SMALL BUSINESS BIG THREAT

Known Covid-19 Cyber Scams

As the Covid-19 pandemic continues, cybersecurity researchers have seen a study rise of Covid-19 related cyber scams. The goal of these scams is to obtain personal information like full names, addresses, Social Security numbers, payment information, etc. Be on the lookout for the following cyber scams:

1. Clinical Trials – You may receive phishing emails or vishing calls asking for volunteers for a clinical trial of a vaccine.
2. Personal Protective Equipment (PPE) Scams – You may receive phishing emails or vishing calls stating a give-a-way of masks and other PPE items or you may be told of businesses and organizations who are hoarding masks and other PPE items and asking you to act against those who are hoarding.
3. Stimulus Fraud – You may receive phishing emails or vishing calls stating your stimulus payment is ready to be delivered.
4. Grant Fraud – You may receive phishing emails or vishing calls stating business grants are ready to be delivered and your small business qualifies.
5. Donation Fraud – You may receive phishing emails or vishing calls asking for money donations, especially for hospitals, research institutions, local charities, etc.

Known Covid-19 Impersonate Websites

Not only are Covid-19 cyber scams increasing, but so is the impersonation of legitimate websites. The goal of impersonation websites is to either promote fake news or to obtain personal information like full names, addresses, Social Security numbers, payment information, username & passwords, etc. Typically, you will come to these websites by clicking links in phishing emails or on other websites. Below is a list of legitimate organizations that are currently being impersonated:

1. World Health Organization (WHO)
2. Center for Disease Control and Prevention (CDC)
3. Johns Hopkins University
4. Small Business Administration (SBA)
5. Internal Revenue Service (IRS)