Zoho eProtect

Best practices to prevent security incidents

ZOHO

Best practices to prevent security incidents

Every email you open, link you click, or password you create can play a role in keeping your organization safe or putting it at risk. Security incidents such as phishing scams, malware infections, and data leaks often start with a single careless action, and their impact can be costly for both you and your company.

This guide is designed to help you stay protected. By following a few simple best practices like using strong passwords, spotting suspicious emails, and keeping your devices updated, you can prevent most security incidents before they happen.

Common threats to watch out for

Cybercriminals use different tactics to trick people into sharing information, transferring money, or granting access to company systems. Knowing what these threats look like helps you avoid them.

Phishing emails: Attackers send emails that look legitimate, often posing as your boss, a vendor, or a trusted service. They may ask you to click a link, open an attachment, or urgently approve a payment.

Social engineering scams: Scammers may call, text, or message you on chat apps while pretending to be IT support, HR, or a familiar contact. They often create urgency or fear to pressure you into sharing passwords or sensitive details.

Malware and ransomware: Malicious software can arrive through infected attachments, unsafe downloads, or even compromised USB drives. Once inside, it can steal data, lock your files, or disrupt operations until a ransom is paid.

Account takeover: Weak or reused passwords make it easy for attackers to guess or steal your login credentials. Once they gain access, they can read emails, steal files, or impersonate you to others in the company.

Best practices to prevent security incidents

1. **Use strong passwords and MFA:** Create long, memorable passphrases and enable MFA on all accounts to add an extra layer of protection.
2. **Be cautious with files and links:** Hover over links to check URLs and avoid opening attachments from unknown or suspicious senders.
3. **Watch for social engineering:** Never share passwords or sensitive information without verifying the requester's identity through a trusted channel.
4. **Verify payment and data requests:** Confirm unusual or large requests through a separate channel, like a phone call or video chat, and not just through email.
5. **Keep devices and software updated:** Install security patches, operating system updates, and antivirus updates promptly.
6. **Use secure networks:** Avoid public Wi-Fi when accessing work accounts. If necessary, connect via a VPN.
7. **Lock devices and secure data:** Always lock your screen when stepping away and avoid storing sensitive files on personal or unsecured devices.
8. **Report suspicious activity immediately:** Alert IT or security teams if you notice unusual emails, logins, or any potential threats.
9. **Limit access to sensitive information:** Only share files or data with colleagues who need them for their work.
10. **Be extra cautious if you work remotely:** Use company-approved devices and software. Avoid storing company data on personal devices unless authorized.
11. **Pause before acting on urgent requests:** Attackers often create a false sense of urgency. Take a moment to verify the request before responding.
12. **Check email senders and tone carefully:** Look for subtle changes in sender addresses, domains, or email tone that may indicate a phishing attempt.

13 **Avoid clicking on pop-ups or unverified ads:** Malicious websites or pop-ups can install malware without your knowledge.

14 **Use encryption when sharing sensitive files:** For confidential information, ensure that the file is encrypted and shared via secure company-approved channels.

15 **Stay informed and participate in training:** Attend regular cybersecurity awareness sessions and practice simulated phishing exercises to improve vigilance.

Conclusion

Cyberattacks often rely on haste and trust, so taking a moment to pause, verify, and report can stop a potential breach before it starts. By staying alert and following these best practices, you help protect not only your company's data but also your own digital safety. Security is a shared responsibility, and every careful action counts.

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.