Cybersecurity Update:

The current Russian invasion of Ukraine has caused anxiety, financial impacts, and political actions around the globe. Loss of life and property have been confined to Ukraine so far but, the impacts are being felt around the world economically and logistically in companies large and small.

In addition to the economic impact in the U.S., there is a high level of concern regarding cyber-attacks. State-sponsored attacks on Ukraine are being used to disrupt everything from utilities, to banking, and communications. The tools being used to cause these disruptions are not always under the full control of the attacker. Many of the threats being released on Ukraine are capable of making their way around the world via the internet. It is also a distinct possibility that the U.S. and its allies could see an increase in targeted cyber-attacks should Russia decide to retaliate against those countries imposing sanctions.

The cybersecurity community is taking this threat seriously and we would ask the small business community to do the same. There is a real possibility that any small business could become the victim of a cyber-attack either directly or indirectly. To minimize the risk, small business owners should, at a minimum, do the following:

- Be more diligent about checking for unusual activity or performance issues on your devices and networks. This should include website traffic monitoring.
- Make a plan to incorporate regular backups if you have not done so already.
- Test a recent backup to make sure it works.
- Check anti-virus and all software (including any website plugins) for needed updates and patches.
- Incorporate a firewall or security monitoring software in your website and online store.
- Use a password manager with complex passphrases (16+ characters with random numbers, letters, and symbols)
- Use multifactor authentication
- Turn on or incorporate virtual private networks (VPN) when online
- Familiarize yourself with your website/online store providers data breach policy to fully understand who is responsible for reporting any breaches that may incur as well as who is liable in the event your site becomes infected.

While you cannot be guaranteed that you will not be impacted by a cyber-attack, you can dramatically reduce your chances of becoming a victim and substantially increase the speed of your recovery by following the above steps. Should you need more details or resources to assist with preparations, please contact your local SBDC offices and use the links below.

- CISA Shields-Up Notice and Guidelines: https://www.cisa.gov/shields-up
- Find a Local SBDC Office: https://americassbdc.org/find-your-sbdc/
- ASBDC Basic Cyber Awareness Resources for Small Business: https://americassbdc.org/cybersecurity/resources/