Hey! What's New? 2025-15

How to Protect and Secure Your Data

In a posting on the *TechRepublic* webpage, Megan Crouse provides a comprehensive list of strategies to help safeguard companies' data from threats and data breaches.

Protect everything with passwords: Crouse says **"**password protection is the first line of defense against unauthorized access to your data; it also helps boost multilayer security for your systems by allowing you to combine password protection with other security measures. To password protect your business data, implement a strict password policy to ensure employees create complex passwords. Additionally, you should have them update their passwords regularly."

Back up regularly. Backing up your data early and regularly is an important component of a data loss prevention strategy. If you back up your data, you can restore it after losing data. "While manual backup does work, you should also consider data backup solutions that automatically back up data based on a schedule you can configure. More sophisticated backup solutions allow you to choose the data to back up."

Keep business software up to date. This will ensure that it has the latest security patches, bug fixes and other updates to protect against new and existing cybersecurity threats. Crouse notes that "most cyberattacks exploit newly found security vulnerabilities, so be vigilant in keeping your business software updated to the latest version."

Use a VPN. Crouse points out that virtual private networks are great for keeping your business data safe as they create "an encrypted tunnel for your data, hiding it from hackers and other malicious actors; it also helps minimize your online footprint. While you can use a free VPN service, ideally, you should invest in a paid VPN subscription from a reputable provider. Paid VPN versions offer more reliable connections, dedicated servers and other premium features."

Install antivirus software. Modern antivirus software helps protect data from ransomware, spyware, Trojan horses, browser hijackers and other cyber threats. "While an antivirus software license for a business comes at a cost, it's a relatively small price to pay to keep your data safe."

Use multifactor authentication. A reliable way to protect your data is to use multi-factor authentication on devices connected to the business network. "MFA acts as an additional layer of security for your data and is becoming a vital part of cybersecurity protocols for businesses. Without using MFA, your data remains vulnerable to unauthorized access due to lost devices or stolen credentials."

Make use of a public key infrastructure. A public key infrastructure is a system for managing public/private key pairs and digital certificates. Because keys and certificates are issued by a trusted third party (i.e., a certification authority), certificate-based security is stronger. Crouse says "you can protect the data you want to share with someone else by encrypting it with the public key of its intended recipient, which is available to anyone. The only person who can decrypt it is the holder of the private key that corresponds to that public key."

Hide data with steganography. You can use a steganography program to hide data inside other data. For example, notes Crouse, "you could hide a text message within a .JPG graphics file or an .MP3 music file, or even inside another text file; however, the latter is difficult because text files don't contain

much redundant data which can be replaced with the hidden message." Steganography doesn't encrypt the message, so it's often used with encryption software. The data is encrypted first and then hidden inside another file with the steganography software."

She adds that "some steganographic techniques require the exchange of a secret key. Others use public and private key cryptography."

Educate yourself and your employees about cybersecurity. According to Crouse, "one of the most crucial steps to protect your data is to educate yourself and your employees about cybersecurity. You need to promote a skeptical mindset when interacting with any unfamiliar website, email or message; this includes learning the importance of following the best practices for data protection, such as not opening emails from unrecognized senders, and not clicking on suspicious attachments."

Learn more at How to Protect and Secure Your Data in 10 Ways.