SBA Loan Scams & Tips for Remote Employees

As many small businesses had to quickly move online after Safer at Home orders began, there was little time to implement elaborate systems and security settings. The same is true for many larger businesses that you interact with as they, too, saw new system uses, quick changes to their business models, or expanded user bases. As often follows swift changes, businesses are now experiencing hackers and other online vulnerabilities.

Here, we will outline a few current scam tip-offs as well as tips for employees who are now working from home.

Be Aware of SBA Loan Scams & Phishing Attempts

The Wisconsin Better Business Bureaus (BBB) have alerted that small business owners in Wisconsin should be aware of scams surrounding an SBA loan “processing fee” that can cost up to several thousand dollars. This request comes through a text or email that appears to come from the SBA.

Common Indicators of Fraud

- Any email communication from SBA will come from accounts ending with **sba.gov**. Always check "official" communications to make sure that the email addresses are coming from a legitimate domain.
- The SBA **does not** contact businesses asking them to apply for any of their loan products. If you are proactively contacted by someone claiming to be from the SBA, suspect fraud.
- Be leery of email links to loan/grant programs if you do not know the source. It is always better to find the agency website through an online search and ensure that the program is listed on their website. Other common indicators of phishing scams:
  - Fake email address (*sbaofficer@gmail.com*) that appear to come from supervisors, government offices, or other leaders or official entities
  - Sense of urgency (*act now!*)
  - Generic greeting line (*Dear Sir/Madam*)
  - Links leading to a destination that is different than the link text (hover your mouse over link to see the destination before clicking)
- Poor grammar
- If you are contacted by someone promising to get approval of an SBA loan, but they require payment up front or offer a high-interest bridge loan in the interim, suspect fraud.
- The SBA limits the fees a broker can charge a borrower to a maximum of 3% (depending on loan amount). Any attempt to charge more than these fees is inappropriate.

- Look out for phishing attacks/scams utilizing the SBA logo. These may be attempts to obtain your personally identifiable information (PII), obtain banking access, or install ransomware/malware on your computer. If you are in the process of applying for an SBA loan and receive email correspondence asking for PII, ensure that the referenced application number is consistent with the actual application number.
- The SBA (and affiliates, like the SBDC and SCORE) will not charge you for assistance with your small business and/or loan application process. Beware of organizations that ask you for payment for this consultation.

Report any suspected fraud to the Office of the Inspector General's Hotline at 800-767-0385 or online.

Cybersecurity Tips for Employees Working Remotely

This may be the first time many employees have worked in a remote environment. Here are some tips from Brian S. Dennis, Director of the Cybersecurity Center for Business at UW-Whitewater for making that process as secure as possible:

- **Don't share your computer**: When possible, use one computer for work and a different computer for everything else. Never let your kids or other family members use your work computer, and don't forget to lock it every time you walk away from it!
- **Verify incoming phone calls**: Without access to our office phones, we're answering phone calls from numbers we might not recognize. Attackers, pretending to be from the IT department or other official organizations, may call asking for passwords or other personal information. If anyone calls asking for this, do not give them any information, take down their phone number and call your supervisor and the local authorities.
- **Update your computer**: Make sure you are updating the latest patches and upgrades. Unpatched computers are easy targets for cyber criminals.
- **Be mindful of malware**: Once malware (often from email links) has been installed on your system cyber criminals can access anything you can.
- **Don't forget about your phone**: Many of us are using our personal smartphones for work these days. Cyber criminals are sending malicious text messages asking for the receiver to open a link. Additionally, there are mobile applications that track your data!
- **Be cautious with wifi**: A lot of us are using our own WiFi routers at home. Make sure your router is password protected.
- **Passwords**: Use strong passwords for everything! If you are overwhelmed with password management, consider a password manager to help keep you safe!
- **Make a plan for video-conferencing**: As many companies and organizations switched over to video-chatting platforms for meetings, users increased exponentially in a short period of time. As you assess what platform works best for your team:
    - Determine external compliance needs.
    - Establish your business needs (one-on-one meetings, webinars).
    - Select one platform and use consistently throughout the organization.
- **Avoid "Zoom-Bombing"** - the name given to hackers sharing obscene material through video platforms - by utilizing available security features. Video conferencing companies are regularly updating these features in the wake of new hacking attempts, so keep checking their blogs or support pages for the latest tools.