The global spread of the COVID-19 [coronavirus](https://www.helpnetsecurity.com/2020/03/11/coronavirus-evolve-security-architecture/) has had a notable impact on workplaces worldwide, and many organizations are encouraging employees to work from home. What are the cybersecurity implications of this shift?

The biggest issue is the increased number of cyber-attacks like phishing and malware, especially since employees will now likely receive an unprecedented number of emails and online requests. Ransomware and other malware prey on a user not thinking about security, expecting an anti-ransomware program to do their jobs. Regular [employee security awareness training](https://phoenixnap.com/blog/security-awareness-training-program) will remind your staff of their roles in preventing phishing attempts from getting through to your systems.

1. **Educate your team how to identify phishing attacks, scams, and good habits when working remotely.** Here are four ways to spot phishing attacks.

* **The email asks you to confirm personal information**

Often an email will arrive in your inbox that looks very authentic. Whether this email matches the style used by your company or that of an external business such as a bank, hackers can go to painstaking lengths to ensure that it imitates the real thing. However, when this authentic-looking email makes requests that you wouldn’t normally expect, it’s often a big giveaway that it’s not from a trusted source after all.

* **The web and email addresses do not look genuine**

It is often the case that a phishing email will come from an address that appears to be legitimate. Criminals aim to trick by including the name of a legitimate company within the structure of email and web addresses. If you only glance at this, they can look authentic, but if you take a moment to examine the email address you may find that it’s a bogus variation intended to appear authentic ‒ for example @mail.uber.work as opposed to @uber.com

Malicious links can also be concealed with the body of email text, often alongside genuine ones.  Before clicking on links, hover over and inspect each one first.

* **There’s a suspicious attachment**

Alarm bells should be ringing if you receive an email from a company out of the blue containing an attachment, especially if it relates to something unexpected. The attachment could contain a malicious URL or trojan, leading to the installation of a virus or malware on your PC or network. Even if you think an attachment is genuine, it’s good practice always to scan it first using antivirus software.

* **The message is designed to make you panic**

It is common for phishing emails to instill fear and panic in the recipient. The email may claim that your account may have been compromised, and the only way to verify it is to enter your login details. Alternatively, the email might state that your account will be closed if you do not act immediately. Ensure that you take the time to think about whether an email is asking something reasonable. If you’re unsure, contact the company through other methods.

1. **Educate your team on COVID-19 related phishing attacks, scams, and good habits when working remotely.**

AVOID COVID-19 SCAMS

* **Watch for phishing emails claiming to be from the CDC or WHO**. Use sites like coronavirus.gov and usa.gov/coronavirus to get the latest information. Never click on links from unknown sources.
* **Do not respond to texts, emails, or calls about COVID-19.** Delete the message and block the sender.
* **Ignore online offers for vaccinations and home test kits.** At this time, there are no products proven to treat or prevent COVID-19.
* **Hang up on robocalls.** Scammers use illegal robocalls to pitch everything from low-priced health insurance to fake work-at-home jobs.
* **Do your homework when it comes to donations.** Never donate in cash, gift card, or wiring money.

*Information sourced from* [*https://www.consumer.ftc.gov*](https://www.consumer.ftc.gov)

To learn about Cloud Proven’s high-level cloud-based data security protection that standard firewalls can’t provide, click on the link for SecureCloud™. <https://www.cloudproven.net/data-security>