Cyber Attacks: A Growing Threat to the Small Business & U.S. Economy

written by Lauri Moon | November 3, 2022

FROM THE DESK OF THE REGIONAL ADMINISTRATOR

CYBERATTACKS: A GROWING THREAT TO SMALL BUSINESS & U.S. ECONOMY

BY: Regional Administrator John Fleming – U.S. Small Business Administration

Last year, cybercrimes targeting small businesses reached a record high of $2.4 billion. With online sales expected to surpass $1 trillion, retailers must evaluate their vulnerabilities to cyberattack and protect their systems. Small businesses are especially attractive targets because they typically lack the security infrastructure of large corporations.

Administrator Isabella Casillas Guzman, head of the U.S. Small Business Administration (SBA) and the voice for America's 33 million small businesses in President Biden's Cabinet, earlier this year announced millions in new funding for states to help small businesses develop cybersecurity infrastructure as part of the SBA's Cybersecurity for Small Business Pilot Program. I encourage you to check out our in-person and virtual events as well as the National Cybersecurity Alliance, a public-private partnership providing virtual and in-person cybersecurity events.

There are simple steps business owners can take to mitigate risk. Here are five easy actions business owners can take:

1. **Update your software:** Check regularly for updates or patches to guard against the latest cyber threats, it's the cheapest and easiest way to prevent online attacks.

2. **Review security protocols**: Ensure your website is protected with a Secure Sockets Layer (SSL) certificate, which authenticates a website's identity and enables an encrypted connection. Also, do not store credit card data on your systems.
3. **Create effective passwords:**Weak passwords are a major reason small retailers are prone to cyberattacks. Unique passwords with at least 12 characters that are a mix of numbers, letters, capital letters, and punctuation are proven most effective. Multi-Factor Authentication provides additional security.
4. **Be aware of social engineering threats:** Hackers bait or trick employees through phishing, baiting, scareware, and incentives that appear to be coming from someone familiar but contain malicious code allowing them access to sensitive information.
5. **Set strict rules on computer use:** Training and guidelines for employees who access your computer systems ensure only activities and data deemed necessary keeps hackers at bay.

Small retailers owe it to themselves, their customers and their employees to ensure online systems are safe. To learn more about SBA's programs and services related to cybersecurity, visit www.sba.gov/cybersecurity.