Watch out for the COVID-19 Loan Relief Scam

The COVID-19 Pandemic has led to challenges for many businesses over the last few months, including financial stress related to the pandemic. In an effort to help relieve some of the stress, the Small Business Administration (SBA) has offered relief programs to qualifying businesses to help weather financial setbacks.

These programs are meant to help businesses in need, however, many applicants found themselves victims of scammers who are pretending to be the SBA looking to garner personal information. Some business owners are anxious to hear back from the SBA about their loan. Here is what small business owners need to be aware of so that they can protect their information.

Email Phishing Scam

The Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) received reports earlier this month that fraudsters were sending out phishing emails that appear to be coming from the Small Business Administration, but are actually coming from scammers. These phishing emails are targeting local business owners who may have applied for the SBA's Economic Injury Disaster Loan Program and usually lead with a subject line such as "SBA Application – Review and Proceed," in hopes of creating a sense of urgency for the receiver.

The emails reference COVID-19 loan relief from the SBA and prompt users to click on a malicious link. When recipients click on the link they are taken to a fake SBA website that has an SBA logo, which redirects to another page where users are prompted to enter in their login credentials for the SBA website. The goal of this scam is to steal the login credentials of users and then use those credentials to access important information for fraudulent use.

What You Can Do

We know how frustrating it can be to deal with scammers, especially when it comes to your business. Here are some ways you can protect yourself and your business so that you do not fall victim to this phishing scam.

Check the Email Address

One sure-fire way to make sure you are communicating with the right person is to double check the email address of those with whom you are corresponding. Any email communication from the SBA should come from the domain @sba.gov. Any email address with a different domain that is referring to an SBA loan should be reported.

Check Any Links

If an email provides links to click on, quickly hover over the link address to make sure it is going to a reputable location. If a link leads you to a web address that is unfamiliar to you, it should be reported.

Do Not Provide Information to Third-Parties

Some scammers are telling recipients that they are a third-party working with the SBA, however, this is not true. The SBA does not use third-party contractors or platforms to gather information from applicants, so anyone making this claim is a scammer.

Report Suspicious Emails

If you believe that you have received an email that is from a fraudster, make sure to report it to the SBA by either calling this hotline number 800-767-0385 or visiting the SBA Scams and Fraud Alerts page at: https://www.sba.gov/document/report-sba-programs-scams-fraud-alerts.

Here at Blackhawk Bank, we want to make sure that business owners are taking extra precautions to protect their information. To learn more about Blackhawk Bank and how we can help your business, contact us today!