Protect Your Business from COVID-19 Phishing Scams

The list of states implementing stay-at-home orders continues to grow while the world scrambles to curb the spread of COVID-19. As a result, the number of employees working remotely has skyrocketed overnight. Unfortunately, COVID-19 phishing scams have also skyrocketed, with scammers taking advantage of relaxed security perimeters.

To protect the organization, businesses must implement additional security measures for the remote work environment. Employees working at home also need to take common-sense steps to work safely. And through it all, communication remains essential.

Examples of COVID-19 Phishing Scams

The most common COVID-19 phishing scams involve the tried and true method of spoofing authoritative sources. Frequently-spoofed organizations include the CDC (Centers for Disease Control), the WHO (World Health Organization) and your own HR.

For example, an email supposedly from the CDC advises readers to click a link to check out new measures to protect businesses and their employees. Another purports to come from HR, with an attached flyer for readers to print and post. Unsuspecting employees can surrender their credentials in seconds, opening the door for hackers.

In another widely-used COVID-19 phishing scam, malicious websites and emails use a legitimate, interactive COVID dashboard from Johns Hopkins University to deploy malware. This scam combines accurate, real-time information with malicious code, allowing hackers to attack the system from outside the usual defense perimeter.

Implement Multi-layered Security and Disaster Recovery

- If you have not already implemented a reliable business continuity and disaster recovery plan, do so now.
- Use multi-factor authentication (MFA) wherever possible.
- Use encryption to protect sensitive data from interception.
- Make use of Domain Name System Security Extensions (DNSSEC) and geo-fencing to minimize the threat landscape.
- If you have not already implemented a Mobile Device Management (MDM) system, do it now.

Tips for Employees Working Remotely

- Close all non-essential applications and web browsers while working.
- Avoid using public Wi-Fi connections.
- Check computers and all mobile devices used for work. Install security patches as necessary for system software and other programs. Keep antivirus software up-to-date and scanning.
- If you have not already done so, set up encryption for your laptop/tablet storage, and keep the encryption keys in a safe location.
- If you work in a public area, do not leave devices unattended while working. Lock your computer when you step away.
- Do not let your guard down. Cyber criminals get more sophisticated every day, and they have no problem taking advantage of crisis thinking. Practice common sense.

Communication Checklist

- Ensure that your employees know company procedures for handling security incidents.
- Some employees have less of a comfort level with technology than others. Make sure they know who to call for help working safely.
- Implement a reliable system to keep staff up-to-date. Email works. However, a communications platform like Microsoft Teams works more quickly and efficiently.
- Add a caution message to the beginning of all external emails instructing your staff to verify important emails by calling the sender. This is particularly important for emails that instruct them to make a change or send funds somewhere.
- Take the opportunity to remind employees about common-sense cyber security tips.

Enlist Help in Building Security for Uncertain Times

eMazzanti cut its teeth in crisis, opening in New Jersey less than one month before September 11, 2001. We have supported our customers through terror attacks, hurricanes, floods, ransomware and more. With deep expertise in enterprise security and crisis control, we will help you keep your vital information assets secure and available.