



## What is phishing?

This technique is called **phishing**, and it's a way hackers can get you into providing your personal information or account data. Once your info is obtained, hackers create new user credentials or install malware (such as backdoors) into your system to steal sensitive data.

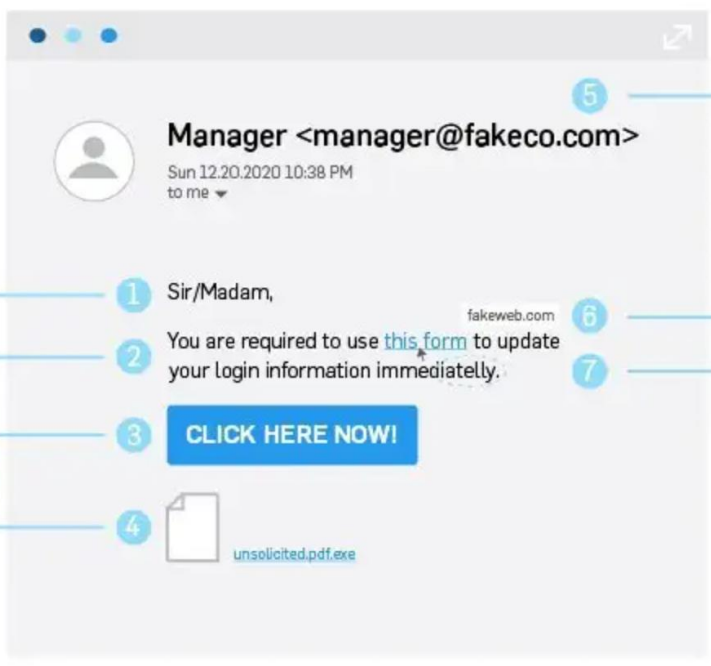
## 7 Signs of a Phishing Email

Generic greeting or no greeting at all

Request for personal information over email

Buttons with hyperlinks to unfamiliar webpages

Unsolicited attachments



"From" email address is not official

Hover your mouse to reveal misleading URL hyperlinks

Spelling and grammar mistakes



## What is email spam?

Email spam, also known as *junk email*, refers to unsolicited email messages, usually sent in bulk to a large list of recipients. Apart from email, spam can also be distributed via text messages or social media.

### 6 key features of junk mail to look for.

1. Suspicious email addresses	2. Typos and poor phrasing
3. Personal data requests	4. Impersonal delivery
5. Sense of urgency	6. Too good to be true.

If you come across any of these in the new email, do the following:

- don't click on any links, download attachments, or respond.
- Mark this email as "Spam" so you won't receive more junk mail from the same sender — or delete it from your inbox.

### Wrapping up

Spam emails might seem funny and clumsy, but they are dangerous — phishing leads to loss of money and possible identity theft. Scammers get more inventive with their schemes — that's why it's important to know the key features of junk mail and never interact with such emails for the sake of your safety.

Some of the common spam emails are:

- Fake Apple ID account verification
- "You've won a lottery."
- Missing account information emails
- Account suspension
- Fake gift card claims
- Fake tax refund notifications
- Fake COVID vaccination appointments
- Bitcoin-related scams including blackmail.
- Fake delivery notifications