S

Spam and Malspam: Differences, Warning Signs, and Safe Response

Spam is unsolicited bulk messaging; malspam uses those messages to deliver malware. Learn the difference from phishing, warning signs, safe reporting, and what to do after a click.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 What is spam?

02 Spam vs. phishing vs. malspam

03 How malspam turns an email into an infection

04 Warning signs of malicious spam

05 What to do with a suspicious email or message

06 What to do if you clicked or opened an attachment

07 How organizations can reduce spam and malspam risk

08 Frequently asked questions

09 References

01 What is spam?

Spam is unsolicited bulk messaging sent through email, text messages, social platforms, calls, or other channels. Some spam is merely unwanted advertising. Other messages promote fraud, steal credentials, or deliver malware. The fact that a message is sent in bulk describes how it is distributed, not how dangerous it is.

Malspam, short for malware spam or malicious spam, is spam designed to install malware. It uses an attachment, link, QR code, or multi-step download to deliver a loader, information stealer, remote access trojan, ransomware, spyware, or another payload.

02 Spam vs. phishing vs. malspam

Category	Main purpose	Typical action requested	Recommended response
Ordinary spam	Promote a product or generate traffic	Read an offer or visit a site	Mark as spam; unsubscribe only when the sender is known and legitimate
Phishing	Steal passwords, payment data, or other information	Sign in, verify an account, pay, or disclose data	Do not use message links; verify through a known channel and report phishing
Malspam	Run malicious code on a device	Open an attachment, enable content, install a file, or follow download steps	Report it; if content was opened, isolate and investigate the device
Scam spam	Obtain money or manipulate the recipient	Pay a fee, buy gift cards, transfer funds, or continue a conversation	Stop contact, verify independently, and report fraud

These labels can overlap. A bulk invoice campaign can be spam because it is sent widely, phishing because it impersonates a supplier, and malspam because its attachment runs malware. Classify the message by the outcome it is trying to cause so you take the right recovery steps.

03 How malspam turns an email into an infection

1. **Distribution:** attackers send messages from compromised accounts, lookalike domains, disposable infrastructure, or botnets.
2. **Lure:** the subject imitates routine work such as an invoice, shipping notice, voicemail, resume, shared document, or account alert.
3. **Delivery:** the message carries an attachment or points to a page, archive, script, shortcut, or fake installer.
4. **Execution:** the recipient runs a file, grants a permission, enables active content, or follows a sequence that launches code.
5. **Handoff:** a small first stage may download the main payload, create persistence, steal data, or connect to command-and-control infrastructure.

A PDF, document, archive, or cloud-service link is not safe solely because the file type or host is familiar. Attackers can use a benign-looking document as a link or container that leads to the next stage.

04 Warning signs of malicious spam

- The display name is familiar but the actual address or domain is not.
- A reply-to address differs from the visible sender, or the conversation is unexpected.
- The message creates urgency, secrecy, fear, or an unusual exception to normal procedure.
- An unexpected attachment asks you to enable content, bypass a warning, extract an archive, or run a shortcut or installer.
- A button or link leads to a different domain than its text suggests.
- A QR code moves the task to a phone where the destination is harder to inspect.
- The request involves credentials, payment, bank-detail changes, gift cards, or sensitive files.
- Email authentication fails or the sending infrastructure does not match the claimed organization.

Spelling and grammar are weak signals. Legitimate messages contain mistakes, and malicious messages can be polished. Verify the sender, context, destination, and requested action together.

05 What to do with a suspicious email or message

1. **Do not reply, open attachments, scan a QR code, or use embedded contact details.**
2. **Verify independently.** Open the service from a saved bookmark or contact the person through a phone number or channel you already know.
3. **Use the provider's Report spam or Report phishing control.** In a workplace, use the approved reporting button or send the original message as an attachment to the security team so headers are preserved.
4. **Do not forward malicious attachments casually.** Follow the organization's reporting process to avoid exposing another person.
5. **Delete the message after reporting** unless responders ask you to preserve it.

Should you click Unsubscribe?

Use a built-in unsubscribe control for a newsletter or business you recognize and previously authorized. For a suspicious or unknown sender, do not follow an unsubscribe link inside the message: it may confirm that the address is active or lead to a malicious page. Mark the message as spam instead.

06 What to do if you clicked or opened an attachment

A click alone does not prove infection, but the response should match what happened.

- **You opened a page but entered nothing:** close it, do not accept downloads or notifications, and report the URL. Update the browser and run a security scan if a download or warning appeared.

- **You entered a password:** from a clean device, change that password, revoke active sessions, review recovery settings, and enable MFA. If reused, change it everywhere.
- **You opened or ran a file:** disconnect or isolate the device and contact IT or security. Run trusted scans, preserve relevant alerts, and check for persistence and follow-on activity.
- **You sent money or financial details:** contact the bank or payment provider immediately using a verified number and report the fraud.
- **You approved an MFA prompt or application access:** revoke sessions, tokens, and connected-app permissions; then review account activity.

07 How organizations can reduce spam and malspam risk

- Deploy layered email filtering, URL analysis, attachment scanning, and safe detonation where appropriate.
- Configure SPF, DKIM, and DMARC for owned domains and monitor reports. These controls reduce spoofing of protected domains but do not make every authenticated message trustworthy.
- Block or quarantine attachment types and nested archives that the business does not need.
- Disable risky active content by default and use application control and endpoint detection.
- Make user reporting easy and connect reported messages to rapid search-and-removal across mailboxes.
- Correlate email delivery with endpoint process creation, DNS, identity alerts, and network connections.
- Use phishing-resistant MFA and require independent verification for payment or bank-detail changes.

08 Frequently asked questions

Can opening an email infect a device?

Modern mail clients reduce the risk of code running merely from viewing a message, but no system is risk-free. Links, attachments, remote content, and unpatched client vulnerabilities create more realistic paths. Keep software updated and avoid interacting with suspicious content.

Does blocking the sender stop spam?

It can reduce messages from one address, but campaigns rotate addresses and domains. Reporting helps the provider detect related messages, while filters and organizational controls address the larger pattern.

Is every unsolicited commercial email illegal?

Laws vary by country and context. Security classification is separate from legal classification: even a legally sent promotion may be unwanted, while a well-targeted malicious message may not look like bulk spam.

09 References

- Google: avoid and report phishing emails
- U.S. FTC: how to get less spam in your email
- CISA: recognizing and reporting phishing

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com