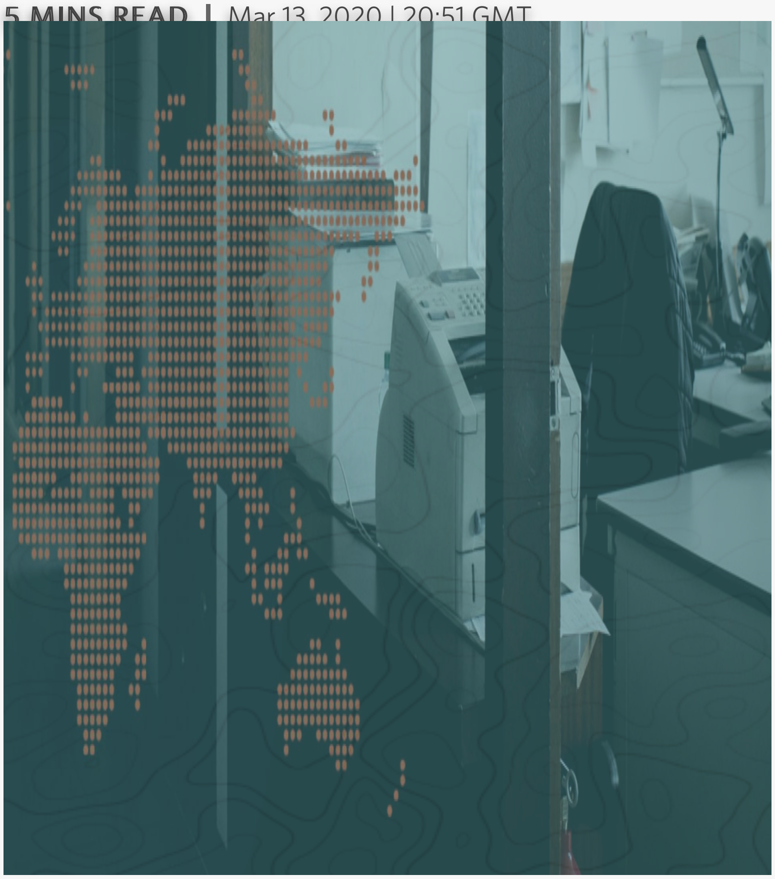
ASSESSMENTS

Ensuring Business Continuity in a World of COVID-19

Scott Stewart
VP of Tactical Analysis, Stratfor

5 MINS READ | Mar 13, 2020 | 20:51 GMT



(PHILIPPE LOPEZ/AFP/Getty Images)

HIGHLIGHTS

- *Employees can lessen the risk of having their data stolen by using VPNs and cellular data.*
- *We recommend that employees be educated about the wide array of phishing schemes seeking to capitalize on COVID.*
- *Employees should also be advised about business email compromise, sometimes referred to as "CEO scams" or "president scams," a growing risk as more business is conducted remotely and over email.*

Editor's Note: *This security-focused assessment is one of many such analyses found at Stratfor Threat Lens, a unique protective intelligence product designed with corporate security leaders in mind. Threat Lens enables industry professionals and organizations to anticipate, identify, measure and mitigate emerging threats to people, assets and intellectual property the world over. Threat Lens is the only unified solution that analyzes and forecasts security risk from a holistic perspective, bringing all the most relevant global insights into a single, interactive threat dashboard.*

Many companies are responding to the COVID-19 pandemic by reducing or banning corporate travel and by asking some or all of their employees to work from home. While having employees work from home will help reduce the transmission of the virus in the workplace, it also brings with it some additional risks, and we'd like to examine a few of them. As the disruptions from responses to COVID-19 mount, it is important to consider the second- and third-order impacts of the extreme efforts being put in place to curb the spread.

Public Wi-Fi

There are two basic ways that information can be targeted when an employee is using public wireless, either by someone in close proximity to the employee's computer as it is transmitting to the network, or by the person or business that owns and operates the wireless router. Because of this vulnerability, employees should assume that other people can see the information they are sending and receiving unless precautions are taken.

Using an encrypted public Wi-Fi network can reduce the risk of certain types of attacks, but the threat remains that the router could be compromised, or the person who owns it could still see traffic going through the router. The easiest way to reduce this threat is to avoid using public wireless. A cellphone used as a mobile hotspot can provide a safer, more secure connection to the Internet. In some cases, however, cellular service in the area may not be strong enough for the phone to be used as a hotspot, or this may not be an option based on the cellular plan.

If public wireless must be used, one way to reduce the risk of compromise is to ensure that all of the websites and apps connected to use encrypted connections. Certain browser plug-ins can help with this, including HTTPS Everywhere, developed by the Electronic Frontier Foundation. But unfortunately, many websites still do not offer any type of encrypted connection, and this approach is not ideal.

A more robust way to mitigate the risk of using public Wi-Fi is to use a virtual private network, or VPN. A VPN creates an encrypted "tunnel" from the computer to the VPN provider, which then forwards the traffic to the intended destination on the Internet. There are two different kinds of VPNs, corporate and personal. Corporate VPNs connect devices to a business's network, protecting business network traffic. Personal VPNs are specifically geared for the individual consumer or business traveler. Many different companies provide free or paid VPN services.

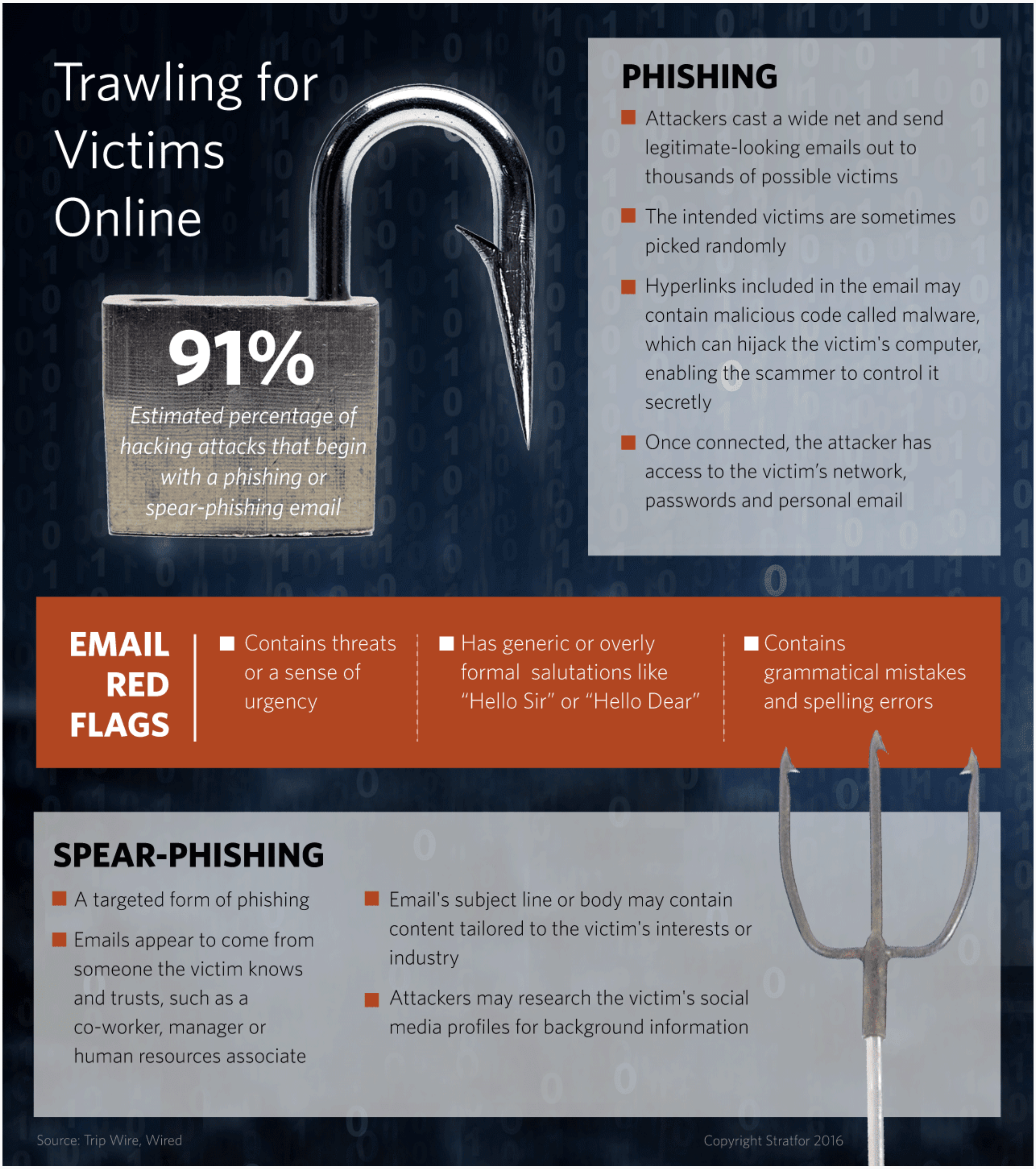
Corporate VPNs are more secure in that they establish a direct secure link (or tunnel) between the employee's device and the corporate system. But depending on how the VPN is accessed, a company may not have the capacity for all of its workers to simultaneously access the VPN. Because of this, it is important for IT teams to take this possibility into account when preparing contingency plans.

If a personal VPN is used, it is critical to remember that the vulnerability is simply being moved from the immediate public network to the VPN provider and beyond. If the websites and applications being accessed do not use encryption, then anyone between those sites and the VPN provider (as well as the VPN provider) will be able to see this data.

The good news is that the perpetrator is limited to accessing only information sent over the network; they cannot access information stored on individual devices. But there are other threats to that information.

Phishing and Business Email Compromise

As with every crisis, a wide array of phishing schemes has emerged attempting to take advantage of the mass hysteria generated by the COVID-19 pandemic. Some of these even claim to have a link that will take people to the widely respected, and very useful, Johns Hopkins COVID-19 website. We recommend that employees be educated about these threats, and be advised to take great care when sent emails with COVID-19 attachments or links. This should also include communications purporting to be from the company, from employees' children's schools or from the local governments, as email addresses can be spoofed.



Trawling for Victims Online

91%

Estimated percentage of hacking attacks that begin with a phishing or spear-phishing email

PHISHING

- Attackers cast a wide net and send legitimate-looking emails out to thousands of possible victims
- The intended victims are sometimes picked randomly
- Hyperlinks included in the email may contain malicious code called malware, which can hijack the victim's computer, enabling the scammer to control it secretly
- Once connected, the attacker has access to the victim's network, passwords and personal email

EMAIL RED FLAGS

- Contains threats or a sense of urgency
- Has generic or overly formal salutations like "Hello Sir" or "Hello Dear"
- Contains grammatical mistakes and spelling errors

SPEAR-PHISHING

- A targeted form of phishing
- Emails appear to come from someone the victim knows and trusts, such as a co-worker, manager or human resources associate
- Email's subject line or body may contain content tailored to the victim's interests or industry
- Attackers may research the victim's social media profiles for background information

Source: Trip Wire, Wired

Copyright Stratfor 2016

Speaking of business emails being spoofed, we also anticipate that business email compromise, sometimes referred to as "CEO scams" or "president scams," will increasingly become a risk as more business is conducted over email remotely – and cybercriminals seek to take advantage of the situation. This is an old, but growing social engineering threat in which hackers impersonate corporate officers and send an email requesting a wire transfer of funds to an account for some plausible reason, or for a fraudulent invoice to be paid out. Such attacks seek to intimidate employees into complying with instructions by combining the appearance of legitimacy with the pressure of an urgent appeal from a corporate authority figure. It is critical that employees be educated about such scams, and be encouraged to double-check with the person requesting a transfer or payment before actually executing it.

Connected Content

Regions & Countries	United States
Topics	Cybersecurity

Article Search

United States and Cybersecurity

Most at Risk in the Places You Least Expect

Dec 03, 2019 | 12:12 GMT

Resilient

Espionage