That email may be infected too

Managing the growing threat of phishing emails during the COVID-19 pandemic

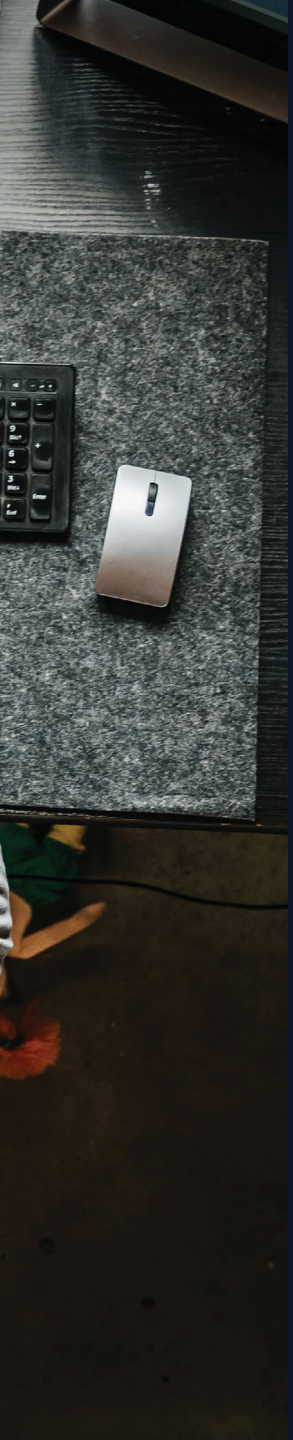
Legal, Compliance and Technology Executive Series

EY
Building a better working world

COVID-19 has upended work and home life for most of us. The shift to remote work and fears about the virus have led to a surge in phishing attempts, with cybercriminals moving quickly to take advantage of the new world reality.

Of special interest to:

Legal counsel
Corporate security officers
Information security executives
Compliance executives
Risk management executives
Internal audit



Scammers exploit the COVID-19 pandemic

Phishing and email scams have long been among the most popular and effective methods used by cybercriminals. They can be used to distribute misinformation, obtain illicit financial gain, and to seek personal and sensitive information from a victim. Employees victimized by attacks can expose critical company data located not just on their own computer, but throughout an entire network.

Now, COVID-19 is giving cybercriminals a new way to dupe anyone anxious about the pandemic. Scammers are sending emails that seem to come from legitimate organizations such as the World Health Organization, the US Centers for Disease Control and Prevention, and other government authorities.

Almost all the fraudulent emails come down to asking the recipient to either click on a link or open an attachment. Either action could result in activating a malware or redirect the user to enter confidential data.

Besides COVID-19 scams, other common scams are:

- **Accounting fraud:** A request from an accounting or a finance department or leader to approve an invoice payment, a journal entry, or other financial transaction
- **Social media spoofing:** A social media notification such as a friend request or a post you should "click to see"
- **Package delivery notification:** A package that requires the recipient to click on a link to confirm delivery or to check tracking status
- **Online shopping account spoofing:** Your online shopping account (e.g., Amazon, Apple) experienced suspicious access activity that requires you to click on a link to review or confirm
- **Password resets:** Your online social media account (e.g., Facebook, Instagram) has been compromised, it requires you to click on a link to regain access to your account

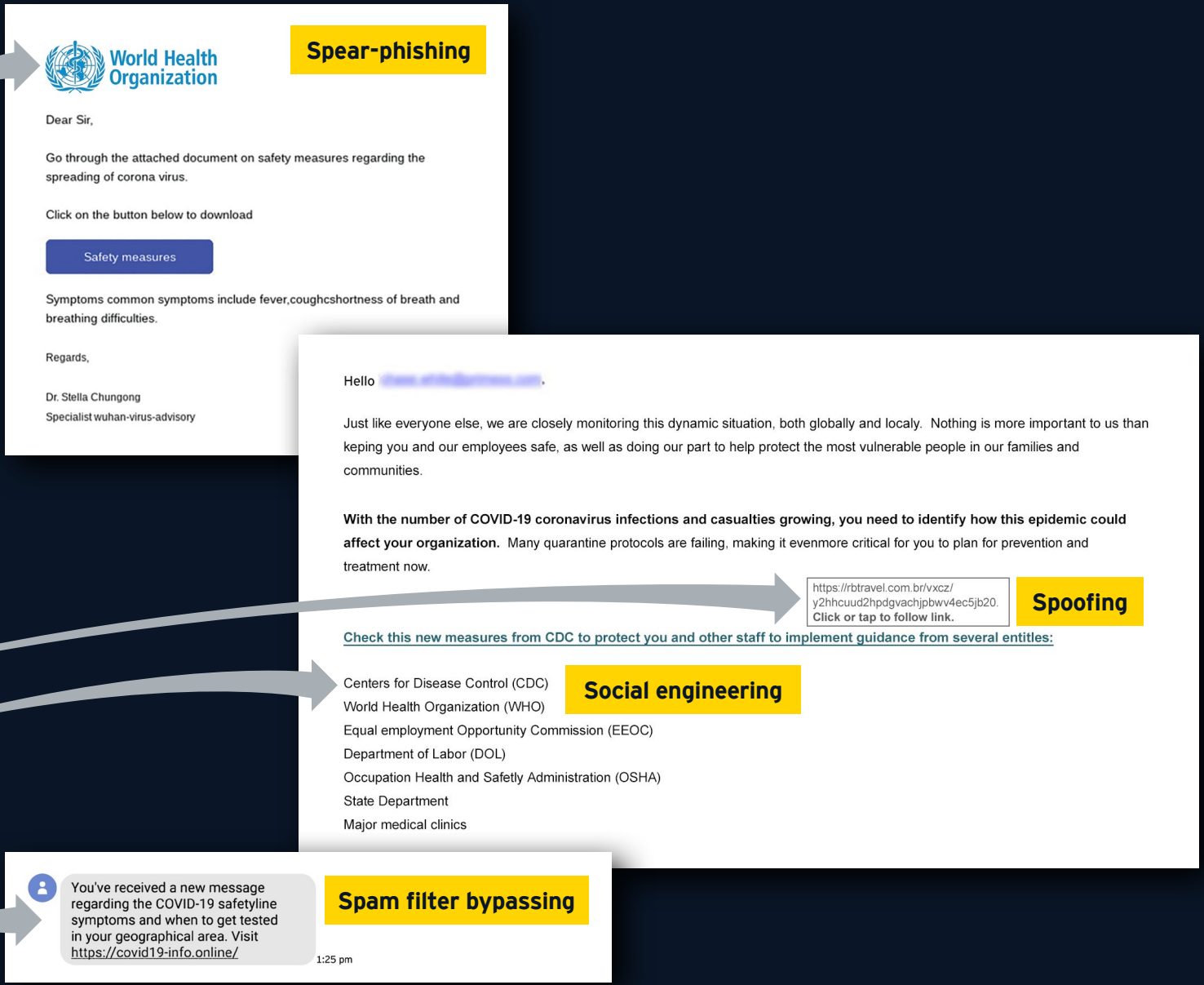
Common forms of phishing attacks

As with most phishing attacks, the criminals often use legitimate content sourced from reputable organizations to entice the reader to click on a link. The URL appears to be from a legitimate website but clicking on it infects the victim's computer by sending them to a malicious site that extracts their data.

Phishing attacks also prey on hunger for information in time of crisis by sending recipients attachments claiming to contain important health information. When the victim clicks on the document, they could unknowingly yield control of their computer to someone working remotely through embedded hidden code.

There are several avenues attackers have been exploiting to conduct phishing attacks. Some of the most common ones are:

- **Spear-phishing:** Faux emails, believed to be from a trusted sender, prompting victims to reveal confidential information or following links to credential harvesting websites or malware
- **Spoofing:** Using look-alike names to authoritative personnel, adding or switching domains to malicious sites, or using similar email or site layouts
- **Social engineering:** Leveraging LinkedIn and other publicly available information to map out corporate hierarchies and using the knowledge for executing educated spoofing attacks
- **Spam filter bypassing:** Tactics like zero-point font used to bypass spam filters that might be in place, often categorized as a more advanced spoofing


World Health Organization
Spear-phishing
Dear Sir,
Go through the attached document on safety measures regarding the spreading of corona virus.
Click on the button below to download
Safety measures
Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.
Regards,
Dr. Stella Chungong
Specialist wuhan-virus-advisory
Hello
Just like everyone else, we are closely monitoring this dynamic situation, both globally and localy. Nothing is more important to us than keping you and our employees safe, as well as doing our part to help protect the most vulnerable people in our families and communities.
With the number of COVID-19 coronavirus infections and casualties growing, you need to identify how this epidemic could affect your organization. Many quarantine protocols are failing, making it evenmore critical for you to plan for prevention and treatment now.
https://rbtravel.com.br/vxcz/y2hhcuud2hpdgvachjpbwv4ec5jb20.
Click or tap to follow link.
Spoofing
Check this new measures from CDC to protect you and other staff to implement guidance from several entitles:
Centers for Disease Control (CDC)
World Health Organization (WHO)
Equal employment Opportunity Commission (EEOC)
Department of Labor (DOL)
Occupation Health and Safetly Administration (OSHA)
State Department
Major medical clinics
Social engineering
You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/
1:25 pm
Spam filter bypassing

The move to work remotely raises the risks of phishing attacks

Phishing is certainly not new, but security experts report attacks are increasing due to the COVID-19 pandemic. As we exercise social distancing and spend more time working remotely, the risk of falling into phishing traps increases. Many face-to-face interactions have moved online and remote employees may be more inclined to use corporate laptops for non-business work. Employees using personal email accounts from corporate laptops can land on infected sites that steal sensitive company information.

> “
>
> A security researcher who goes online by the name of DustyFresh began tracking some of these domains last week.
>
> According to a list the researcher shared online, crooks have created more than 3,600 new domains that contain the “coronavirus” term between March 14 and March 18.[1]

Organizations have long been under the threat of phishing emails that impersonate a co-worker or a manager. You might get an email that appears to be sent by a colleague asking you to follow instructions to “transfer money,” “send financial data” or “allow access to confidential product information.” In the past, you might have called out to someone in the next cubicle to ask for verification, but if that’s not an option, you may automatically click on the link. As employees lose face-to-face contact, the risk of being victimized increases exponentially.

[1] Source: https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/

For more information, contact EY Cyber Response Services at:

CyberResponse@ey.com or visit us at: **ey.com/CyberResponse**

Staying vigilant can prevent successful phishing attacks

- Utilize your company's security measures for suspicious emails sent to your corporate address. For example, many businesses have tools in place that allow you to immediately flag any email you cannot readily verify.
- Review your company's cybersecurity guidelines and take training if needed.
- Use secure in-house corporate tools such as instant messaging and collaboration sites instead of email when possible. If you aren't comfortable with these tools, now is the time to adopt them.
- Check the email address of the sender to make sure the domain name is accurate. For example, **real.employee@acme.com** is not **realemployee@acmee.com**.
- Be cautious of generic emails that do not specifically address you.
- Question the authenticity if the email is full of grammar and spelling mistakes.
- Most email software (e.g., Microsoft Outlook) will advise you of suspicious email. Don't ignore those warnings.
- Use instant messaging or a phone call to contact a colleague who appears to be the sender of a suspicious email.
- Be cautious of instructions that ask you to download a file such as an invoice or a bank statement.
- When directed to a URL, check the address to determine if it's for a familiar website. Don't click on any link unless you can verify it.
- Don't perform any actions that are outside standard workflows (e.g., transferring money to process payments) without verification.
- Do not reply to emails that ask for personal information. Legitimate organizations asking for sensitive information will send you a secure link that encrypts data.
- Don't open attachments without verifying them. Contact the sender via phone or use a secure in-house communication tool to first confirm the authenticity of the documents.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

EYG no. 001483-20Gbl
WR #2003-3459650
ED None

ey.com

Contacts:

Global
Todd Marlin
todd.marlin@ey.com

Americas
Shawn Fohs
shawn.fohs@ey.com

Manish Khera
manish.khera@ca.ey.com

Asia Pacific
Chi Chen
chi.chen@cn.ey.com

Jack Jia
jack.jia@hk.ey.com

Nick Robinson
nick.robinson@hk.ey.com

Ichiro Sugiyama
ichiro.sugiyama@jp.ey.com

Europe, Middle East, India & Africa
Lorenz Kuhlee
lorenz.kuhlee@de.ey.com

Bodo Meseke
bodo.meseke@de.ey.com

Brenton Steenkamp
brenton.steenkamp@nl.ey.com