

Sombudha Adhikari Discusses Several Steps Small Businesses Can Take to Prevent Cyber Security Attacks

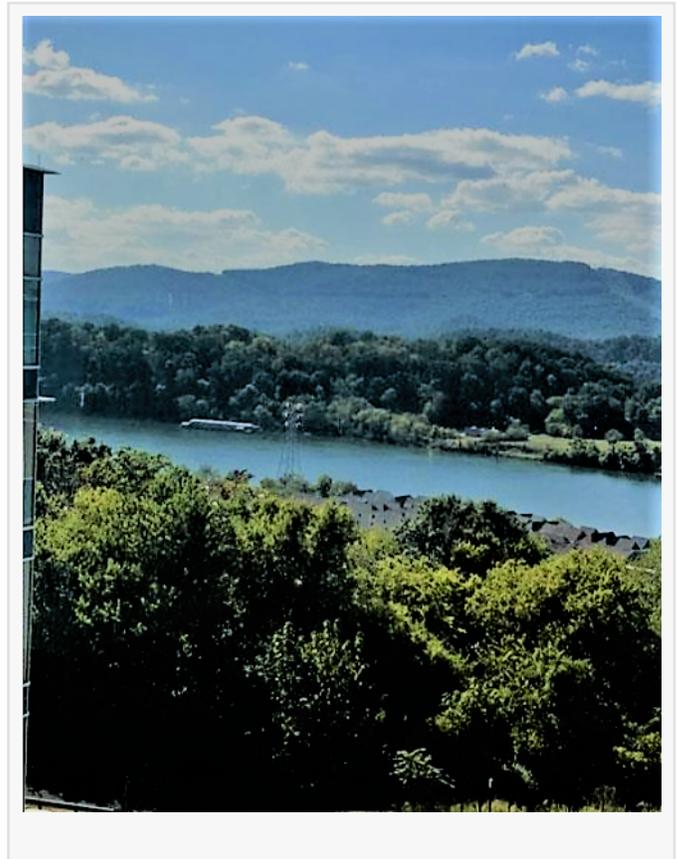
Software engineer Sombudha Adhikari recently discussed several steps small businesses can take to prevent cybersecurity attacks.

WHITEHOUSE STATION, NJ, UNITED STATES, September 14, 2020 /EINPresswire.com/ -- Cybersecurity attacks don't just happen to large corporations, like Sears and Target. Software engineer and cybersecurity specialist Sombudha Adhikari recently explained that cybersecurity attacks can occur just as easily, if not easier, for small businesses. In an effort to aid small businesses, Sombudha Adhikari offered several ways owners can prevent cyber attacks on their companies.

"Many small business owners assume cyber attackers aren't concerned with hacking them, because they don't see the same profits as larger corporations," Sombudha Adhikari said. "They're putting themselves at more risk with this mentality."

Sombudha Adhikari added that research has shown roughly 85 percent of small business owners think they are at a lower risk of experiencing data breaches, malware, viruses, hackers, and more. However, about 40 percent of cyber attacks are against businesses with 500 employees or less. Sombudha Adhikari stated that many times, data breaches don't come from outside sources. The smaller, family-like atmospheres of these smaller businesses can result in cyber-attacks from within the company.

"It's important for small business owners to train all employees in the principles of cybersecurity," Sombudha Adhikari said. "Each employee should also have his or her own user account, so breaches can be traced back to the individual, not a broad spectrum of employees."



Sombudha Adhikari stated that additional steps small companies can take to prevent cyber-attacks involve keeping software up-to-date at all times. This means using and updating antispyware software and antivirus software as well as applications and operating systems. Sombudha Adhikari suggests that every company, no matter the size, use a firewall for its internet connection and keep WiFi networks secure and hidden at all times.

Many times, employers think updating their cybersecurity will be too expensive, but the cost of a cyber attack is drastically more detrimental. Sombudha Adhikari explained that almost 60 percent of small companies that become victims of cyber attacks end up closing entirely within six months. The average cost of a cyber attack is more than \$200,000, and that's a price most small businesses can not risk losing.

"It's essential for small business owners to not their guards down," Sombudha Adhikari said. "It may seem easier to give employees access to certain data and information, but authority needs to be limited to only certain, high-trusted team members."

Sombudha Adhikari expressed the importance of limiting access to information and data, as well as changing all passwords regularly. It's easy for employers to let their guard down, as they work with the same employees for long periods of time, but that's when many cyber attacks occur. Physical access to network components and computers should always be documented and controlled.

"The statistics surrounding cyber attacks on small businesses are something to fear," Sombudha Adhikari finished. "Preventative action is the only way to protect your business and your profits."

Caroline Hunter
Web Presence, LLC
+17862338220
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/526217096>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2020 IPD Group, Inc. All Right Reserved.