Scam of the Week: Exploiting the Coronavirus: Financial Relief Scam Targeting Organizations

The coronavirus pandemic continues to impact organizations across the globe. This hardship gives cybercriminals the perfect bait: a promise of financial relief. Currently, cybercriminals are impersonating the United States Small Business Administration (SBA) with a very convincing phishing email. While this specific scam targets organizations in the US, this tactic could be used in any country, for any kind of relief fund.

The phishing email states that your loan application has been approved and it includes a link to “start the funding process”. If you click this link, you are taken to a phony login page that is nearly identical to the SBA's official website for the relief fund. The bad guys are phishing for these specific login credentials to gain access to sensitive data, such as your organization’s federal tax ID and banking information. This type of information, in the hands of a cybercriminal, would be a disaster.

Here’s how you can stay safe from scams like this:

- Never click on a link in an email that you were not expecting.
- When an email asks you to log in to an account or online service, log in to your account through your browser and not by clicking the link in the email. That way, you can ensure you’re logging in to the real website and not a phony look-alike.
- Call the organization in question. Just be sure to look up the official phone number—do not call the phone number provided within the email.

Stop, Look, and Think. *Don't be fooled.*
The KnowBe4 Security Team
KnowBe4.com