

FOR IMMEDIATE RELEASE

Contact: Heather Ruiz – Director of Marketing

heather.ruiz@bit-wizards.com, 850-659-3775

Bit-Wizards Stresses Importance of IT Security in Light of Cybersecurity Awareness Month

Fort Walton Beach, FL – October 12, 2023– Managed IT Services provider Bit-Wizards is urging businesses of all sizes to prioritize security in response to Cybersecurity Awareness Month. With the average cost of a data breach in the United States reaching \$9.48 million in 2023, up from \$9.44 million in 2022, Bit-Wizards emphasizes the importance of businesses taking proactive measures to protect against cyber threats.

High-profile companies such as T-Mobile, MGM, Activision, and many others have already suffered financial losses due to cyberattacks this year, and with the holiday season approaching, Bit-Wizards warns that cybercrime tends to spike during this time. Businesspeople often let their guards down, and more employees are traveling and working remotely, making organizations more vulnerable to security risks.

“There’s an increase in activity for cyber threats this time of year because hackers know that people are not being as vigilant as they normally are,” says Jason Monroe, Director of Solution Consulting at Bit-Wizards. “By nature, we’re relaxed, we’re happy, and we don’t think anything can touch us.”

To combat this, Bit-Wizards urges businesses to implement:

Employee training: The main problem with employees is that they simply don’t know that they’re doing anything wrong, or they don’t know what to look for. Training your employees to be skeptical about every external email should be ongoing training that happens regularly. Your employees are your last line of defense before a cyber-criminal can get into your network, but they are also the reason why the doors are left unlocked and opened. Training on computer security best practices, passwords, phishing, ransomware, and other threats should be frequent and ongoing.

Cybersecurity measures: Taking cybersecurity measures such as undergoing regular penetration tests is a smart way to help defend your network. A penetration test is an authorized attack on a network to

evaluate its security posture. When you undergo a pen test, you're hiring a company to ethically hack your system. The main focus of this exercise is to attempt to find a vulnerability in a company's system and then exploit that vulnerability. Pen tests are important because they uncover security vulnerabilities before an actual hacker does, keeping your business one step ahead.

Continuous IT management: Outdated IT management often leaves businesses vulnerable to cyber threats, which is why it's crucial for businesses to keep hardware and software up to date, secure, and backed up. For businesses without dedicated IT resources, IT management is often mishandled, leading to security risks. Hiring a managed service provider (MSP) to handle your IT can help your business stop wasting money on security failures.

Bit-Wizards' Managed IT Services team makes sure your employees understand security best practices and that they're properly trained on all the equipment and tools they're using. Bit-Wizards is also SOC compliant and we voluntarily undergo penetration testing twice a year. This keeps our data and our clients' data safe.

"We've been in the business for 23 years, which is a rarity in the technology space," says Sam Blowes, Director of IT at Bit-Wizards. "In nearly two and a half decades, things have changed so much, and we've been here for all of it. So, we can tell you with confidence that it's simply not cost-effective to skimp on IT security."

When you partner with Bit-Wizards, we guard your company. Our security features include enterprise-grade firewalls, virus protection, advanced threat protection for email, alert monitoring, personnel training, regular backups, and cloud-based recovery restoration. For companies interested in learning more or getting IT security help from Bit-Wizards, [click here](#).

###