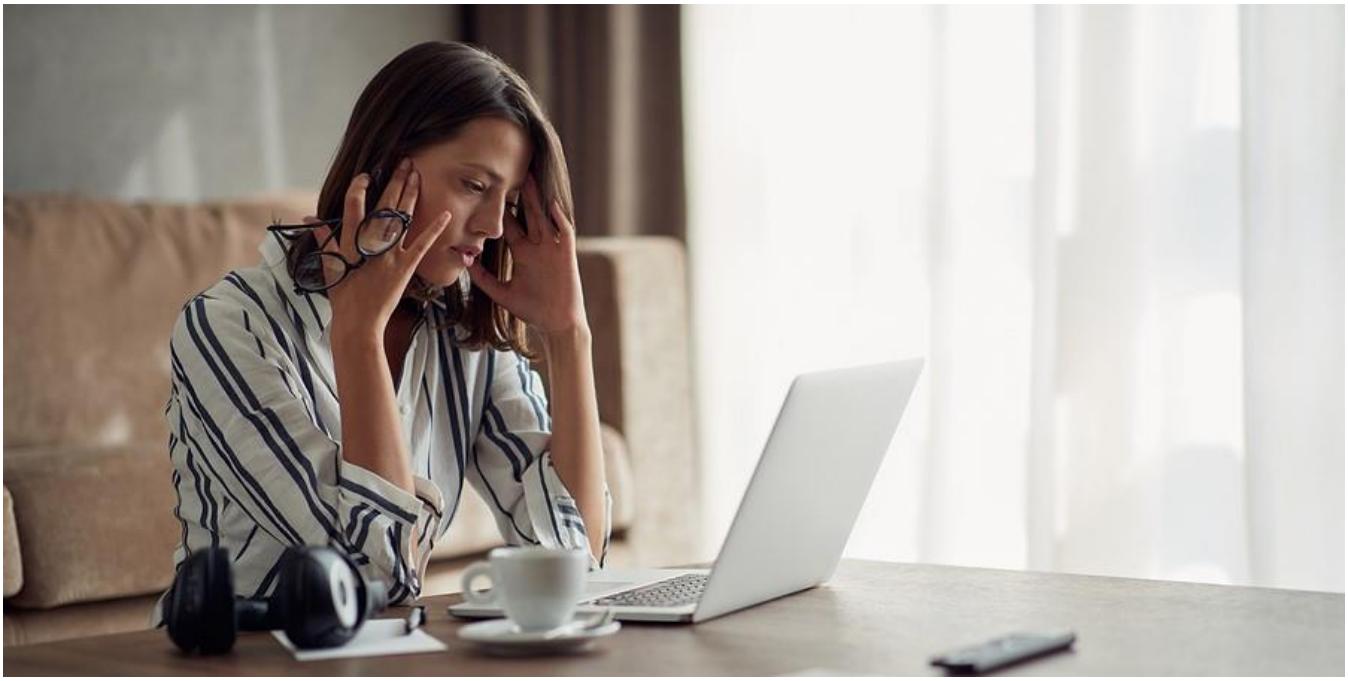
Coronavirus Phishing Attacks Target Remote Workers



Spurred by social distancing orders, the American workforce is returning home. In fact, Netskope Threat Labs reports that 58 percent of users worked remotely last week. This compares with an average of 27 percent prior to the pandemic. Unfortunately, researchers have also recorded a corresponding spike in coronavirus phishing attacks.

Cyber criminals love a crisis, from terror attacks to natural disasters. Using emotional appeals and a sense of urgency, they trick users into surrendering sensitive information or unknowingly downloading malware. And most of the time, they use email to launch the attack.

Remote Work Raises the Risk

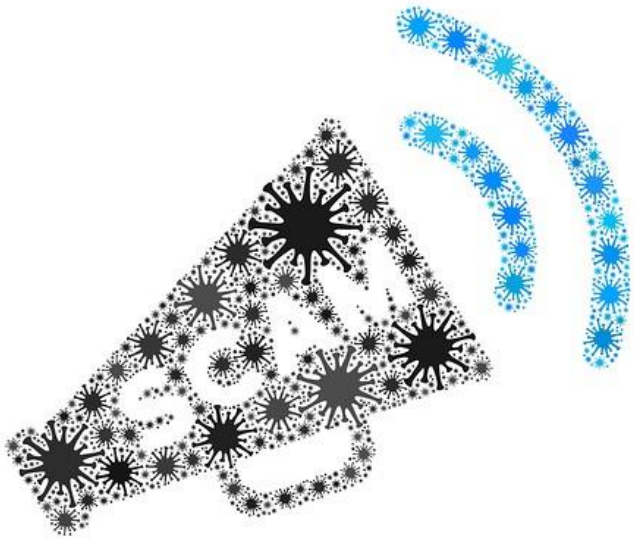
While advances in network technology and mobile devices have made work at home possible, remote work increases the attack surface and, consequently, the risk. Employees often work outside the usual security perimeter from home networks already crowded with IoT devices like gaming consoles, TVs and appliances.

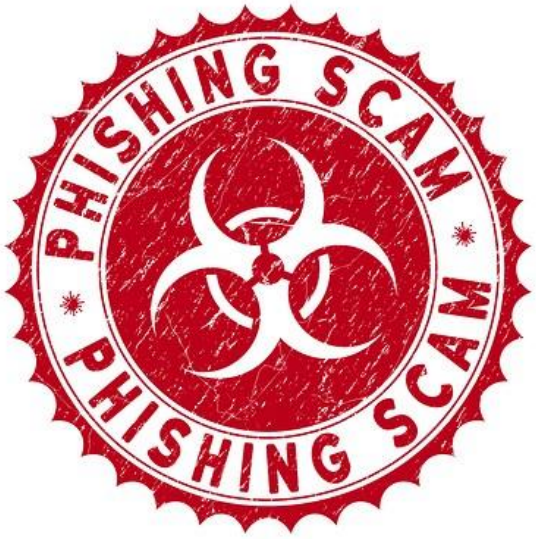
These home networks (or, worse, public Wi-Fi) often lack the security measures of corporate networks. And in a crisis like this pandemic, criminals count on the changing work environment to overwhelm and distract IT departments. Security professionals must address the challenge of protecting hundreds of new devices while providing additional avenues for workers to connect.

In today's world, there may be two classes of home worker and therefore two threat levels:

1. **Company A is already Remote Worker ready**. They have cloud-based systems with proper authentication or MFA or have Remote access through VPN or Terminal Servers. Therefore, the home worker is an extension of the corporate system and the risks have not changed. The attacks have simply masked and multiplied.

2. **Company B is not setup very well for Remote Workers**. It has employees either using their personal email or working from applications and data running on their local workstation. These users are at risk from increased phishing attacks but now also suffer added levels of risk due to lower levels of protection on personal email accounts and workstations.





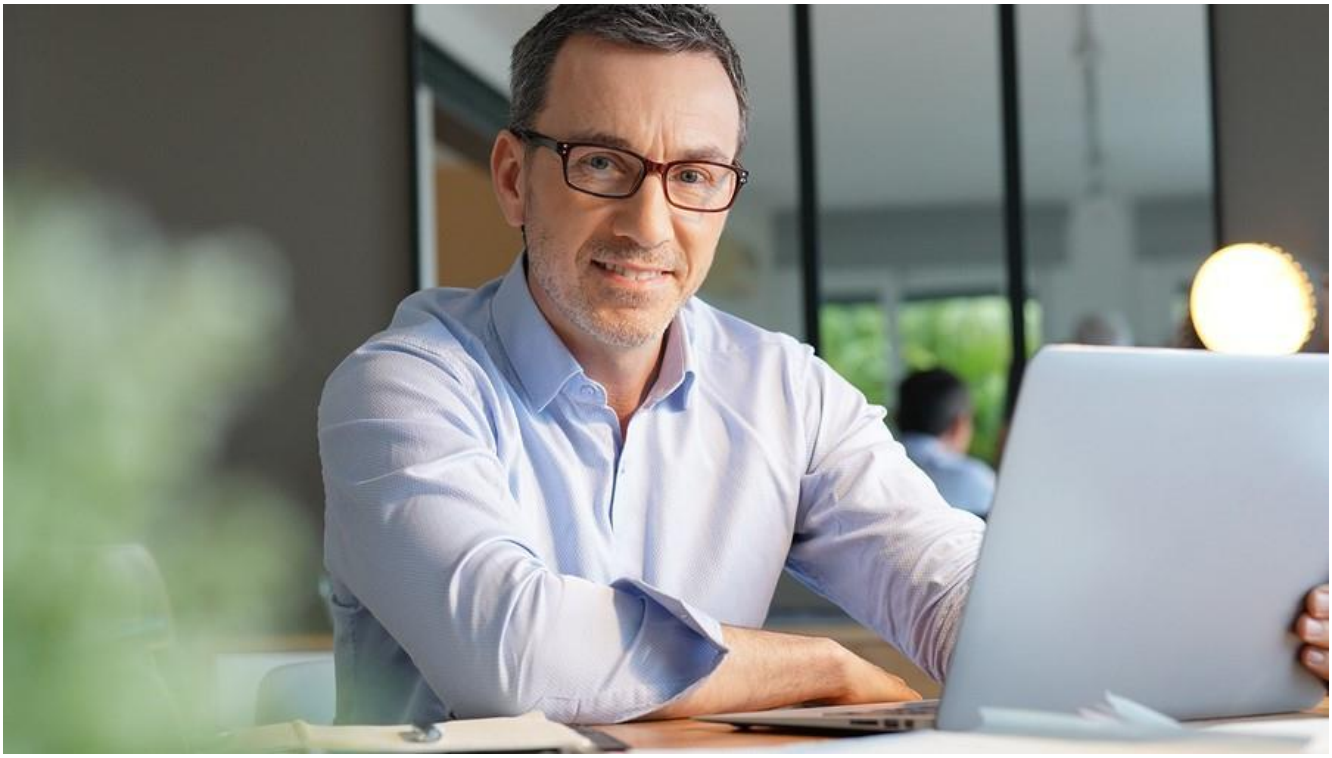
Signs of Coronavirus Phishing Attacks

Workers can help secure the organization and its information assets by learning to recognize and guard against social engineering scams. Criminals use many of the same phishing techniques they have used successfully for years. Additionally, coronavirus phishing attacks include some features specific to this situation.

For example, hackers often spoof the email addresses of trusted executives or HR employees and distribute emails that supposedly provide important company policies. Remote workers expecting such updates click without thinking. However, the attached "policy" actually downloads malicious code.

In other common attacks, phishing emails seem to come from official organizations like the CDC or WHO and promise important information about the virus. Some even use a legitimate, interactive COVID-19 map from Johns Hopkins University. But, again, malicious links or attached files infect the user's device with malware when clicked.

Users should keep in mind that no email from a legitimate government agency will request a login and password or other personal information. Additionally, knowing the URLs for these official agencies will help users spot a fake. For instance, an email from WHO will include "@who.int" rather than "who.com" or "who.org."



Tips for Organizations

Organizations should take steps now to protect against the increased risks attached to remote work. Ideally, the work environment at home should provide the same security available within the office walls.

- **Protect the network** – Implement Mobile Device Management (MDM).
- **Enable email protection features** – Double-check the email protection features of your email service. For example, ensure automated encryption to protect data both in transit and at rest.
- **Use multi-factor authentication (MFA)** – Never rely on passwords alone to secure remote work.
- **Educate employees** – Remind employees about emerging threats and common-sense email safety. Additionally, give them the information they need to ensure they have security measures in place at home. This should include password policies, as well as procedures for updating firewalls and other software and firmware.

Enlist Expert Help

In uncertain times, the last thing you need is to add panic about email security to your list of worries. Instead, partner with a trusted email consultant and cyber security provider to implement the necessary protections that will provide peace of mind.

The experts at Messaging Architects conduct comprehensive risk assessments and implement cyber security defense measures to guard against coronavirus phishing attacks and other threats to your network.