Coronavirus and Cybersecurity

How to Stay Safe From Opportunistic Phishing Attacks

Hackers love emergencies and times of general uncertainty. Why? Because people are scared, distracted, potentially desperate, and are therefore vulnerable—making them ideal targets.

As COVID-19 continues to spread and global concern about the pandemic rises, bad actors will be impersonating trusted institutions like healthcare organizations, insurance companies, banks, and airlines in order to steal money, harvest credentials, or install malware on your computer...and that's just on the consumer side.

When it comes to business, trusted individuals and brands will be impersonated. For example, hackers will impersonate out-of-office CxOs and popular web conferencing applications, especially as organizations encourage and rely on remote-working.

Internally at Tessian, we've shared tips with our employees on how to spot this type of scam and what to do in case you're targeted. We think it's important to spread the message and raise awareness with everyone.

TESSIAN

Consumers: What Should You Look For?

Hackers will be impersonating trusted brands

Carefully inspect all emails, but be especially wary of those coming from healthcare organizations, insurance companies, banks, and airlines, especially those that ask you to "Confirm you are safe", "Confirm you haven't traveled to recently affected COVID-19 countries", or anything similar.

Hackers will often change, remove, or add one letter to a legitimate-looking email address

Display names – which many of us rely on to identify senders – can be easily changed. Look beyond the Display Name and examine the full email address of senders. But, be aware: hackers can directly spoof an email addresses, too. That means you have to evaluate the entire email for authenticity.

Hackers will motivate you to act

The goal of a phishing attack is to steal money, harvest credentials, or install malware. That means you'll be encouraged to download an attachment, follow a link, transfer money, or respond with personal details. These are all red flags.

Hackers may make spelling errors or craft emails with branding inconsistencies

While hackers can certainly craft perfectly believable correspondence, phishing emails may contain tell-tale signs of fraudulence. Look out for spelling errors or branding inconsistencies either in the logo, email template, or a landing page.

Employees: What Should You Look For?

Hackers will be impersonating people within your organization and third-parties like suppliers or vendors

You should be cautious when responding to any internal email that mentions the sender being out-of-office hat requires urgent action and any third-party email that comes from a source you don't recognize/

Hackers will often change, remove, or add one letter to a genuine email address

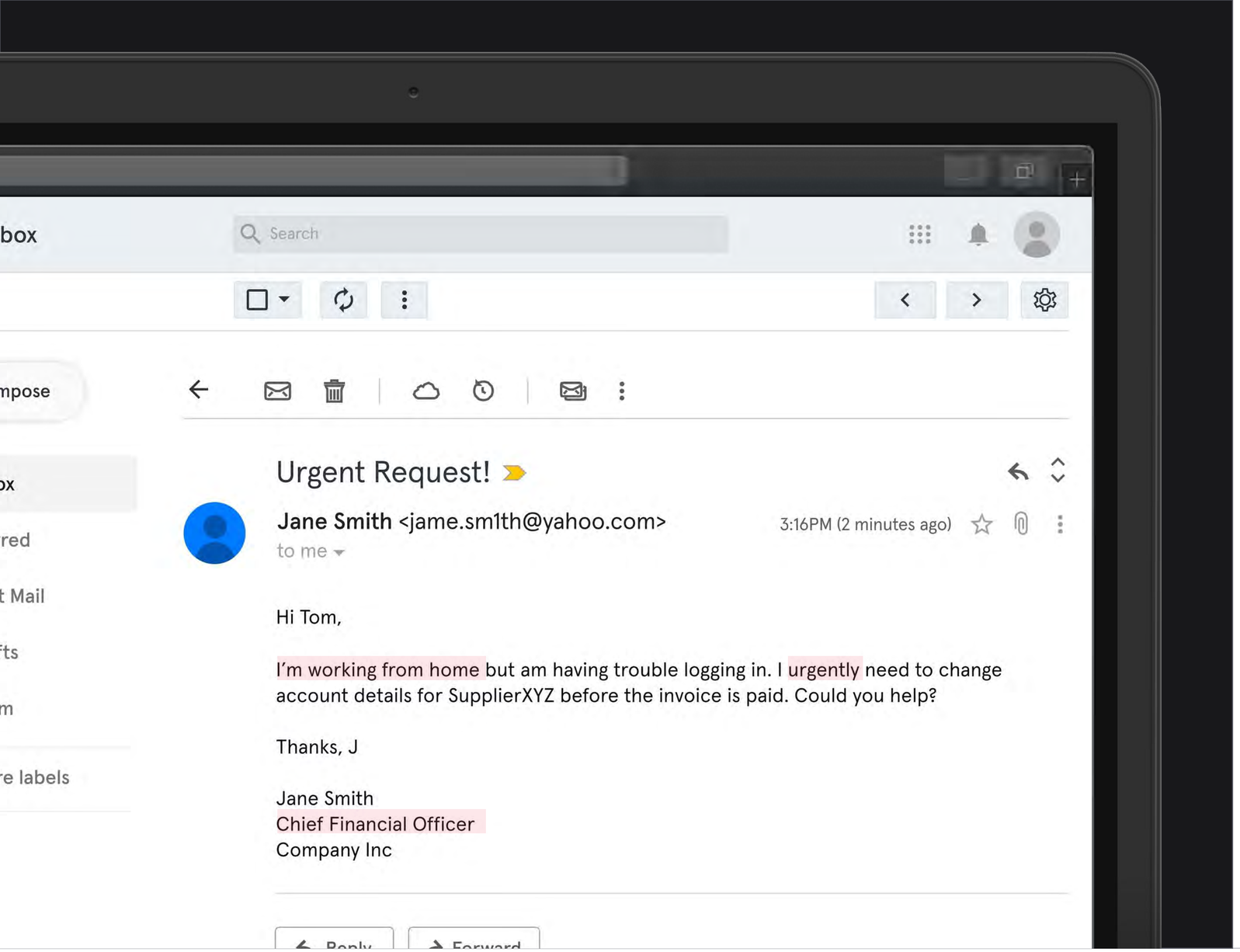
Display names – which many of us rely on to identify senders – can be easily changed. Look beyond the Display Name and examine the full email address of senders. But, be aware: hackers can directly spoof an email addresses, too. That means you have to evaluate the entire email for authenticity.

Hackers will motivate you to act

The goal of a phishing attack is to steal money, harvest credentials, or install malware. That means you'll be encouraged to download an attachment, follow a link, transfer money, or respond with personal details. These are all red flags.

Hackers may use language or make requests that are out-of-character

While hackers can certainly craft perfectly believable correspondence, phishing emails may contain spelling errors, language or requests that are out-of-character, and branding inconsistencies.

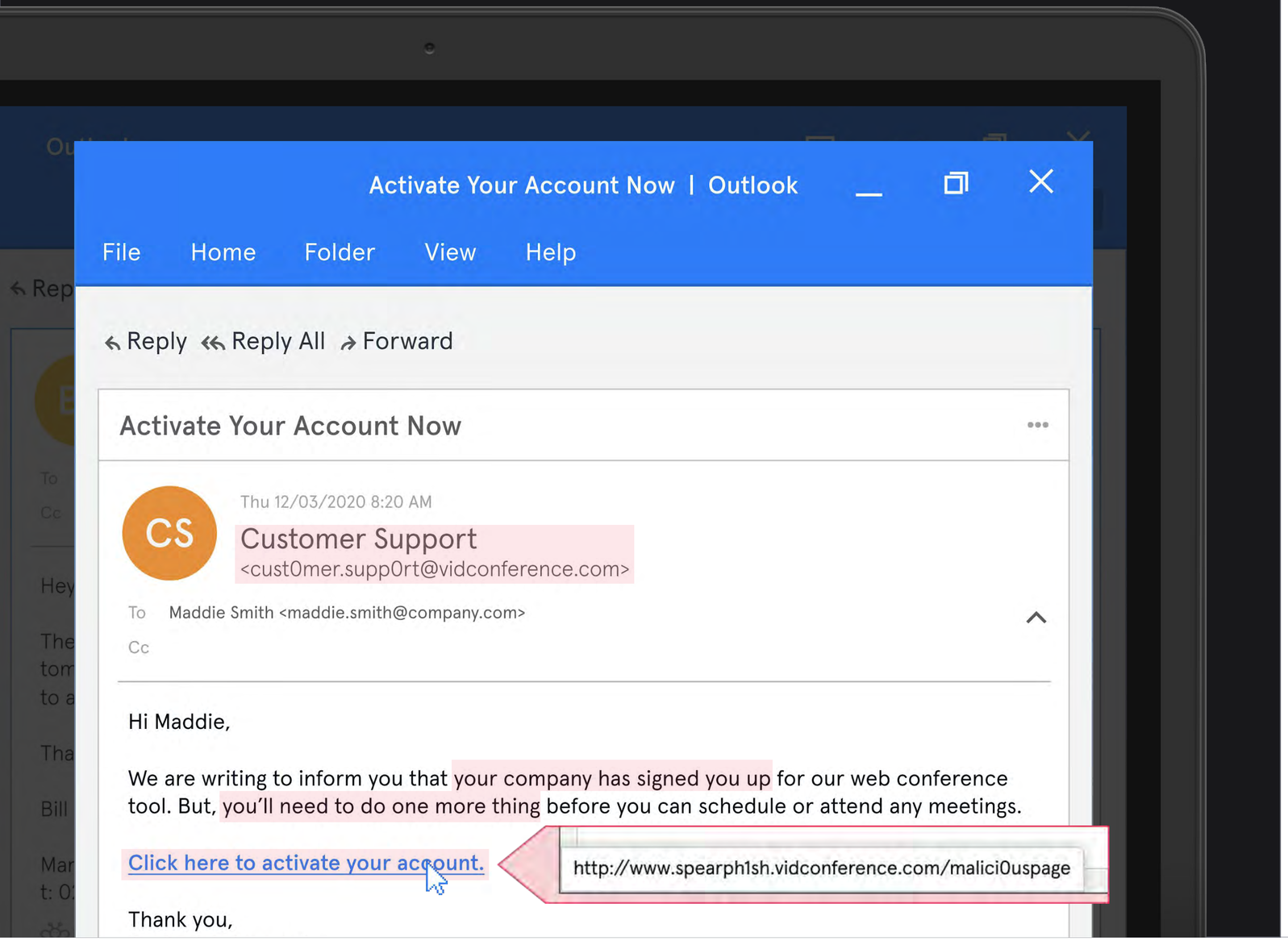


CORONAVIRUS AND CYBERSECURITY

The Out–Of– Office Boss

What's wrong with this email?

1. The sender's email address – which is in stark contrast to the Display Name – is from a freemail domain (@yahoo.com) and not from within the organization.
2. The attacker is giving the email a sense of urgency.
3. That attacker is using remote–working as a ploy to encourage the target to do something unusual.
4. The attacker is impersonating a person in power; this is common tactic in social engineering schemes.

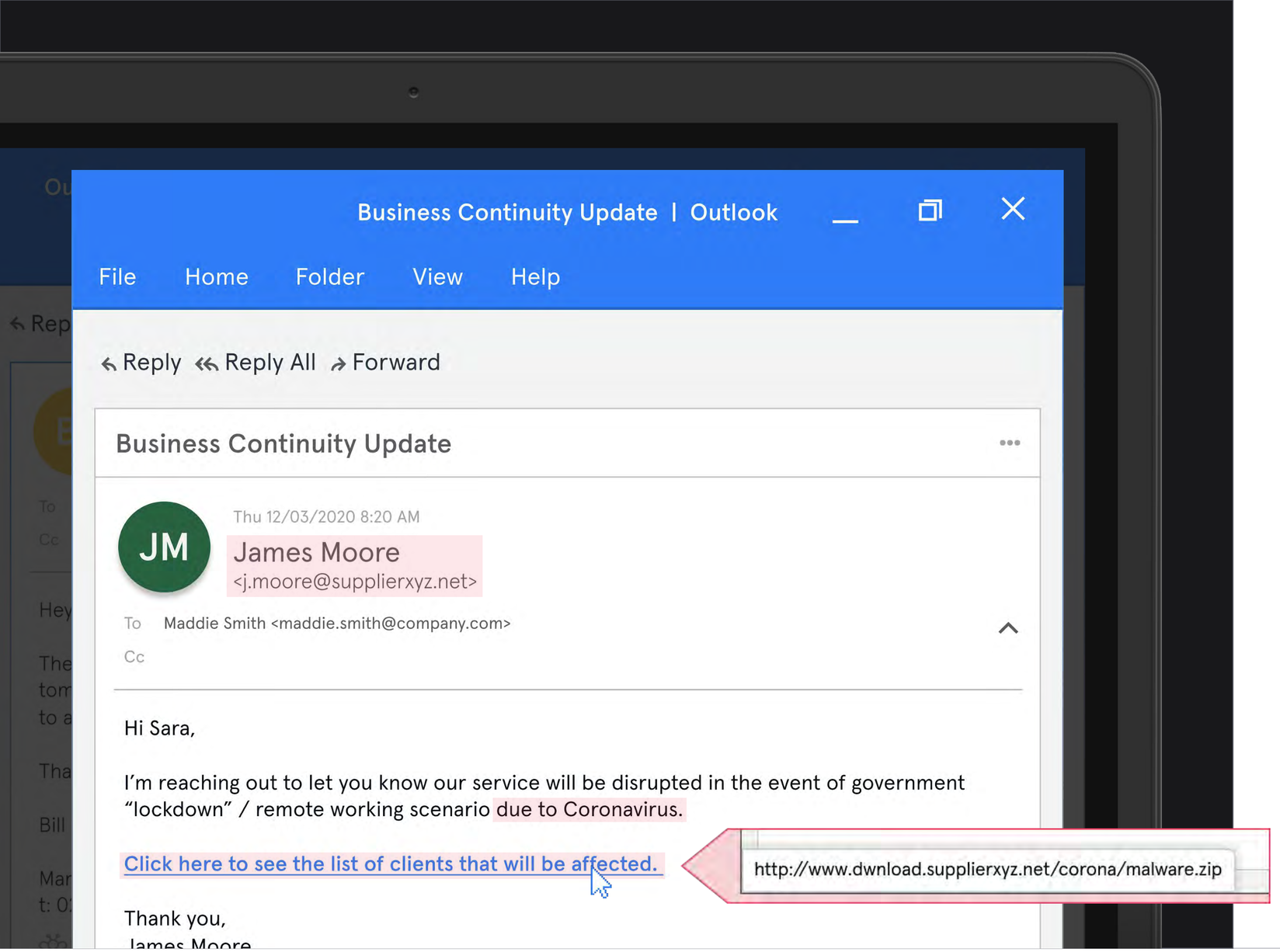


CORONAVIRUS AND CYBERSECURITY

The Fraudulent Third Party

What's wrong with this email?

1. The sender's email address contains irregular characters and doesn't match the Display Name.
2. Organizations should send internal communications to let their employees know they've implemented new tools or platforms. You shouldn't be hearing about it from the third-party first.
3. Upon hovering over the link, you'll see the URL is suspicious. Please note, though: A suspicious URL can still take you to a landing page that appears legitimate.



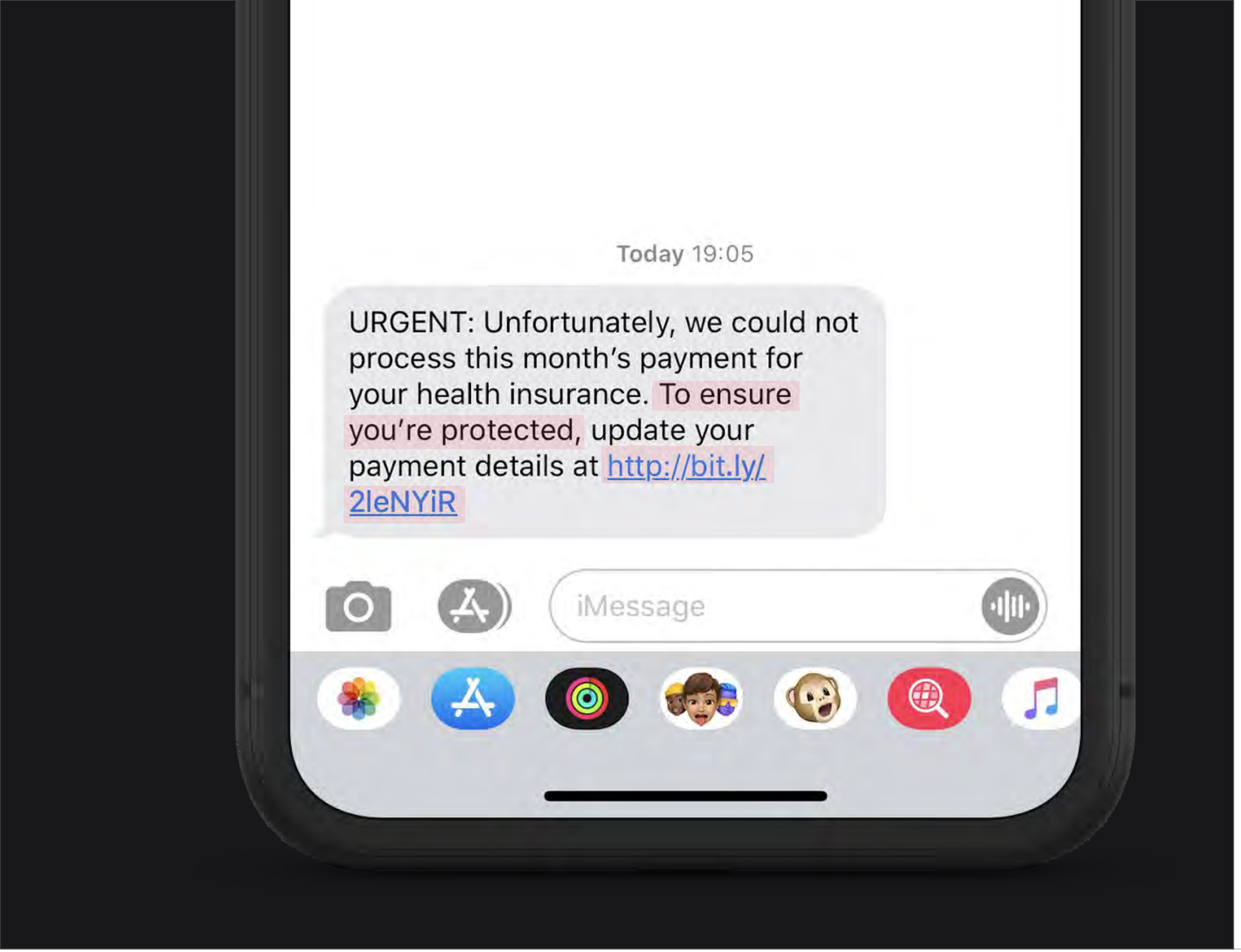
CORONAVIRUS AND CYBERSECURITY

The Concerned Counterparty

What's wrong with this email?

1. The top-level domain (.net) is unusual and inconsistent with previous emails from this supplier.
2. The attacker is using fear and urgency to motivate the target to act.
3. Upon hovering over the link, you'll see the URL is suspicious. Please note, though: A suspicious URL can still take you to a landing page that appears legitimate.

TESSIAN



CORONAVIRUS AND CYBERSECURITY

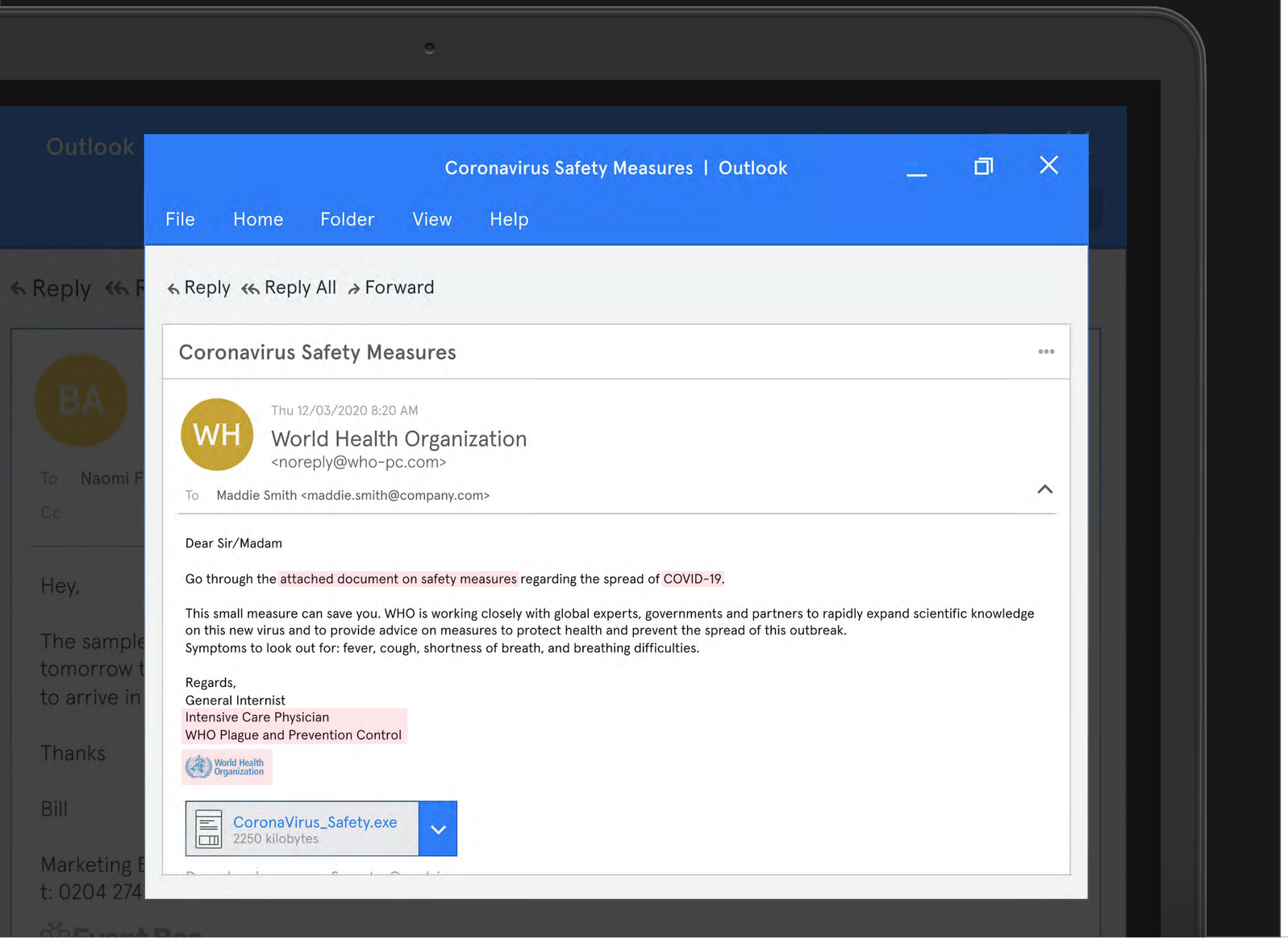
The Proactive Health Insurance Provider

What's wrong with this SMS?

1. The attacker is using fear to motivate the target to act.
2. Because no health insurance provider is mentioned by name, you can assume this text has been sent to a large pool of targets.
3. Legitimate organizations will never ask you to update your payment details via text.
4. The text message contains a shortened link; the target can't see the URL of the website they're being led to.

CORONAVIRUS AND CYBERSECURITY

The “Helpful” Government Organization



What’s wrong with this email?

1. All valid email correspondence from WHO will come from @who.int, not any other variation.
2. The attacker is using the fear of COVID-19 to motivate the target to download the malicious attachment
3. Like many other organizations, WHO has stipulated they will never send unsolicited emails containing attachments.

What to Do if You're Targeted

1.
If anything seems unusual, **do not follow or click links or download attachments.** Instead, visit the brand's website via Google or your preferred search engine, find a support number, and ask them to confirm whether the communication is valid.

2.
If the email appears to come from someone you know and trust, like a colleague, **reach out to the individual directly** by phone, Slack, or a separate email thread. Rest assured, it's better to confirm and proceed confidently than the alternative.

3.
If you're an employee who's been targeted,
contact your line manager and/or IT team.

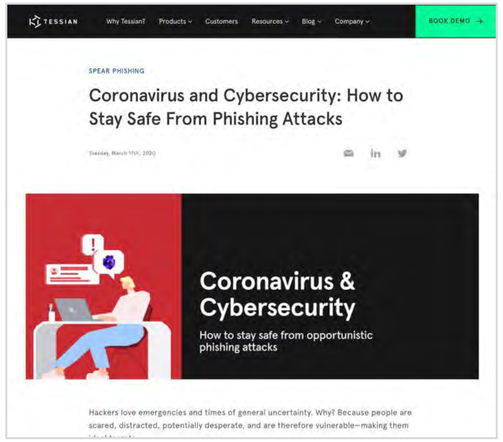
How to Avoid Being Impersonated

1.
For those of you who are working remotely or are otherwise Out of Office, **don't include any personally identifiable information (PII) in your automated emails** or on social media. For example, don't provide your personal mobile number or email address. Don't tell people to email a colleague in your absence; this information helps bad actors map connections and relationships within an organization, which can be used to make future phishing emails seem more convincing. Hackers can use this to their advantage to target your colleagues.

2.
Organizations should i**mplement SPF, DKIM, and DMARC** to prevent hackers from directly spoofing their domain.

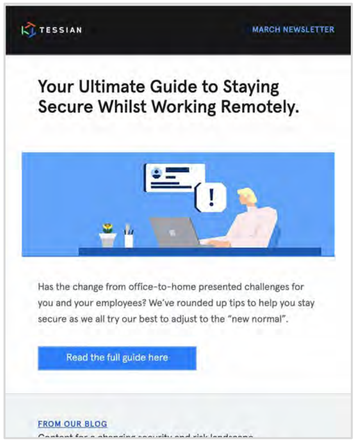
3.
Both brands and senior leadership should **advise customers and employees what they will and will not ask for** via email, phone, or text. People will then have a better sense of what requests are out of the ordinary and therefore suspicious.

We’re Here to Help.



For more information on how to stay safe from opportunistic phishing attacks.

Read the Blog Post →



We’ll be sharing more security tips. Be the first to know about new articles or updates.

Sign-Up For Our Newsletter →

TESSIAN