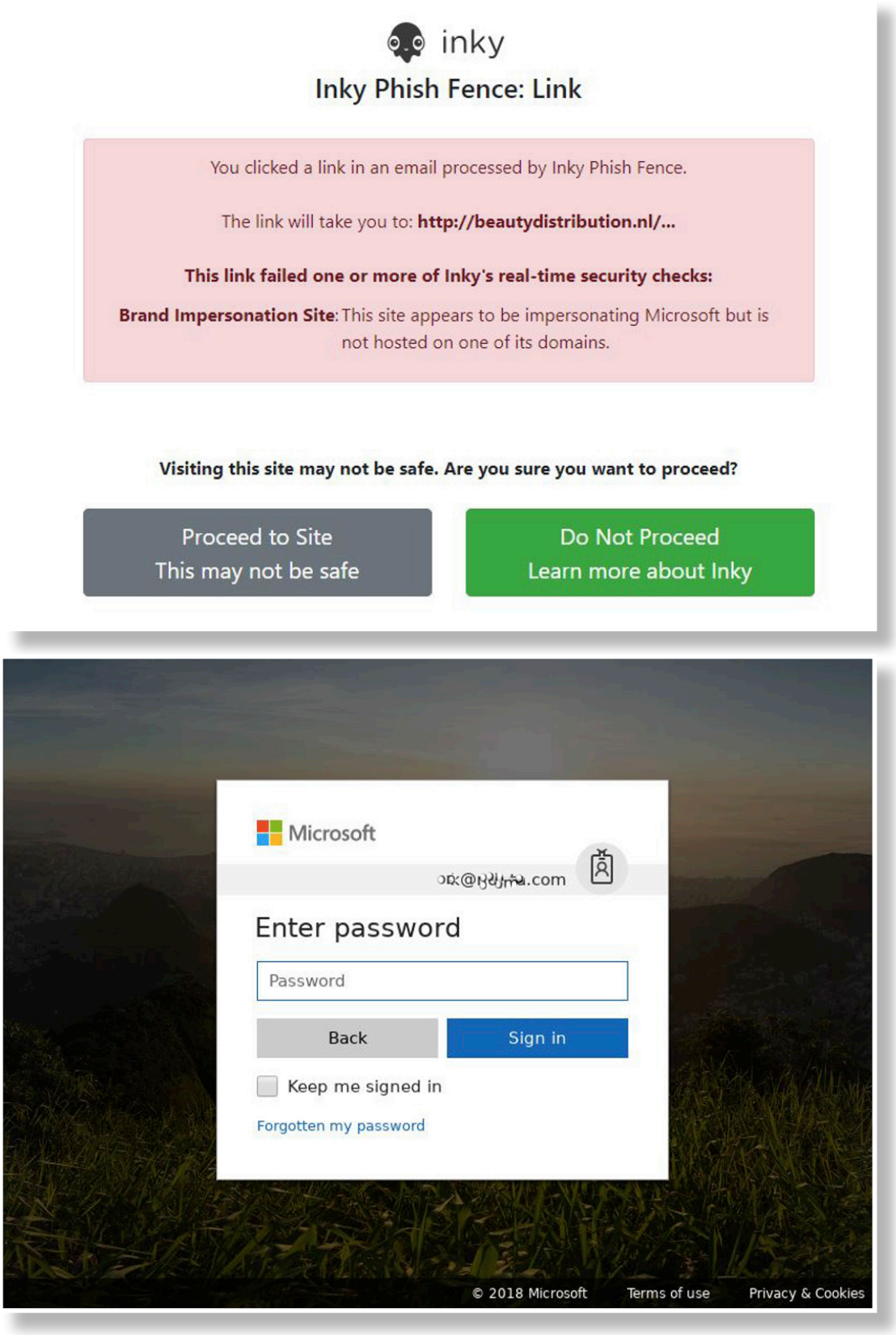


Microsoft

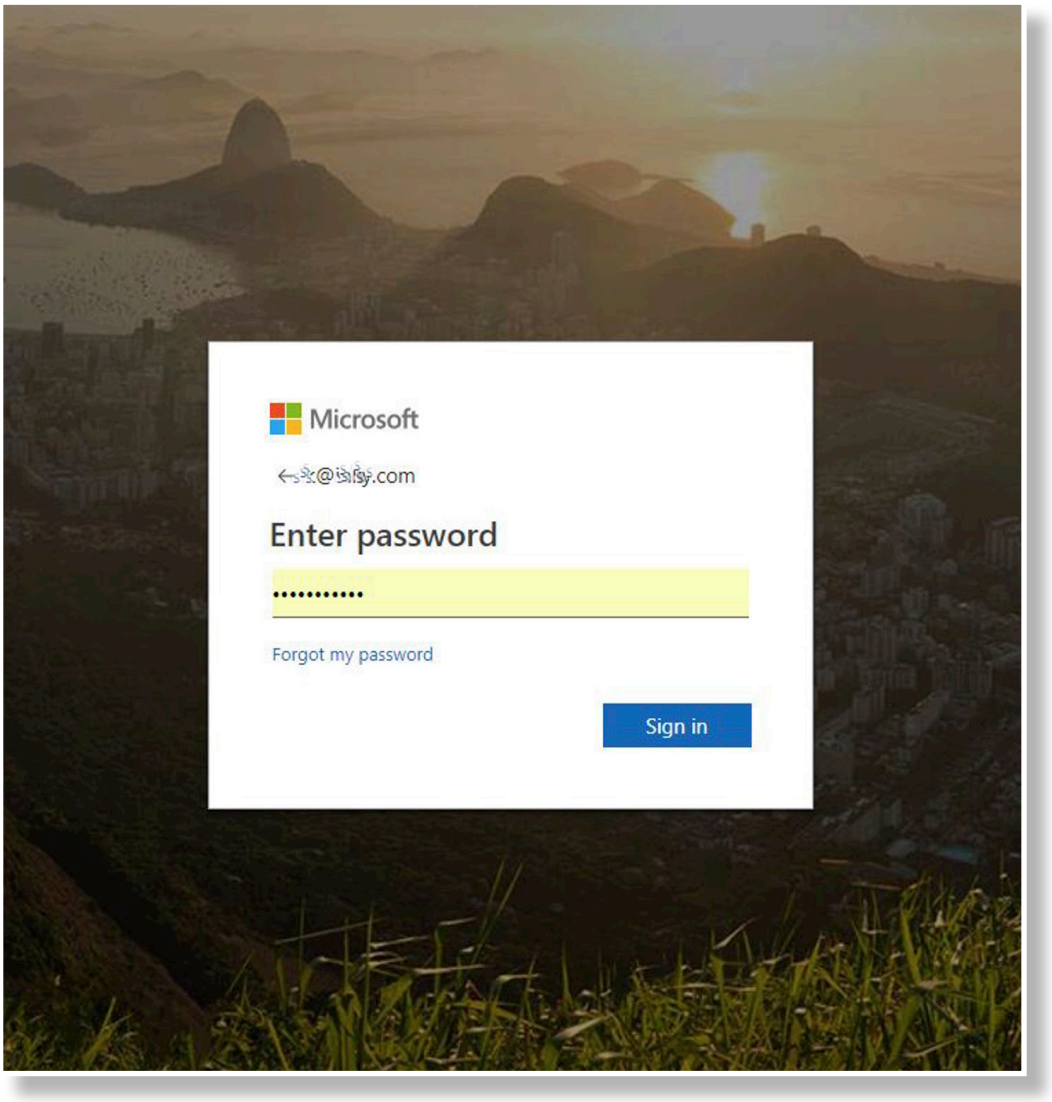
Microsoft was one of the phishers' favorite companies to impersonate. The reason? Because Microsoft has such a well integrated suite of products, nearly universally used. Thus, most targets wouldn't think there was anything wrong with a SharePoint download pausing to ask for O365 login credentials.

Many phishing attacks targeted O365 because obtaining legitimate login credentials would potentially allow the attacker to move laterally through the target company's digital assets.

Here's one as viewed through INKY's "safety window," a view of the real site rendered from the actual HTML into a harmless .png file. You can see it, but it can't hurt you. Looking closely, it shows that the link leads to a site called beautydistribution.nl in the Netherlands (which probably distributes a bit more than just beauty).



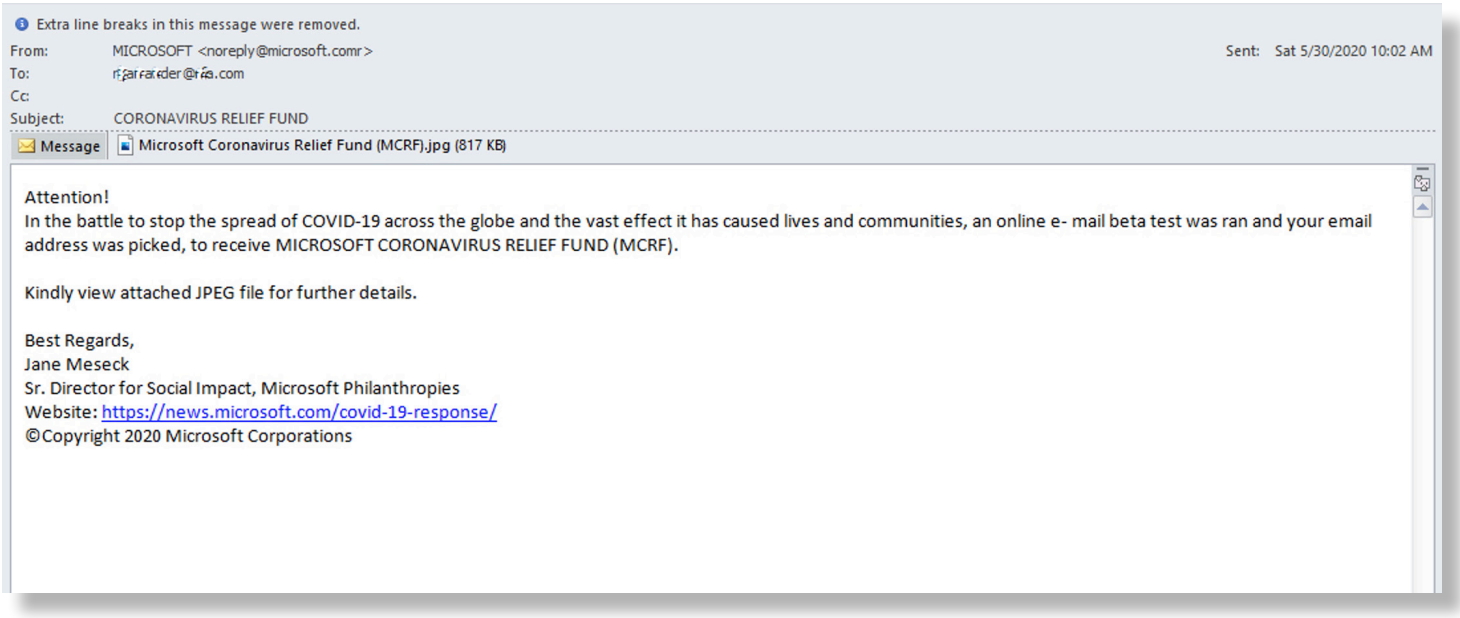
But compare that to a real O365 login, as shown here:



They're nearly identical. Even a practiced eye might not see anything wrong with the bad one.

If this next one looks too good to be true, that's because it is. A confusingly written missive, it appears to come from Microsoft, except that the display address says the sender is "noreply@microsoft.comr." Of course, no such domain exists (there is no .comr suffix approved by the Internet Corporation for Assigned Names and Numbers or ICANN). But a quick reader might not see that slight difference.

The content supposedly informs the recipient that Microsoft is donating a large sum of money to them (which is entirely plausible!).


Extra line breaks in this message were removed.

From: MICROSOFT <noreply@microsoft.comr>
Sent: Sat 5/30/2020 10:02 AM
To: [redacted]
Cc:
Subject: CORONAVIRUS RELIEF FUND

Message | Microsoft Coronavirus Relief Fund (MCRF).jpg (817 KB)

Attention!
In the battle to stop the spread of COVID-19 across the globe and the vast effect it has caused lives and communities, an online e- mail beta test was ran and your email address was picked, to receive MICROSOFT CORONAVIRUS RELIEF FUND (MCRF).

Kindly view attached JPEG file for further details.

Best Regards,
Jane Meseck
Sr. Director for Social Impact, Microsoft Philanthropies
Website: https://news.microsoft.com/covid-19-response/
©Copyright 2020 Microsoft Corporations

Clicking on the attachment reveals an image of a "funds release form" with a lot of Microsoft-ian elements, like the logo and the name "Microsoft" displayed as the "from" address. Microsoft does have a lot of money, which it could be giving away to … you. But then again, perhaps not.

The recipient is asked to print the form, fill it out, and email it to a "Dr. Nicola Hodson" at an email address with a "microphilanthropies.com" domain. The attacker's goal is to harvest the recipient's PII.

Microsoft
Redmond, Washington

Website: https://news.microsoft.com/covid-19-response/
Our Ref: UK/020-22468/COVID

RESPONDING TO COVID-19 TOGETHER

MICROSOFT CORONAVIRUS RELIEF FUND (MCRF)

As the world responds to the outbreak of **COVID-19**, our thoughts are with the people affected and the medical professionals working around the clock to help those most in need. At Microsoft, we're working to do our part by ensuring the safety of our employees, striving to protect the health and well-being of the communities/world in which we operate. Providing technology, tips and resources to our customers to help them do their best work while remote during this pandemic.

In the battle to stop the spread of **COVID-19** across the globe, and limit its impacts as much as possible, information accuracy is key, as people need to know and understand the way in which the virus is transmitted and what they can and should do to avoid infection and spread.

As the coronavirus outbreak continues to worsen around the world, it is taking a devastating toll on **LIVES AND COMMUNITIES**. To help address some of these challenges, Microsoft has donated **[One Billion United States Dollar]** to support **"SMALL AND MEDIUM SIZED BUSINESS (SMB)**, health organization and governments and health workers on the frontline of this global pandemic."

One of the key areas in combating coronavirus pandemic by Microsoft; is directly reaching out to individuals globally, with the help of our online e-mail beta test. Your email address was picked to receive the sum of **$2,864,000.00 USD [Two Million, Eight Hundred and Sixty-Four Thousand United States Dollar]** from Microsoft Coronavirus Relief Fund (MCRF).

Furthermore, your detail falls within our UK representative office as indicated in our database and your Microsoft Coronavirus Relief Fund (MCRF) will be released to you from our UK regional office in London United Kingdom.

You are required to contact Microsoft Coronavirus Relief Fund (MCRF) in UK below for the documentation and processing of your fund, between the hours of 8:00am-7:30pm on Monday to Saturday.

CONTACT DETAILS:
Dr. Nicola Hodson
General Manager, Marketing & Operations Microsoft UK
Email: **dr.nicola.hodson@microphilanthropies.com**

Kindly e-mail the Microsoft Coronavirus Relief Fund (MCRF) department at once with the Verification and Fund release form below for the validation of your Microsoft Coronavirus Relief Fund (MCRF). You are also advised to contact our General Manager, Marketing & Operations Microsoft UK (Dr. Nicola Hodson) via the above email with the following details below to avoid unnecessary delay and complications.

MANDATORY VERIFICATION AND FUNDS RELEASE FORM
- FULL NAME:
- AGE/SEX:
- OCCUPATION/POSITION:
- RESIDENTIAL ADDRESS:
- TELEPHONE (MOBILE):
- EMAIL ADDRESS:
- NATIONAL/COUNTRY:
- WHAT IS YOUR COMMENT ON THE CORONAVIRUS PANDEMIC?
- HOW DO YOU INTEND TO HELP HUMANITY, ONCE YOU RECEIVE YOUR MICROSOFT CORONAVIRUS RELIEF FUND (MCRF)?

Microsoft values your right to privacy! Your information is 100% secured and will be used exclusively for the purpose of this Microsoft Coronavirus Relief Fund (MCRF) only.

You can either fill your Mandatory Verification and Funds Release Form by printing and manually filling out the requested details or you can fill directly on email, lastly you can provide the details in Microsoft Word/WordPad/Notepad.

NOTE: This is **MICROSOFT CORONAVIRUS RELIEF FUND (MCRF)** not a **LOTTERY**. Microsoft is not into **LOTTERY**.

For security reasons, you are advised to keep Microsoft Coronavirus Relief Fund (MCRF) information confidential, till your claims are processed and your money remitted to you. This is part of our precautionary measure to avoid double claiming and unwarranted abuse of this program by some unscrupulous elements. **PLEASE BE WARNED!**

Congratulations from the staffs & Members of Microsoft Empowering Innovation/Philanthropies and Microsoft Coronavirus Relief Fund (MCRF) department

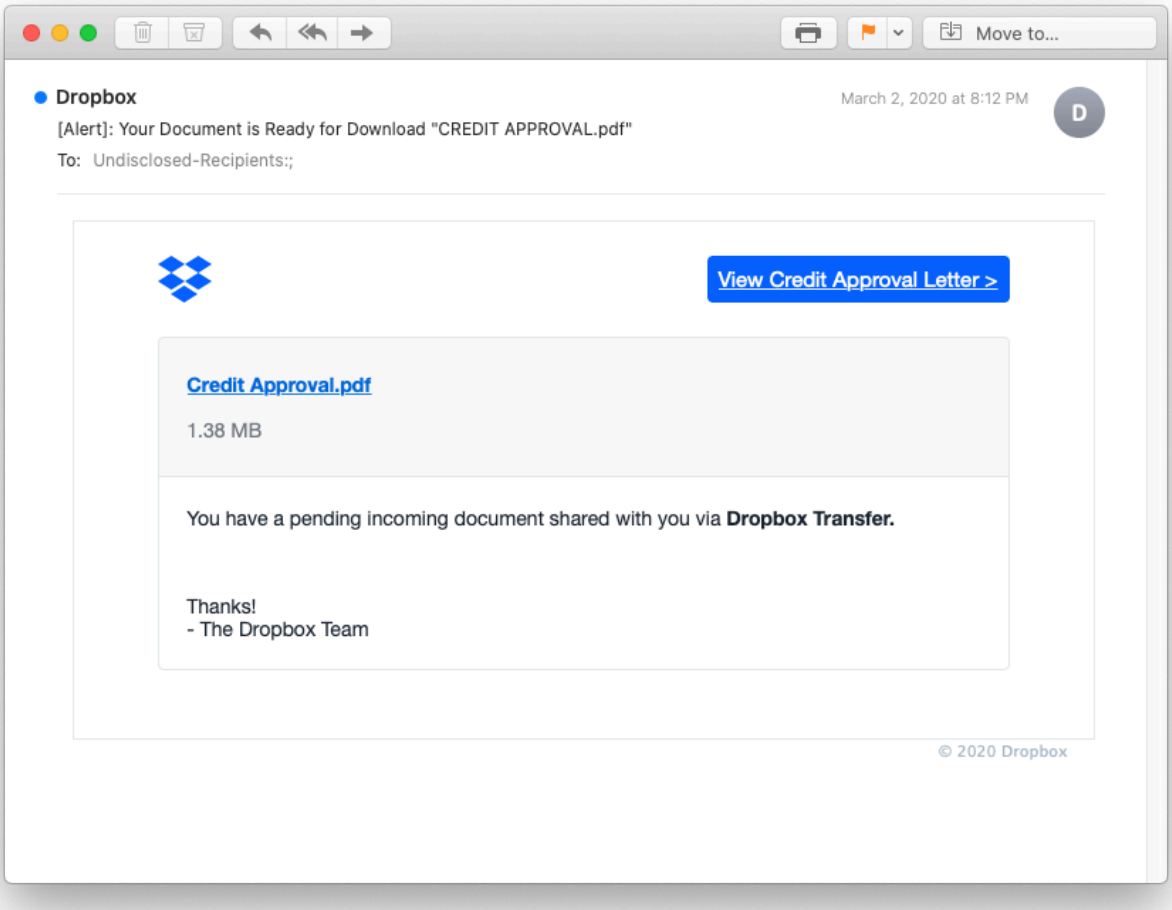
.
Sincerely,
Mr. Satya Nadella
Executive Chairman of Microsoft Corporation

Powered by Microsoft

Dropbox

Many people isolated in their homes turned to tools like Dropbox to stay connected to colleagues and exchange files. Since the Dropbox interface is essentially an email with a notification that a file awaits downloading, it's a nearly perfect medium to deliver malware directly to a recipient's machine.

This one, sent on March 2, looks pretty hopeful. It has the Dropbox logo and Dropbox displayed as the sender. Apparently, the recipient has been cleared for a loan. All they have to do is download a file called "Credit Approval.pdf."



However, INKY, looking under the hood, saw something else entirely. Phish Fence displayed a bright red “high-alert” warning banner in the recipient’s email itself, and if they clicked on the “Details” link in the banner, they would see the output from INKY’s analysis, shown here:

Danger! This message looks malicious.
(From: no-reply@drop-box.com, External)

Potential Sender Forgery
The sender (Dropbox <no-reply@drop-box.com>) may be trying to trick you into thinking this message is from a major brand, a known contact, or a coworker (Dropbox).

Brand Impersonation
This message appears to be impersonating Dropbox but was not sent from one of its domains.

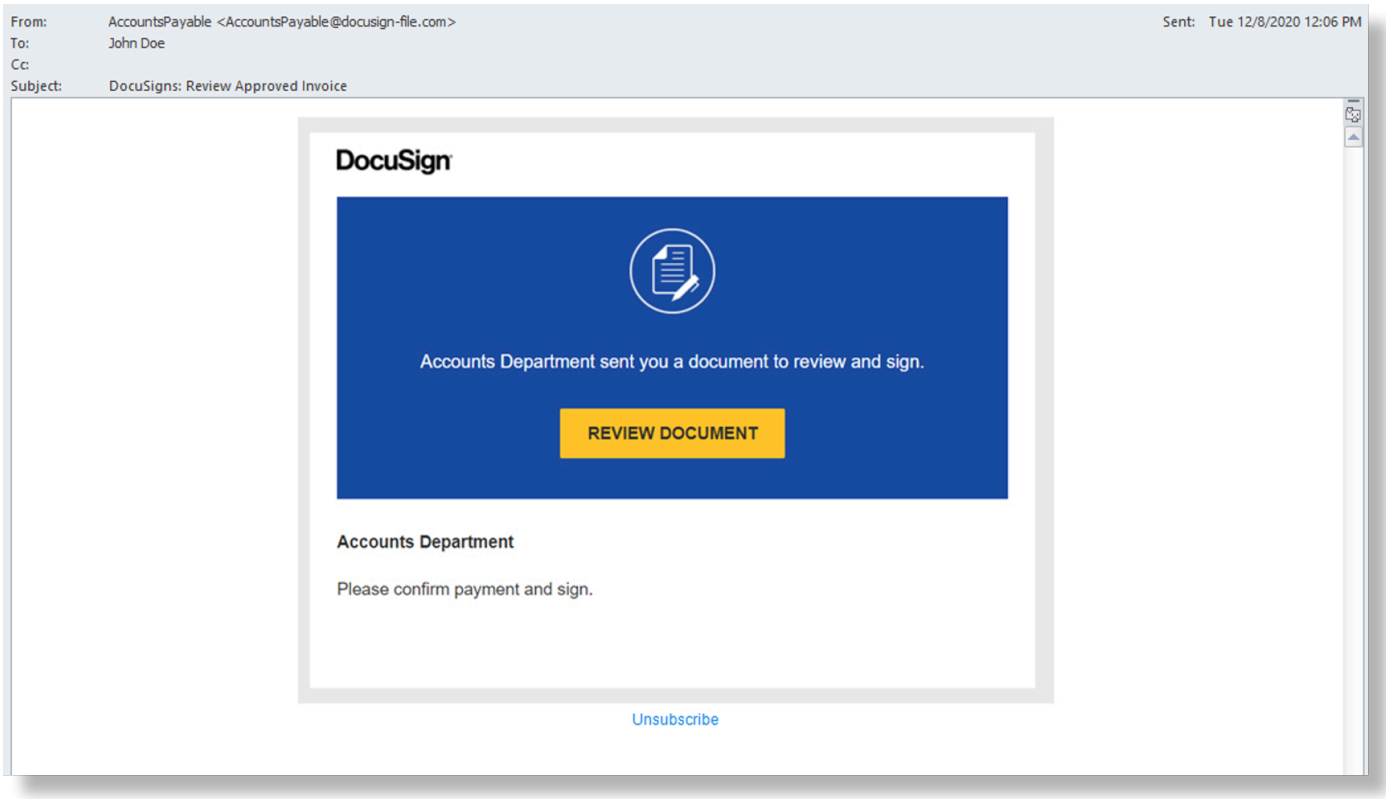
Potential Sender Forgery
This message looks different than the usual mail from this sender (Dropbox). This may be a sign of email forgery or spear phishing.

First-Time Sender
This is the first message you've received from this sender. Be careful when replying or interacting with any attachments or links.

Confusable Domain
It contains a domain name (drop-box.com) that may be confused with a website (dropbox.com) run by a brand commonly targeted by phishing scams (Dropbox, dropbox.com).

With the pandemic accelerating digital transformation, individuals and companies turned increasingly to DocuSign to complete transactions. The digital signature and document management company eliminated the last source of personal contact in many transactions: the wet signature. With a legally binding digital signature, parties to a transaction could execute the entire thing remotely.

However, the phishers were also alert to this trend and sent out many phishing assays in the form of email like the one shown here as a human would see it.



The email looks pretty good. It has DocuSign's logo and colors, and the right layout for a document signing, right down to the big yellow "REVIEW DOCUMENT" button. The domain from which it was sent — docusign-file.com — is easily confusable with DocuSign's real domain: docusign.com. After all, it's supposed to be a file from DocuSign. So, why not docusign-file.com? And "AccountsPayable" is an entirely plausible sender.

Good thing INKY saw through the ruse.

To set this phish up, first a bad actor gained access to a Twilio SendGrid account. SendGrid is a legitimate service that lets mostly small businesses send email to a list of prospects or customers. With the compromised SendGrid account, the perpetrator staged an attack on a hijacked list, mailing recipients the DocuSign phishing email.

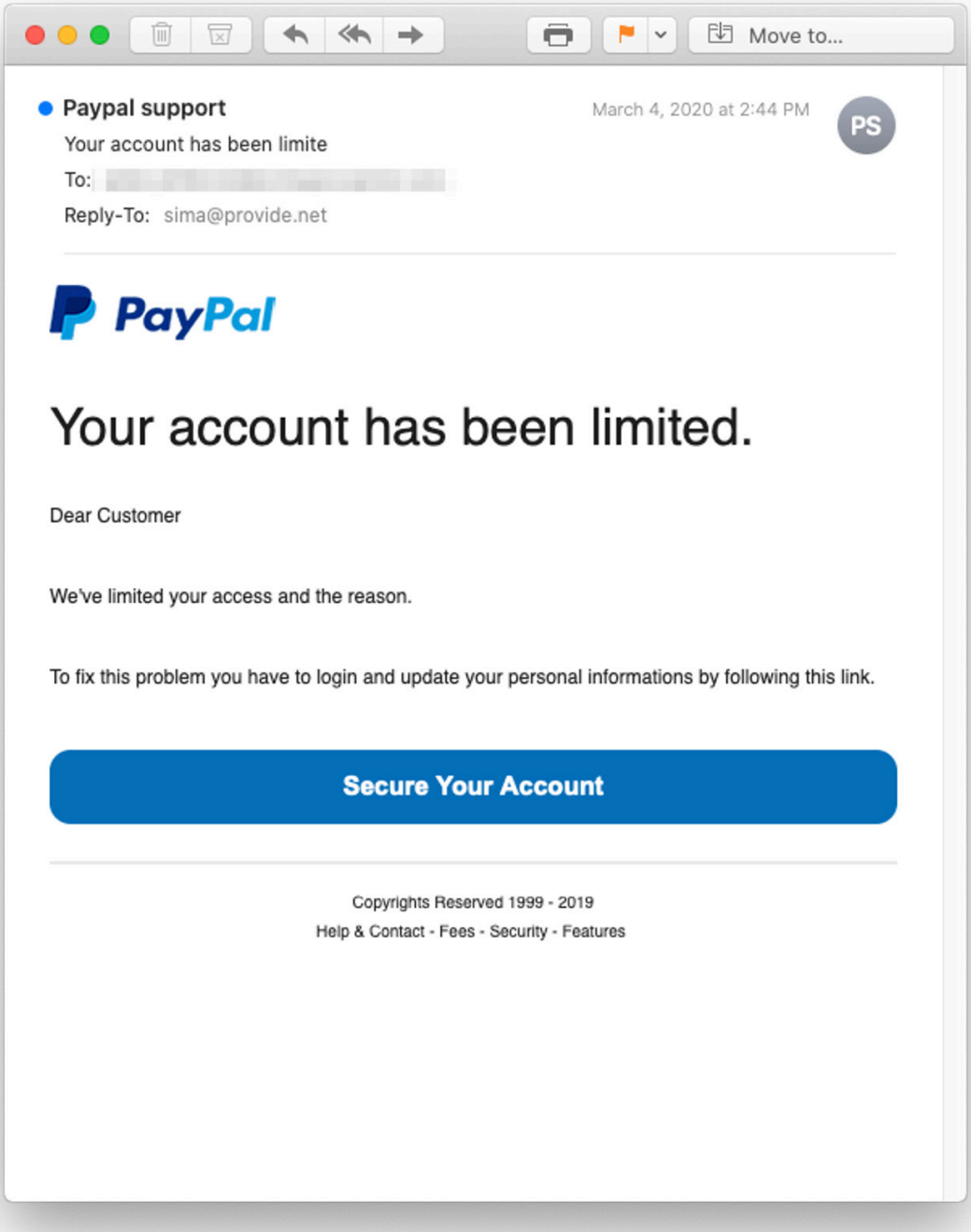
Behind the big yellow button was a malicious link that hosted a DocuSign credential harvesting page, which has since been taken down.

The same email, viewed as a machine would see it, displays the hallmarks of perfidy. In the header shown below, the first "Received" block above the visible (to a human) date-from-subject block shows that SendGrid, not DocuSign, sent the email. The email passed DKIM and SPF tests because it came from a real place — just not the place it said it was coming from.

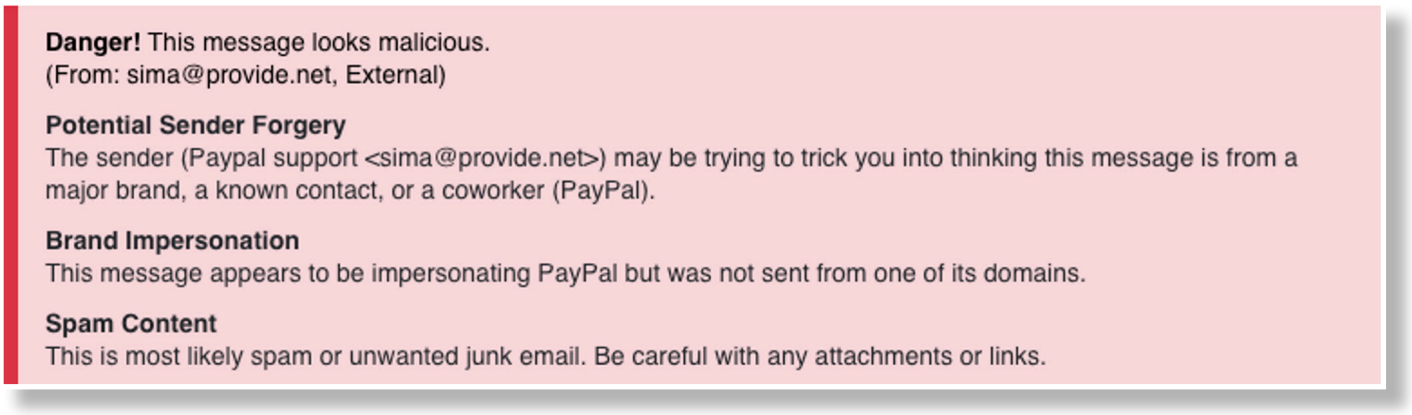
INKY, looking at the email both ways (as a human and as a machine), detected that the email was purporting to come from DocuSign, but was not sent from a domain controlled by DocuSign, an event that caused INKY to throw a red flag.

```
Received: from DM3PR03CA0020.namprd03.prod.outlook.com (2603:10b6:0:50::30) by
 DM6PR11MB2921.namprd11.prod.outlook.com (2603:10b6:5:70::26) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.3611.31; Tue, 8 Dec 2020 17:06:15 +0000
Received: from DM6NAM04FT045.eop-NAM04.prod.protection.outlook.com
 (2603:10b6:0:50:cafe::4) by DM3PR03CA0020.outlook.office365.com
 (2603:10b6:0:50::30) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3632.18 via Frontend
 Transport; Tue, 8 Dec 2020 17:06:15 +0000
Authentication-Results: spf=pass (sender IP is 149.72.187.51)
 smtp.mailfrom=sendgrid.net; example.com; dkim=pass (signature was
 verified) header.d=sendgrid.net;example.com; dmarc=none action=none
 header.from=docusign-file.com;compauth=fail reason=001
Received-SPF: Pass (protection.outlook.com: domain of sendgrid.net designates
 149.72.187.51 as permitted sender) receiver=protection.outlook.com;
 client-ip=149.72.187.51; helo=o1.ptr8786.letscoolaircon.com.sg;
Received: from o1.ptr8786.letscoolaircon.com.sg (149.72.187.51) by
 DM6NAM04FT045.mail.protection.outlook.com (10.13.159.46) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.3632.21 via Frontend Transport; Tue, 8 Dec 2020 17:06:15 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=sendgrid.net;
        h=content-type:from:mime-version:subject:reply-to:to:list-unsubscribe;
        s=smtpapi; bh=L3yehVLwBeT3R3C84mFJRmasTZuNyP4HrEC2AVO+Znk=;
        b=FgI+njpo4s1J3+220EB0cXrBvaNxijN69T66J2ozxfZssIOpBX1NjqDJll1fyeckvpKC
        L7dbntTUxYsiqGg3LkR5LohGGBHw4hpuDE1Y7DTYDMLPbyWD+C0JXAEFedcU9lG6Lz7K+L
        2huP4USonBF1+EgxuC4Hbp8EQqwMPI70c=
Received: by filterdrecv-p3mdw1-6f5f88f6c4-cvkg5 with SMTP id filterdrecv-p3mdw1-6f5f88f6c4-cvkg5-20-5FCFB285-AC
        2020-12-08 17:06:13.747519457 +0000 UTC m=+417817.584276718
Received: from MTU3MTc2ODI (unknown)
        by ismtpd0100p1iad2.sendgrid.net (SG)
        with HTTP
        id LIZKDPK4QRegElZvx9vFHQ
        Tue, 08 Dec 2020 17:06:13.700 +0000 (UTC)
Content-Type: multipart/alternative; boundary=db2a79e7928f0403eb807fd8711010e8cc6c80b092bc9cb2658e8cb47225
Date: Tue, 08 Dec 2020 17:06:14 +0000 (UTC)
From: AccountsPayable <AccountsPayable@docusign-file.com>
Mime-Version: 1.0
Message-ID: <LIZKDPK4QRegElZvx9vFHQ@ismtpd0100p1iad2.sendgrid.net>
Subject: DocuSigns: Review Approved Invoice
Reply-To: AccountsPayable@docusign-file.com
```

It could be devastating news to an individual sheltering in place at home. Apparently, PayPal has “limited” the recipient’s account. Terrible! What to do about it? Well, click the big soothing blue button that says “Secure Your Account.” Who wouldn’t?

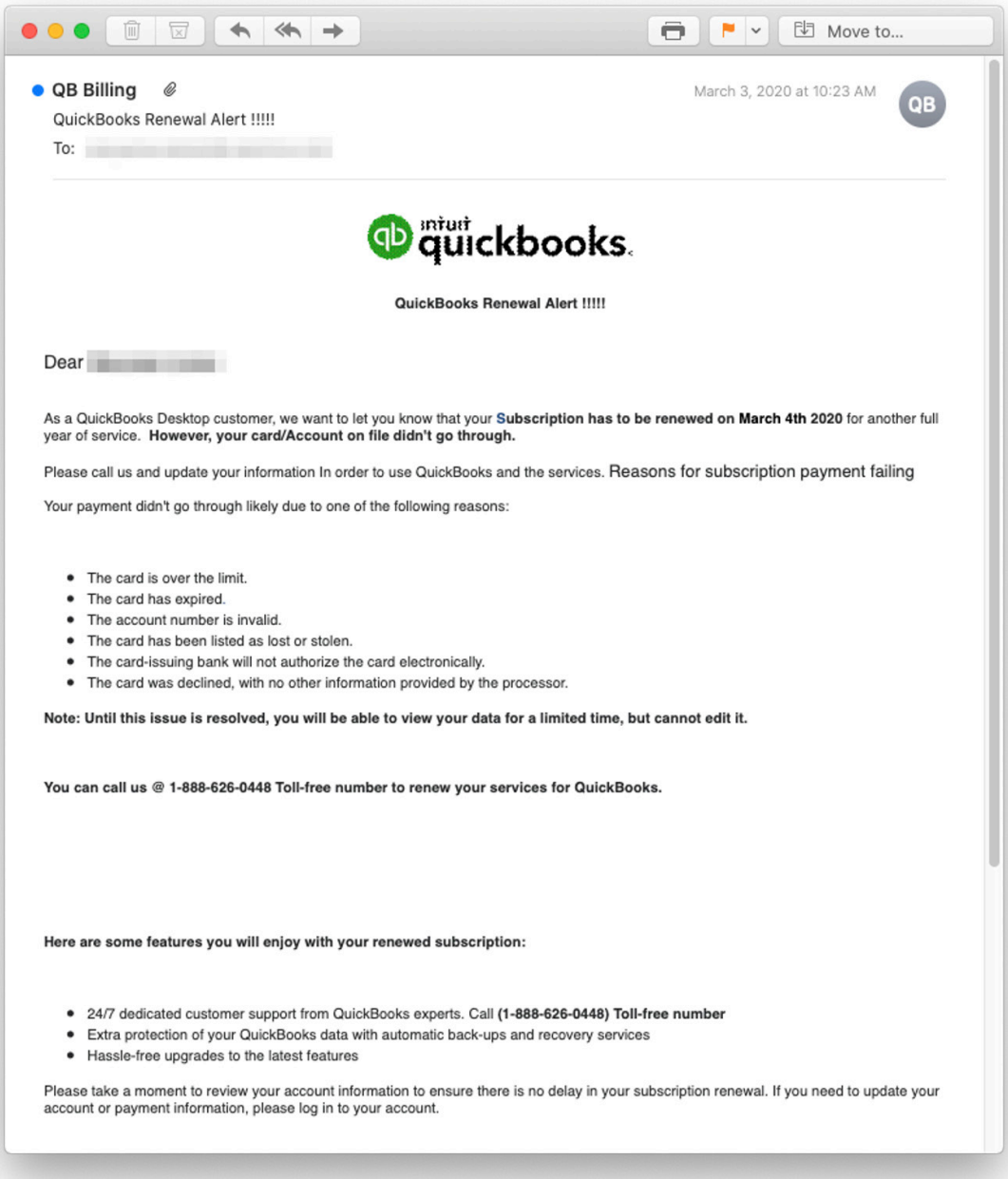


But INKY thought there was something wrong with this email. INKY sniffed out a brand forgery because it does image analysis and recognized the brand PayPal and then looked to see whether the actual sending domain was under PayPal's control. Since it wasn't, INKY threw a red flag:



QuickBooks

In this example, Intuit's QuickBooks is apparently telling the recipient that there's a problem with the subscription renewal and gives them one day to set things to right. It solicits a phone call. Likely, the phone is covered by a black hat, who would try to extract PII, login, and financial data from the hapless caller.



But INKY saw it differently. Using its unique ability to “see” an email the way a person would AND the way a machine would, INKY found that the assertion in the text and implied by the image that this message came from Intuit was false. The details showed this:

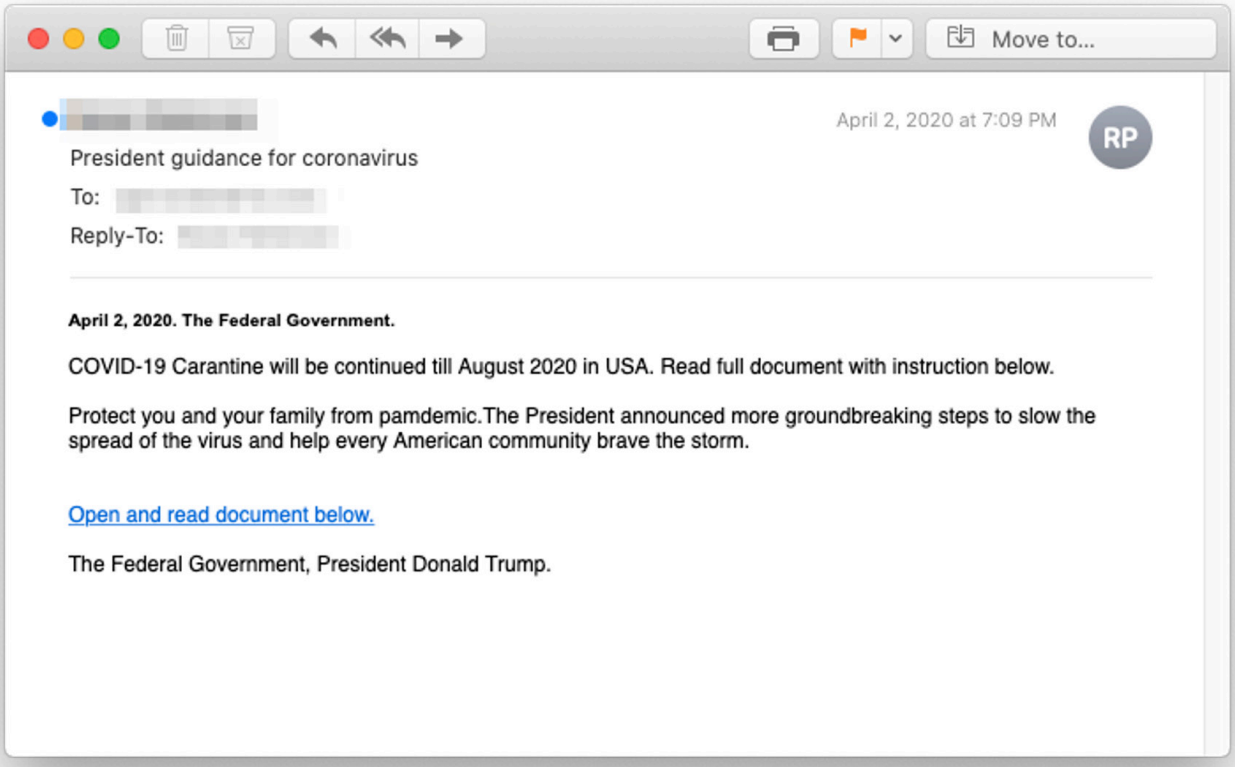
Danger! This message looks malicious.
(From: intuit@qb-billing.com, External)

Brand Impersonation
This message appears to be impersonating Intuit but was not sent from one of its domains.

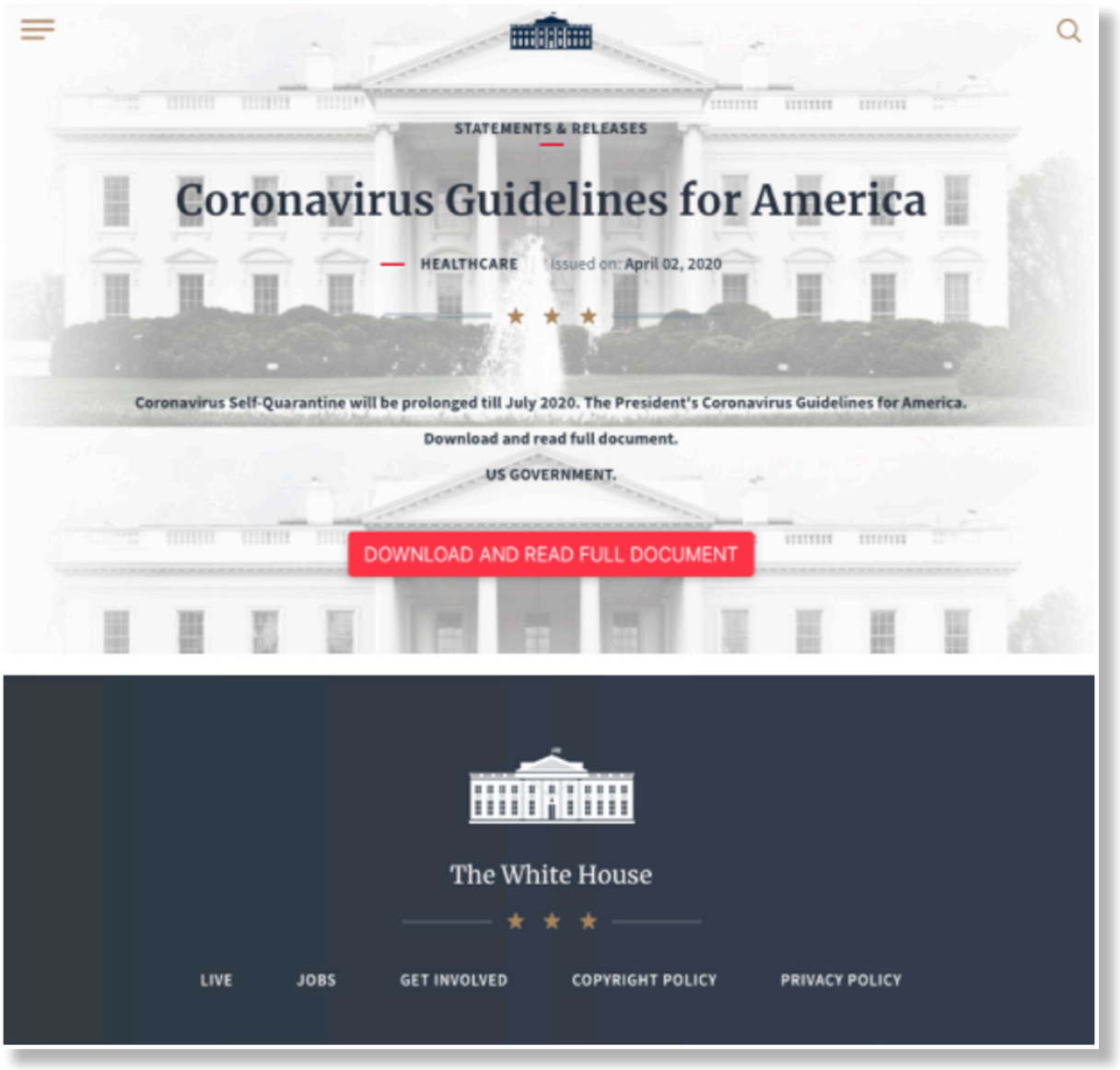
Sensitive Content
The message appears to discuss sensitive information (e.g., passwords, account information, etc). If possible, instead of clicking a link, go directly to the sender's web site to carry out the requested action, or confirm the request outside of email before replying.

Trump

And no set of spoofed senders would be complete without a contribution from Donald Trump. In the following message (out of which PII has been blocked), the President himself is apparently telling the recipient how to stay safe.



Clicking on the “Open and read document below” link took the target to a pretty good looking “White House” Web page with the title “Coronavirus Guidelines for America.”



Clicking on the red “DOWNLOAD AND READ FULL DOCUMENT” button downloaded a poisoned Word document. The file — Information.doc — contained a Trojan set in a macro. When a victim tried to read the file, it asked them to “Enable Macros,” and then the Trojan downloaded malware from another server, which served up ransomware, other malware, like a key logger, or even a legit but compromised remote diagnostic tool controlled by a bad actor.

So much for keeping America safe!

2020 Was a Great Year for Phishing Expeditions

When the pandemic tightened its grip on the United States in March and April, society was upended. Many norms were broken, and almost everyone found themselves navigating unknown waters. This disorienting environment was perfect for phishing attacks.

People craved information and sought it on the Internet. And much of it came in through unsolicited email. Overwhelmed, few had the perspective or judgment to separate the wheat from the chaff, and even if they did, increasingly clever ruses managed to fool even the most discerning of recipients.

Brand forgery came into its own in 2020. Ready-made tools on the Dark Web allowed scammers with only limited skills to launch refined assaults. A subcategory of brand forgery — the VIP spoof — also ran rampant.

The most sophisticated attacks were reserved for the most valuable people: the VIPs. Spear-phishing — phishing attacks created specifically for an individual — hauled aboard some of these whales in 2020. On an Internet that makes it simple to assemble a digital twin, a record of someone so detailed it's like a replica, spear phishers were easily able to craft ruses of stunning realism. News (e.g., I'm in jail and need someone to bail me out) about a real relative in a real location could find a vulnerability in a target not normally subject to lapses in judgment.

What secure email gateways don't say when they claim to catch 99.7% of all incoming phish is that the best spoofs — reserved for the most important people, those who can move large sums of money around or have access to key secrets — get through. That's the whole point. It's not enough to stop most of the phish when the most devastating ones penetrate anyway. In 2020, phishers initiated attacks of this type that reaped billions of dollars fraudulently.

While INKY evolved to ferret out "account takeover" (ATO) attacks (where a real domain and legitimate email address have been hijacked by bad guys), most secure email gateways let them through because their SPF and DKIM signatures looked fine. At each stage, when the white hats finally caught up, the black hats evolved their strategy, and the game was on again. Tactics and techniques are in constant flux in the dynamic world of phishing.

Looking Forward to the Next

As we head into the decade leading up to 2030, it's worth asking how the phish-scape will evolve. It's clear that public health will drive phishing in 2021, and to some degree beyond. As the decade moves forward, phishing attacks will be crafted around other emerging geopolitical issues like climate change, migration policy, income inequality, and the role of institutions in individuals' lives.

Probably the factor that will most influence the shape of things to come in the near term will be how work will evolve as we emerge from the pandemic. Right now, conditions are optimal for phishers. People are isolated and still getting used to unfamiliar procedures and circumstances. The IT department has not been able to figure out how to keep everyone safe outside the corporate firewall.

While some have argued that work has changed permanently, that office culture is dead, and that most people will continue to work at home, others contend that people are social animals and will gravitate back toward office settings once enough citizens are vaccinated for the virus. It's most likely that a middle way will arise, in which offices still exist, but not in a format as rigid as before, and people will work in public spaces to be sociable as well as at home for productivity reasons.

But the overall digitization of society was accelerated during 2020 and there's no going back. As the decade unfurls, there will continue to be Zoom meetings and an increased use of digital tools like DocuSign, QuickBooks, and Dropbox. Since communications are imperfect, and the black hats are constantly evolving, new phishing schemes will appear, and the white hats will have to adapt their tactics.

With more value migrating online, the Willie Sutton principle will keep phishers' attention directed toward hacking of ever greater sophistication. Since phishing emails are almost always the front edge of major incursions, we can expect to see more attempts to launch attacks that enable, for example, ransomware across whole linked networks, or that set up beacons that call down modules from malicious host servers and assemble them into ever more dangerous but quiet mechanisms for stealing data or money.

With impersonation being one of the phishers' best friends, and with no institution held sacred, we can expect to see plenty more spoofs of government bodies, respected corporations, famous individuals, prestigious universities, and well known international organizations.

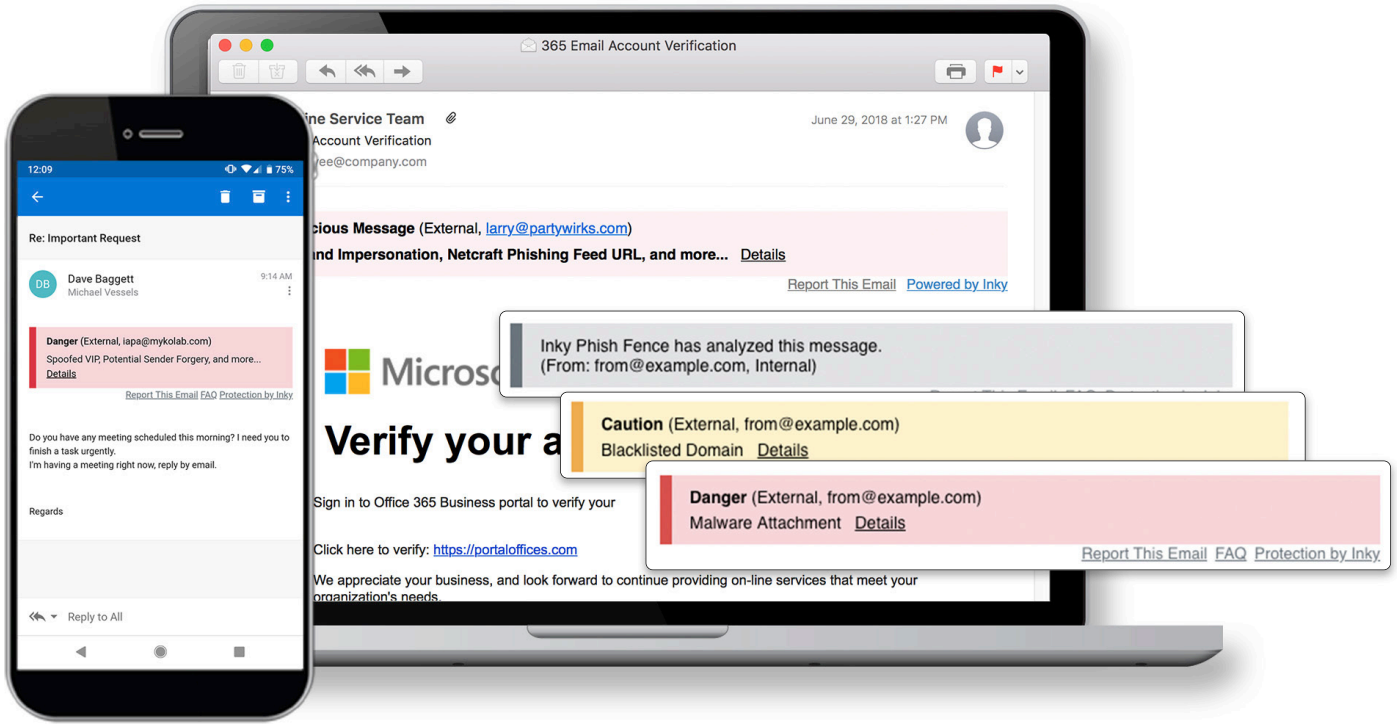
In the Next Year

In the immediate future, we can expect phishing attacks to be crafted around medical news as the COVID-19 vaccine is rolled out. In 2021, the ins and outs of vaccine dissemination will occupy much of our attention. People will be watching for updates on vaccine distribution, efficacy, and requirements. Slight changes in circumstances and policies will affect individuals, businesses, and educational institutions.

Parents will ask natural questions. When will it be safe to return to school? How will classes be conducted? Will graduation requirements change? What about the financial implications?

Businesses will analogously be looking for guidance. When will it be safe to open buildings? How many people can congregate at once in a room? On a floor? What will be involved in bringing ventilation systems up to snuff?

With a high degree of certainty, we can expect phishing attacks to weave these themes into their narratives in 2021.



What Makes INKY Different?

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.

Alerts are added to the email itself, which means they look the same on desktop or mobile. This is a significant difference from other systems, which display warnings in headers or with add-ins that may not render properly, or at all, 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.

Unlike any other anti-phishing 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.

We're passionate about email.

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

www.inky.com