SOPHOS
Cybersecurity delivered.

Cybersecurity Best Practices

Tips to help you stay safe online

Keeping yourself protected from cybercrime isn't just about having the latest security solutions. Good IT security practices, including regular training for employees, are essential components of every single security setup. Make sure you're following these 9 best practices:

1. **Patch early, patch often**

   The exploitation of unpatched vulnerabilities was the root cause for almost half of cyber incidents investigated by Sophos in 2021.[1] The earlier you patch, the fewer holes there are to be exploited.

2. **Back up regularly and keep a recent backup copy off-line and off-site**

   73% of IT managers whose data was encrypted were able to restore it using backups.[2] Encrypt your backup data and keep it off-line and off-site. Practice restoring data from backups regularly.

3. **Enable file extensions**

   File extensions in Windows are hidden by default. Enabling them makes it much easier to spot file types that wouldn't commonly be sent to you and your users, such as JavaScript files.

4. **Open JavaScript (.JS) files in Notepad**

   Opening a JavaScript file in Notepad blocks it from running any malicious scripts and allows you to examine the file contents.

5. **Don't enable macros in document attachments received via email**

   Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. A lot of infections rely on persuading you to turn macros back on, so don't do it!

6.

Be cautious about unsolicited attachments

Cybercriminals often rely on an ages-old dilemma: knowing that you shouldn't open a document until you are sure it's legitimate, but not being able to tell if it's malicious until you open it. If in doubt, leave it out.

7.

Monitor administrator rights

Constantly review local and domain admin rights. Know who has them and remove those who don't need them. Don't stay logged in as an administrator any longer than necessary.

8.

Regulate internal and external network access

Don't leave ports exposed. Lock down your organization's RDP access and other remote management protocols. Furthermore, use two-factor authentication and ensure remote users authenticate against a VPN.

9.

Use strong passwords

A weak and predictable password can give hackers access to your entire network. We recommend making them impersonal, at least 12 characters long, using a mix of upper and lower case, and adding random punctuation Ju5t.LiKETh1s!

1 The Active Adversary Playbook 2022 - Sophos
2 State of Ransomware 2022

2022-09-12 EN (DD)

SOPHOS