



Headline 1 – Basic Cyber Hygiene Using an MSP

Headline 2 – MSPs for Basic Cyber Hygiene

Headline 3 – Leveraging an MSP for Cyber Hygiene



<https://www.istockphoto.com/vector/man-in-a-biochemical-protection-suit-disinfection-gm165677982-10392611?phrase=cyber%20security%20hygiene>

Establishing basic cyber hygiene is critical in today's world of increased numbers of bad actors and cyber threats. Here's how using an MSP can help.

Key Takeaways:

- What is cyber hygiene?
- Why is cyber hygiene essential for business systems?
- What are the basic best practices for performing cyber hygiene?
- Discover how an MSP provides built-in expertise for performing cyber hygiene.

Cyber hygiene practices keep data safe and protected, but unfortunately, it's a security practice that is often overlooked. Securing data helps protect all devices from malware attacks that hinder functionality and performance. Cyber hygiene comprises the precautions and practices users take to keep sensitive data organized, safe, and secure from cyberattacks or cyber criminals.



This guide describes the benefits of practicing effective cyber hygiene to keep business data, users, devices, and systems secure.

What is cyber hygiene?

Cyber hygiene, or cybersecurity hygiene, refers to the practices end users and organizations regularly perform to ensure device and data security. For organizations, [cyber hygiene](#) means updating, monitoring, and maintaining security on all devices, networks, and data.

The purpose of performing cyber hygiene is to keep business and user data secure. Like personal hygiene, cyber hygiene keeps systems healthy and prevents data breaches or other security incidents. Organizations must be prepared to secure all hardware, software, and devices used or connected to within a business network.

Cyber hygiene provides a [basic level of protection](#) against:

- Data loss
 - Hard drive or online data storage that isn't properly backed up or secured
- Corrupted or rearranged data
 - Data may not be removed but instead corrupted and made unusable
- Security breaches
 - Direct attacks from cybercriminals to gain access through malware, spam, or virus-infected code
- Non-updated software or hardware versions
 - Always keep systems on the latest security updates
- Non-updated security software or systems
 - Using old or out-of-date antivirus software is useless in protecting business data

Cyber hygiene is critical to providing constant and effective security for all business systems and devices to keep threats locked out.

Why is cyber hygiene essential for business systems?

Cyberattacks cost U.S. and global businesses money every year, regardless of their size. As business and technology continue to move online, cyberattacks increase. Planning for constant, consistent security implementations is critical to keep businesses growing and data safe.

Businesses must invest in improving their security posture on an ongoing basis. A solid security posture reduces the risk of business operations being interrupted, data compromised, stolen, or ransomed. A business's revenue should be invested into building better products and providing exceptional customer experience – not paying ransoms to get data returned from hackers.



Keep in mind that data breaches carry significant government fines, downtime, legal liabilities, and lost business reputation and trust. Effective cyber hygiene is a small but crucial price to pay for protecting the business and its assets.

What are the basic best practices for cyber hygiene?

Cybersecurity is critical to both end users and business organizations. The best practices for each vary in responsibility and scope, but both are essential for keeping systems consistently secured and protected.

[Cyber hygiene best practices](#) for end users includes scheduling regular backups for all files and utilizing device and file encryption to protect data. Ensure that end users change their passwords a minimum of every 90 days and use multifactor authentication. Keep all your devices and software up to date, especially for security-related patches.

Finally, protect your personal information and business data by keeping up on news about scams and phishing attempts. Only share data when necessary and know exactly who you're sharing data with and for what reason. End users can do their part to protect themselves and the business, and businesses must also be positioned to practice proper cyber hygiene.

Cyber hygiene best practices for businesses include:

- Use allowlisting or blocklisting for controlling access
- Practice high-level authentication and use one or more types of multifactor authentication
- Configure systems using the principle of least privilege for user roles
- Remove access immediately for terminated employees regardless of role or level
- Use device controls that can lock or disable a user's device remotely
- Create a backup strategy to ensure critical information is duplicated and securely stored
- Perform regular security assessments against the system
- Perform regular security testing against the system to identify issues

Cyber hygiene best practices for businesses include:

- Use allowlisting or blocklisting for controlling access
- Practice high-level authentication and use one or more types of multifactor authentication
- Configure systems using the principle of least privilege for user roles
- Remove access immediately for terminated employees regardless of role or level
- Use device controls that can lock or disable a user's device remotely
- Create a backup strategy to ensure critical information is duplicated and securely stored
- Perform regular security assessments against the system
- Perform regular security testing against the system to identify issues



Cybersecurity and cyber hygiene are complex and time-consuming for both users and organizations. Keeping all systems and devices up to date on the latest security protocols is not a simple task, but it is vital for keeping business and user data secure.

Benefits of leveraging an MSP for cyber hygiene

MSPs provide cyber hygiene and other security and maintenance procedures for you. No need to schedule or find security specialists on your own – simply leverage the MSP services that provide continuous upgrades, maintenance, and security procedures to fully protect the system. In addition to regularly performing routine maintenance and updates, MSPs can enforce continuous security monitoring to ensure your system is always protected.

MSPs provide the tools and expertise necessary to continuously maintain an organization's security posture at the highest level. Leverage the security expertise within the MSP to keep up with your organization's cyber hygiene.

Securing systems, devices, and data is critical to the success of the business and the protection of user and customer data. Keep your business moving forward securely by leveraging the security expertise within an MSP.

Are you ready to benefit from cybersecurity services?

Need help choosing cybersecurity best practices and implementing them for your small business? [Endsight](#) is your MSP security partner, 24/7. We keep your business up and running using the latest advanced security and business management technology. Get your [free cybersecurity assessment](#) today and see how [Endsight](#) can help your business grow.

Alt CTA 1: Do you want technical support and assistance setting up security or a routine cyber hygiene process? Need to implement a credible security posture? Look no further than Endsight. Check out our [free cybersecurity assessment](#) and see how we can help secure your business.

Alt CTA 2: Is the stress of maintaining security monopolizing your work time? If you need to focus on business details, leave the security and network management – including effective cyber hygiene – up to Endsight. [Find out how Endsight](#) can help you build the business without having to worry about network security, performance, or access. [Get a free cybersecurity assessment](#).

Alt CTA 3: Burned by a previous cybersecurity service experience? Endsight is different! We are the managed cloud partner you can trust – all day, every day. We'll keep your business up and running seamlessly and securely. Check out why our [clients chose us](#) to help their business.

.....
For publishing



This is information writers provide for the production team when they are publishing the blog.

Page title: Establish Basic Cyber Hygiene Using an MSP

Meta Description: This guide describes the benefits of practicing effective cyber hygiene to keep business data, users, devices, and systems secure.

Permalink (slug): establish-basic-cyber-hygiene-using-MSP

Keywords: Establish basic cyber hygiene using an MSP, cyber hygiene

Image alt text: The image displays a cartoon person in a white hazmat suit, mask, and gloves running and spraying foaming solution over objects to represent how to establish basic cyber hygiene using an MSP.

Tags: #ITmanagement #ITsecurity