Emails Seemingly Sent from the Small Business Administration Regarding COVID-19 Loan Relief Could Be Phishing Emails: Exercise Caution!

Amundsen Davis Data Privacy & Security Alert
August 14, 2020

The Small Business Administration (SBA) has been added to the list of organizations recently targeted by cyber threat actors. The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is currently tracking an unknown malicious actor (or actors) spoofing the SBA's COVID-19 relief webpage via phishing emails. These emails include a bogus link to a fake SBA login page used for malicious redirects and credential stealing.

What can you do?

- **Be Alert.** If you are a company that benefits from SBA small business loans then your due diligence around logging-into and accessing accounts should be heightened. Be aware of potential phishing emails and make sure to notify your organization so that all employees stay vigilant.
- **Watch for Suspicious Links.** CISA released an alert to show businesses how the malicious link will appear. Given the growing sophistication of threat actors, even the web address looks legitimate, so it is understandable why organizations may readily conclude that the link is legitimate. However, there are other red flags within the link including a ".com" web address to a consulting website. As these attacks become more advanced, it is important to remind your employees to be extremely cautious when clicking on links within an email. Double and triple checks of emails from outside sources are appropriate. And, when it doubt, contact your IT department.
- **Strengthen Your Security.** Depending on the strength of your security system, it can be easy for this type of spoofed email to make its way into your inbox. Now is a great opportunity to strengthen the security posture of your organization's system. Some of the implementations recommended include maintaining up-to-date antivirus signatures and engines, ensuring the latest security updates, enforcing a stronger password policy, and enabling a personal firewall for employees.

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

COVID-19 Resource Center & Task Force

Cybersecurity & Data Privacy

This cyber threat, found at the intersection of a continued, favorite tool of threat actors (phishing emails) and the daily stress for small businesses (the financial impact of COVID-19), is only the latest in a string of malicious attacks of businesses' data security systems. Regular training and updating of cyber-security practices remain crucial.

Emails Seemingly Sent from the Small Business Administration Regarding COVID-19 Loan Relief Could Be Phishing Emails: Exercise Caution!