CYBERSECURITY DURING A PANDEMIC

How to stay safe when working from home

As COVID-19 continues to spread across the globe, cybersecurity concerns are on the rise. Hackers love times of uncertainty. As a whole, people are scared, distracted, and working remotely – making you an ideal targeted.

Bad actors impersonating trusted institutions, individuals, and brands will become more prevalent. Even with companies tightening cybersecurity measures, hackers will continue with phishing and fraudulent attacks to gain personal records and install malware on your computer.

As we continue to rely on remote work, it's vital that individuals stay aware of how to keep themselves and their companies safe against cyberattacks. Below are some tips on how to spot this type of scam and what to do in case you're targeted.

TYPES OF ATTACKS

Phishing Emails or Messages – Emails or messages that attempt to fool you into taking an action such as clicking a malicious link, opening an infected attachment, or filling out a form

Spear Phishing – Similar to phishing, but instead of randomly emailing groups of people the attacker targets specific individuals with a message relevant to their work or personal lives

C-Suite Fraud – Attackers pretend to be a senior leader from your organization to trick you into doing something you should not do, like transferring money or providing access to a secure database or system

Phone Calls – We've all received a scam phone call – similar to phishing, hackers can call you on the phone pretending to be an individual or organization you know and trust, such as a help desk or a vendor you work with normally

USB Drops – An intentionally placed infected media, such as a USB drive, in hopes that someone will pick it up and insert it into their computer

SIGNS YOU'VE BEEN HACKED

- Your antivirus program triggers an alert
- Your friends and coworkers are receiving odd emails or messages from you that you never sent
- Your password no longer works for one of your accounts
- You get a pop-up message saying your computer has been infected
- Your browser is taking you to random websites that you can't close

WHAT SHOULD YOU LOOK FOR?

Hackers will often:

- Impersonate trusted brands, people within your organization, or vendors you use
- Change, remove, or add a letter to a legitimate looking email address
- Make spelling and grammatical errors
- Be inconsistent with their branding
- Motivate you to act

To prevent being hacked, you should:

- Carefully inspect all emails, especially those coming from companies that would have your private information (banking accounts, social security number, or private contact information)
- Be cautious when responding to any internal email that mentions the sender being out of office and requires urgent action
- Look beyond the display name to identify the sender – display names can be easily changed but email addresses are more difficult to spoof
- Check for spelling and grammatical errors and make sure the branding of the logo, email template, and website all match
- Confirm the sender and check for all other signs of hacking before opening a file, clicking a link, or responding with personal details

WHAT TO DO IF YOU'RE TARGETED

If an email, message or phone call seems unusual it's always better to confirm and proceed confidentially than risk the alternative.

- Most importantly, don't click any links, open any attachments, or respond with private information before confirming it is a valid communication
- If the message is from someone you know and trust, reach out to them on a different channel (call them, message via your internal communication tool, or start a new email chain) to ask if they sent the original message
- Visit the brand's website, find their support number, and ask them to confirm whether the communication is valid
- If you are targeted through your work account, reach out to your IT department and let them know

For more tips on how to confidently secure your home while you work remote, we suggest checking out the SANS 'Creating A Cyber Secure Home' video.