Take These 3 Steps to Protect Your Data From Coronavirus (COVID-19) Scams

Coronavirus (COVID-19) isn't just a growing threat to public health – it's also a growing threat to your company's cybersecurity. From using scary subject lines to adopting faux official letterhead, bad actors are scrambling to use the climate of fear and disruption caused by COVID-19 to their advantage.

Disasters, emergencies, and global pandemics provide a target-rich environment for cybercriminals to launch phishing attacks and employ other dirty tricks to gain access to your data. It only takes one staffer opening a bogus email, clicking on a dangerous link, or downloading a malware-laden attachment for them to succeed. Here are three ways that you can act immediately to prevent a potentially disastrous Coronavirus-related data breach.

1 Plan, Preserve, and Protect

Use expert guidance from agencies like CISA to prepare your organization for risks posed by COVID-19. Is your cybersecurity plan adequate for the unique challenges presented by increased virtualization if your staff is quarantined or working remotely for safety? Two-factor authentication and other tools like VPN help keep your organization's data and systems safe even when workers aren't in the office.

2 Trust but Verify

Get updates about COVID-19, scams and frauds related to the Coronavirus pandemic, and its impact on cybersecurity from trusted, official sources, and encourage your staff to only use vetted information for planning and communications. Be wary of any email with a COVID-19-related subject line, attachment, or hyperlink. Avoid sharing or clicking on social media posts, text messages, or IMs offering Coronavirus information, vaccination, treatment or cures.

3 Make Prevention a Priority

Refresh every staffer's training on how to spot phishing scams and online fraud. Remind your staff that government agencies will never ask for sensitive personal, financial or business information via email. Reinforce that clicking on links or opening attachments from unfamiliar sources is a quick way for scammers to infect your systems with malware. Employee Security Awareness Training and Phishing Simulations can help make sure that your staff is ready to spot and defend against attack.

Constant vigilance against cyberattacks is a smart strategy for any business. In these uncertain times, we're happy to be your trusted source for the tools and strategies that you need to keep cybercriminals out of your business.

References:

https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf
https://www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines
https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams
https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing
https://www.cisa.gov/coronavirus
https://www.consumer.ftc.gov/blog/2020/03/ftc-fda-warnings-sent-sellers-scam-coronavirus-treatments