STRATEGIC MANAGEMENT SERVICES

FBI Alerts Businesses and Teleworkers of Cyber Risks During COVID-19 Crisis

By Richard Kusserow | April 23, 2020

- **Cyber criminals are compromising cloud-based email services costing businesses more than $2 billion.**
- **COVID-19 scams target: teleworkers, first responders, medical facilities**
- **FBI tips to guard against attacks.**

The Federal Bureau of Investigation (FBI) has issued an alert stating that cyber criminals are mimicking popular cloud-based email services to compromise business accounts and exploit the COVID-19 pandemic to perpetrate fraud in telework environments. The scams are initiated through phishing kits which are designed to mimic the cloud-based email services in order to fraudulently request or misdirect transfers of funds using stolen credentials. Since 2014, the FBI Internet Crime Complaint Center (IC3) has received complaints totaling more than $2.1 billion in actual losses from scams mimicking two popular cloud-based email services. These scams often use phishing kits that impersonate popular cloud-based email services by identifying the service associated with each set of compromised credentials and targeting the victims. Once the email account has been compromised, cyber criminals use the information from the account to impersonate email communications between compromised businesses and third parties to request that pending or future payments be redirected to fraudulent bank accounts. In recent weeks, cyber scammers have engaged in phishing campaigns against first responders, launched denial-of-service attacks against government agencies, deployed ransomware at medical facilities, and created fake COVID-19 websites that download malware to victim's devices. The FBI offers the following tips:

- Enable multi-factor authentication for all email accounts;
- Verify all payment changes and transactions in person or via a known telephone number;
- Educate employees about identifying phishing emails and responding to suspected compromises;
- Prohibit automatic forwarding of emails to external addresses;
- Add an email banner to messages coming from outside your organization;
- Prohibit legacy email protocols (POP, IMAP, and SMTP) that circumvent authentication;
- Ensure changes to mailbox login and settings are logged and retained for at least 90 days;
- Enable alerts for suspicious activities, such as foreign logins;
- Enable security features that block malicious emails;
- Implement anti-phishing and anti-spoofing policies;
- Disable legacy account authentication; and

- Configure Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication Reporting and Conformance to prevent spoofing and validate emails.

Strategic Management compliance consultants have over 40 years of experience in providing research, analysis, and program support for privacy and security rule compliance. Call us at (703) 683-9600 or contact us online for a tailored assessment of your organization's particular needs.