Essential Guide:

5 STEPS TO KEEP YOUR BUSINESS SAFE

MORE INFO

(915) 4 00 56 59
contact@go-sentry.com
2200 N. Yarbrough Dr. Ste E8
El Paso, Tx
www.go-sentry.com

Sentry

Sentry

5 SIMPLE STEPS TO IMPROVE YOUR BUSINESS CYBERSECURITY

USE STRONG, UNIQUE PASSWORDS

One of the most fundamental cybersecurity practices for businesses is to use strong, unique passwords for all accounts. This is a critical first line of defense against unauthorized access to your systems and data.

Avoid Password Reuse

Reusing the same password across multiple accounts is a major security risk. If one of your accounts is compromised, it leaves all your other accounts vulnerable. Hackers can easily try the same password on other sites, potentially gaining access to sensitive information or critical systems.

Utilize a Password Manager

To avoid password reuse, it's highly recommended to use a password manager. These secure applications generate, store, and automatically fill in complex, unique passwords for each of your accounts. This ensures that even if one password is discovered, your other accounts remain protected.

Create Strong Passwords

Passwords should be long, complex, and random. Aim for at least 12 characters, including a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using common words, phrases, or personal information that could be easily guessed.

Sentry

ENABLE TWO-FACTOR AUTHENTICATION

Two-factor authentication is a critical security measure that adds an extra layer of protection beyond just a username and password. By requiring a second form of verification, 2FA significantly reduces the risk of unauthorized access to your accounts, even if your password is compromised.

Enhance Account Security

2FA makes it much harder for attackers to gain access to your accounts, even if they have obtained your password. This is because they would also need access to your second factor, such as a code sent to your mobile device or a biometric identifier like a fingerprint.

Protect Against Credential Theft

If your username and password are stolen through a data breach or phishing attack, 2FA prevents the attacker from being able to use those credentials to log in and access your systems.

Use Authenticator Apps or Hardware Tokens

Rather than relying on SMS or email for the second factor, consider using a mobile authenticator app or a hardware security key. These options are more secure and less vulnerable to interception or bypass.

Sentry

KEEP YOUR SOFTWARE UPDATED

Maintaining up-to-date software is a critical component of a robust cybersecurity strategy. Software updates often include important security patches and bug fixes that address vulnerabilities that could be exploited by cybercriminals.

Patch Security Vulnerabilities

Software vendors regularly release updates to address newly discovered security vulnerabilities in their products. These patches are designed to close the gaps that could allow attackers to gain unauthorized access or compromise your systems. Keeping everything updated helps protect you from the latest threats.

Prevent Exploits and Attacks

Cybercriminals are constantly scanning for systems with known vulnerabilities that they can exploit. If you fail to install the latest updates, you leave your business exposed and at risk of being targeted by malware, ransomware, or other types of attacks.

Ensure Compatibility and Stability

In addition to security fixes, software updates often include improvements to functionality, performance, and compatibility.

Monitor and Audit Software

Maintain an inventory of all the software and systems used across your organization. Regularly review this list and ensure that everything is receiving the latest security patches and updates in a timely manner.

Sentry

TRAIN YOUR EMPLOYEES

Your employees are often the first line of defense against cyber threats, which is why educating and training them on cybersecurity is so crucial. By empowering your team with the knowledge and skills to identify and respond to potential security risks, you can significantly enhance the overall security of your organization.

Recognize Phishing and Social Engineering

Teach your employees to recognize the signs of phishing emails, suspicious websites, and other social engineering tactics that cybercriminals use to try and gain access to your systems and data.

Understand Secure Practices

Educate your team on best practices for password management, data handling, and other security-conscious behaviors. This includes using strong, unique passwords, enabling two-factor authentication, and being cautious when accessing unknown or untrusted sources.

Report Suspicious Activity

Ensure your employees know how to identify and report any suspicious activity or potential security incidents. This allows your security team to quickly investigate and respond, potentially preventing a minor issue from escalating into a larger breach.

Implement Ongoing Training

Cybersecurity threats are constantly evolving, so your training program should be an ongoing effort. Regularly update your curriculum to address the latest trends and techniques, and provide refresher courses to keep your employees informed and vigilant.

Sentry

BACK UP YOUR DATA REGULARLY

Maintaining regular backups of your critical business data is a crucial safeguard against the devastating impact of a successful cyber attack, such as ransomware or a data breach. By having reliable, up-to-date copies of your information, you can quickly recover and restore your systems in the event of an incident.

Protect Against Data Loss

In the event of a successful cyber attack, malware infection, or other system failure, regular backups ensure you can restore your data and minimize the impact on your business operations. This prevents you from permanently losing critical information.

Facilitate Rapid Recovery

When a security incident occurs, having readily available backups allows you to quickly recover your systems and get back up and running. This reduces downtime, lost productivity, and the potential financial and reputational damage.

Implement a Comprehensive Backup Strategy

Use a combination of on-site, off-site, and cloud-based backups to ensure redundancy and protect against multiple failure scenarios. Automate the backup process wherever possible to ensure it is consistently performed.

Secure Backup Storage

Ensure that your backup storage, whether physical or cloud-based, is properly secured with strong access controls, encryption, and other security measures to prevent unauthorized access or tampering.

Sentry

NEXT STEPS

At Sentry, we understand that maintaining robust cybersecurity practices is an ongoing effort, and staying vigilant against the latest threats is essential. While the steps we've covered can significantly improve the security posture of your business, our team of cybersecurity experts can go even further to ensure your company is even more secure.

Our personalized services can help you implement these security controls in a comprehensive manner, as well as develop a tailored cybersecurity strategy that specifically addresses the needs of your organization. By working with Sentry, you can be confident that your business is protected against the latest threats and prepared to withstand any security incident.

Contact us now for a free, personalized consultation on how we can help further secure your business.

Sentry
(915) 4 00 56 59
contact@go-sentry.com
2200 N. Yarnrough Dr. Ste E8
www.go-sentry.com