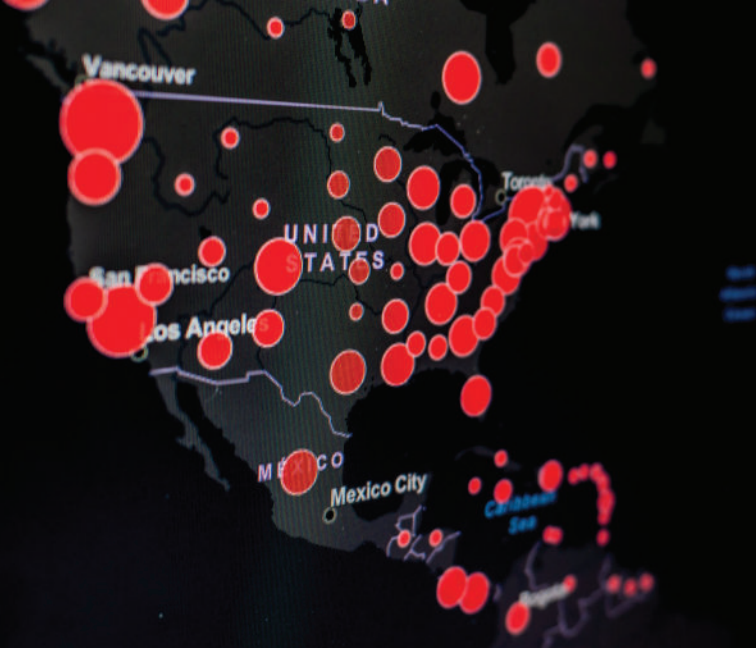


Staying CyberSecure During a Crisis

For some, working from home may be unfamiliar, while others may be accustomed to it. Staying secure while working remote can be easier with these quick tips.



As a result of the COVID-19 outbreak, cybercriminals are using phishing attacks to prey on coronavirus fears and targeting organizations that now have more remote workers and fewer IT and security staff. Binary Defense would like to offer some tips and tricks to keeping your data safe and secure.



Check sources of all emails and double check attachments or links before opening them. Hackers are generating content that mimics and functions like legitimate sources like the World Health Organization.



If you are seeking information, instead of opening an email, go to their official website for updated information.



When accessing email and other accounts set up two-step authentication. This process requires both something you know (your password) and a physical item you have (cellphone) to allow you into your accounts, offering more security for your sensitive documents.



Keep your work data specifically on your work computer, this ensures your data is staying on a device that is secure.



Do not use public Wi-Fi. If you are working at a coffee shop, try using a personal hotspot instead of connecting to an open connection that anyone can access.

With the cybercriminals developing new COVID-19 related attacks every day, no business is immune. Businesses of all sizes, in every industry, need advanced protection. Binary Defense offers Managed Detection and Response (MDR) and SOC-as-a-Service (SOC). Both deliver 24/7/365 monitoring to secure the remote workforce and stop cyberattacks.