URGENT: Accredited Businesses Targeted by Phishing Scam

Unknown scammers began sending a wave of bogus emails to business owners and consumers. These emails were disguised to look like Better Business Bureau correspondence and asked people to open an attached Standard Business Questionnaire (SBQ), a form that BBBs use to gather information from businesses to create or update Business Reviews.

This attachment, however, delivers malware to the user's computer, and should NOT be opened.

The Council of Better Business Bureaus (CBBB) has contacted its security vendor and initiated a takedown of the malicious site(s) behind this phishing scam. Over the past three years, BBB has taken down nearly 200 fraudulent sites of this kind.

Here are three ways to identify these scam emails:

The From line is "BBB Accreditation Services firstnamelastname@newyork.bbb.org.
The Subject line references “BBB SBQ Form” along with random reference numbers.
The malicious attachment is labeled “BBB SBQ Form.zip.”
The return addresses in the phishing emails are protected by CBBB’s use of DMARC (Domain-based Message Authentication, Reporting & Conformance), which helps protect recipients from fraudulent email. End users without DMARC filtering, however, must rely on their own spam filters for protection.

CBBB is asking that anyone who receives one of the fraudulent emails to forward it to phishing@council.bbb.org.

Media:
Evan Kelly, Senior Communications Advisor
BBB serving Mainland BC
604-488-8702