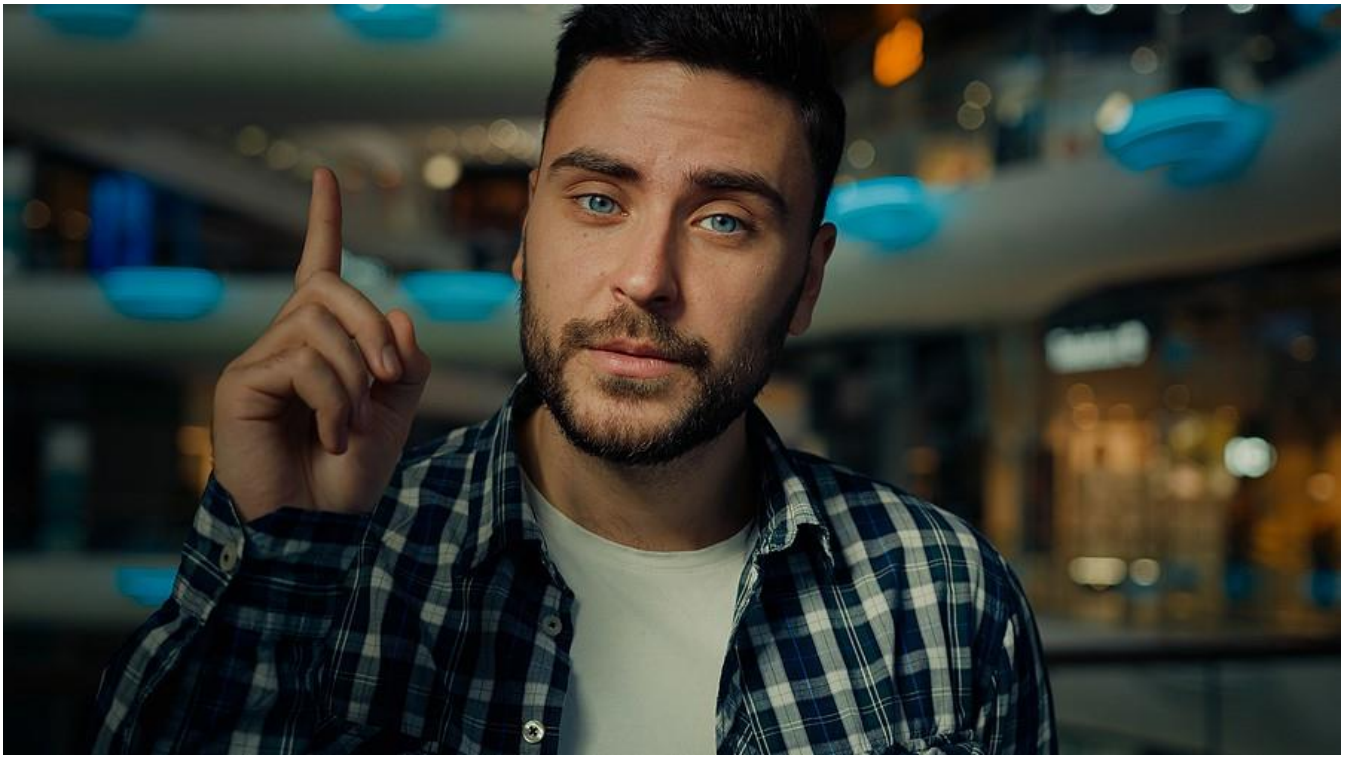
Fortify Small Business Security During Cybersecurity Awareness Month



October is Cybersecurity Awareness Month, a global initiative to raise awareness and educate business leaders and individuals about the importance of cybersecurity in our connected world. Cybersecurity is not only a concern for large corporations and government agencies, but also for small businesses.

Numerous Cyber Threats Bring Severe Consequences

Small businesses face numerous cyber threats, including ransomware, phishing, data breaches, and identity theft. According to a report by Verizon, 28% of data breaches in 2020 involved small businesses. And a report by IBM and the Ponemon Institute estimated the average cost of a small business data breach in 2022 to be $3.68 million.

Data breaches often bring severe consequences for small businesses, such as loss of customer trust, legal liability, and regulatory fines. In addition, small businesses often lack the resources, expertise, or awareness to implement effective cybersecurity measures. This makes them more vulnerable to cyberattacks than larger organizations.

Cybersecurity Awareness Month Checklist

However, small business owners and leaders who take simple steps to increase their cybersecurity awareness protect themselves better from cyber risks. Consider these tips and resources to be cyber smart during Cybersecurity Awareness Month and through 2024:

Create Strong Passwords and Use a Password Manager

Passwords are the first line of defense against unauthorized access to your online accounts and devices. Use long, complex, and unique passwords for each account, and avoid using personal or common information that can be easily guessed or found online.

A password manager can help you create and store strong passwords securely, so you don't have to remember them or write them down.

Turn on Multifactor Authentication

Multifactor authentication (MFA) adds an extra layer of security to your email, banking, and social media accounts. It can prevent hackers from accessing your accounts even if they have your password.

MFA requires something you know (such as a password), something you have (such as a phone or a token), or something you are (such as a fingerprint or a face scan) to log in. Enable MFA wherever possible.

Recognize and Report Phishing

Phishing involves sending fraudulent emails or messages that appear to come from legitimate sources, such as your bank or a colleague. The goal of phishing is to trick you into clicking on malicious links, opening infected attachments, or providing sensitive information.

To avoid falling victim to phishing, be wary of unsolicited or unexpected emails or messages. They often ask you to take urgent action, provide personal or financial information, or download or open files.

Check the sender's address, the spelling and grammar, and the URL of any links before clicking on them. If you suspect an email or message is phishing, delete it or report it to your IT department or email service provider.

Update Your Software

In addition to delivering new features or fixing bugs, software updates also patch security vulnerabilities that hackers can exploit. Thus, you should keep your operating system, applications, browsers, and antivirus software up to date on all your devices. Also enable automatic updates if possible.

Cybersecurity Awareness Month Education Resources

Not a one-time event, cybersecurity awareness requires constant learning and improvement. As a small business owner, you should educate yourself and your employees about the latest cybersecurity trends, threats, and information security governance best practices.

You can use various resources and tools to learn more about cybersecurity, such as:

- The Cyber Security Awareness Hub. This valuable resource from eMazzanti Technologies advocates for a layered security approach combined with education. Download an Awareness Kit and build a strong cyber security culture using its numerous helpful cyber security resources.
- The Cybersecurity Awareness Month Partner Toolkit by CISA (Cybersecurity and Infrastructure Security Agency). This provides several resources and communications for organizations to talk to their employees and customers about staying safe online.
- Cybersecurity Awareness Education and Resources by Microsoft Security. Discover self-paced learning paths, certifications, technical documentation, news, insights, and events for cybersecurity professionals and enthusiasts.

Cybersecurity a Human Issue

Often considered a technical issue, cybersecurity also depends on multiple human factors. It requires everyone's participation and collaboration to create a safer and more secure online business environment. Follow the above tips and resources to increase small business cybersecurity awareness and resilience this month and beyond.