5 ways to Protect Your Business from COVID-19 Phishing SCAMS

Since the COVID-19 pandemic began, cybercrime has increased by up to 300%. According to cyber security experts, a big part of that increase has come in the form of COVID-19 phishing scams. Now more than ever, organizations must remain hyper-vigilant to protect assets and employees from attack.

With many employees working from home (WFH), everyone appears to be a target. With expanded security perimeters, reports of phishing attacks are way up, even within our own organization.

Current COVID-19 Phishing Scams

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

For example, an email that appears to be from the CDC urges readers to click a link to consider new measures to protect businesses and their employees. Another message claims to come from HR, with an attached flyer for readers to print and post. Unsuspecting employees quickly surrender their credentials, opening the door for hackers.

Recently, an eMazzanti Technologies staff member received multiple phishing emails seeking to take advantage of the crisis work environment. The messages requested payment and referenced invoice numbers and information obtained from emails previously stolen from a vendor.

5 ways to Protect Your Business

To protect the organization, WFH employees need to take common-sense steps to work safely. Likewise, businesses must implement additional security measures for the remote work environment. And through it all, communication remains essential. Ideally, the WFH environment should provide the same security available at the office.

1. Implement Multi-layered Security and Disaster Recovery

- First, implement or update a reliable business continuity and disaster recovery plan so data can be recovered quickly if compromised.
- If you have not already implemented a Mobile Device Management (MDM) system, do it now.
- Make use of Domain Name System Security Extensions (DNSSEC) and geo-fencing to minimize the threat landscape.

2. Thoroughly Train Employees

Regularly educate employees about emerging threats and common-sense email safety. Additionally, give them the direction they need to ensure they implement security measures at home. Include password policies, as well as procedures for updating firewalls and other software and firmware.

Tips for Employees Working Remotely

- Install security patches as necessary for operating systems and other programs on all computers and mobile devices used for work. Keep antivirus software scanning and up to date.
- Set up encryption for your laptop/tablet storage and keep the encryption keys in a safe location.

- Close all non-essential applications and web browsers while working.
- Avoid using public Wi-Fi connections and leaving devices unattended in public areas.

3. Enable email protection features

Review and employ the email protection features of your email service. For example, ensure automated encryption to protect data both in transit and at rest.

Outlook offers multiple options for Junk email filtering, including No Automatic Filtering, Low, High and Safe Lists Only. Users may also disable links in phishing emails and select an option to receive warning messages about suspicious domain names in email addresses.

4. Strengthen Access Management

Employ a layered approach to access management. Start with automatically enforcing strong password policies. Then bolster defenses with multi-factor authentication (MFA). To achieve a balance between security and usability, define access based on risk.

For instance, system administration activities present greater risk, as do connections from certain locations. Define risk-based access that requires MFA for these and other higher risk activities.

5. Deliver Regular Security Updates

All organizations should implement a reliable system to keep staff up to date on security matters. That might be email or a communications platform like Microsoft Teams that works more quickly and efficiently. Take the opportunity to remind employees about common-sense cyber security tips.

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.

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.

Building Security in Times of Crisis

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.

Reduce the risk of COVID-19 Phishing Scams and other security threats by strengthening email and WFH security. Partner with trusted email consultants and cyber security professionals to implement the necessary protections to deliver peace of mind.

The email experts at Messaging Architects conduct comprehensive risk assessments and implement cyber security defense measures to guard against COVID-19 phishing scams and other threats to your network.