Intelligent Technical Solutions

15 Cybersecurity Best Practices

01 Conduct regular security and network assessments

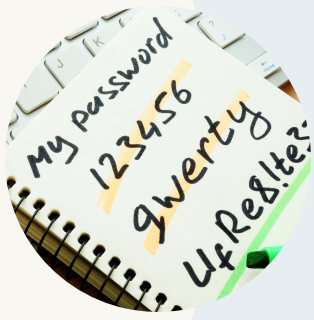
Regularly check for gaps and vulnerabilities. Set a schedule for performing network and security scans, reviewing access controls, and even assessing your facility's physical security.

02 Be wary of spam emails

One way malware can get into your network is through malicious spam or phishing emails. Although it's easy to assume that your employees already know how to spot scams, phishing emails are becoming harder to recognize.

03 Enforce safe password practices

Require employees to use unique passwords that combine upper- and lowercase letters, numbers, and symbols. It's also essential to change passwords every two to three months.

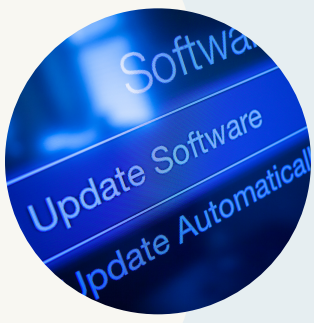


04 Implement and regularly conduct Security Awareness Training

The simplest way to prevent cyberattacks is through user education. Since your employees are the ones primarily handling your data, it's vital that they're trained on your company's security policies.

05 Keep software up-to-date

Software updates often contain essential changes to fix or improve the performance and stability of applications as well as remove outdated features. These improvements include critical patches to security vulnerabilities, which ensure protection from the latest known attacks.

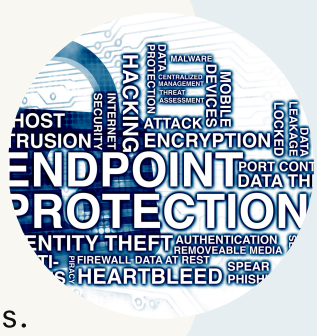


06 Perform a routine backup

If your business does fall victim to a cyberattack, backups will act as your last line of defense. Having an up-to-date backup means you can quickly restart your company's archive in the event of data loss.

07 Employ advanced Endpoint Detection and Response (EDR)

EDR detects and investigates suspicious activities on your company network and devices. This security solution employs a high degree of automation that enables your IT staff to quickly identify and respond to threats.



08 Use Multi-Factor Authentication (MFA)

Enabling MFA settings on most major networks and email services is simple to do, and doing so provides an additional layer of security. MFA requires users to provide other credentials besides their password to verify their identity.

09 Monitor the Dark Web for compromised credentials or information

Regularly check if your company accounts and passwords have been compromised and posted on the Dark Web.

10 Implement a Security Incident and Event Management (SIEM) solution

SIEM tools aggregate and analyze security data from various sources across your entire IT infrastructure. Implementing a SIEM solution allows you to ensure you remain compliant with increasing cybersecurity requirements.

11 Deploy secure web gateways

A secure web gateway protects your network by filtering malicious Internet traffic in real-time. It detects web and email threats as they emerge and subsequently blocks them before they reach your systems.

12 Secure mobile devices

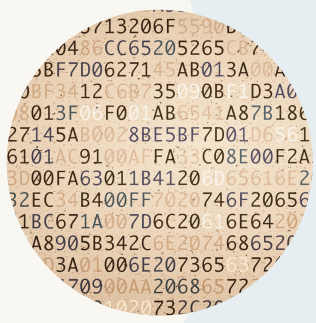
If your employees are using personal smartphones or tablets for work, make sure they password-protect their devices, encrypt their data, and install security apps. Also, create reporting procedures for lost or stolen devices. These ensure that your company data remains safe even if your employees aren't using company computers.

13 Turn on your Firewall security features

A firewall is an important first line of defense against cyberattacks. Essentially, it prevents unauthorized access to and from your network. If you have employees working from home, consider providing them with firewall software and support to ensure compliance.

14 Encrypt your data

Encryption prevents third parties from accessing your data while it's at rest or in transit. This method of secure communication is invaluable in combating advanced threats as well as maintaining regulatory compliance.



15 Invest in Cyber Insurance

Cyber Insurance can't protect your business from threats, but it can help you cushion the blow of a breach or an attack by offsetting recovery costs. With Cyber Insurance, you can keep your business on a stable financial footing if a significant attack does occur.

Need help with your Cybersecurity?

For almost 20 years, Intelligent Technical Solutions has been helping hundreds of businesses bolster their cybersecurity. We understand that finding the right partner is essential to protecting your network.

With our free network assessment, you don't have to be at sea with your risk posture. Know where you stand with your technologies, gain better visibility into your network, and learn how to optimize your systems to better align with business goals by requesting your free network assessment today. Contact us!

Intelligent Technical Solutions

Phone: (702) 605-6670

Click here to request for a Free Network Assessment.