Zoho eProtect

Malware prevention guide

ZOHO

Malware prevention guide

Malware attacks don’t just target large companies. They rely on everyday users making a single careless move. Whether it’s a disguised attachment, a fake software update, or an infected website, one wrong action can compromise personal and organizational data.

This guide shows you how to stay alert, avoid risky behaviors, and prevent malware that sneaks in through email from gaining a foothold on your devices.

94% of malware is delivered through emails . →

What is malware?

Malware refers to any malicious software that's propagated with the intention to destroy, corrupt, or deny access to sensitive data on a system. Threat actors perpetrate malware in different forms such as viruses, bots, ransomware, and much more. They plan the attack in such a way that their file or URL containing malware evades the security filters set up by organizations and silently makes its way to the users’ systems to infect them without detection.

Common ways of malware infection

Phishing emails: Malicious attachments or links disguised as legitimate messages trick users into downloading malware.

Infected downloads: Free software, pirated content, or files from untrusted websites often carry malicious content.

Malicious links: Clicking on suspicious ads, pop-ups, or fake login pages can silently install harmful software.

Compromised websites: Visiting hacked or unsecured sites can trigger drive-by downloads without your knowledge.

External storage devices: USB drives or external storage devices can spread malware when plugged into a computer.

Fake updates: Pop-ups urging you to make urgent software or browser updates may deliver malware instead of legitimate patches.

Public Wi-Fi traps: Attackers on unsecured networks can inject malware into your browsing session or downloads.

Signs your device may be infected

Slow performance and battery drain:

Programs take longer to load and your system feels unusually sluggish. It heats up and loses its charge faster than usual.

Frequent crashes or freezes:

Apps or the entire device suddenly shuts down or restarts unexpectedly.

Unexpected pop-ups:

Random ads, warnings, or alerts appear even when no browser is open.

Unknown files or apps:

New programs, shortcuts, or files that you didn't install appear randomly.

High data or CPU usage:

Unexplained spikes in network activity or processor usage indicate hidden background processes.

Unauthorized account activity:

Strange logins, password resets, or financial transactions occur on your accounts.

Malware prevention tips

1. **Check links before clicking:** Avoid opening suspicious links or attachments even if the email appears to come from someone you know.
2. **Verify the sender:** Check for misspelled domains or unusual reply-to addresses before trusting an email.
3. **Use strong passwords and MFA:** Protect email accounts with unique passwords and MFA to block unauthorized access
4. **Keep software updated:** Regularly install security patches for your email client, browser, anti-virus software, and operating system to close known vulnerabilities.
5. **Implement security solutions:** Use spam and malware filters to block dangerous messages before they reach your inbox.
6. **Report suspicious emails:** Immediately flag or forward phishing attempts to your IT or security team.
7. **Avoid public Wi-Fi for email:** Use a VPN or secure network to check emails safely outside the office.
8. **Backup important data:** Keep regular offline or cloud backups to recover quickly if malware slips through.

What do you do if you spot an email with malware?

If you notice any of the red flags above, follow these steps immediately to stay safe:

- Do not click anything or respond to the email.
- Verify the sender.
- Report it.
- Mark as malicious.
- Change your password immediately if you've engaged with the email.

Conclusion

Malware thrives on careless clicks and unsafe email habits. By staying alert, verifying messages, and using security tools consistently, you can block infections before they start and keep both your data and organization safe.

This guide was released by Zoho eProtect as part of Cybersecurity Awareness Month 2025. eProtect is a cloud-based email security and archiving solution that provides advanced threat protection for all on-premise and cloud email accounts. eProtect is the security solution powering Zoho Mail, a platform trusted by millions of users.