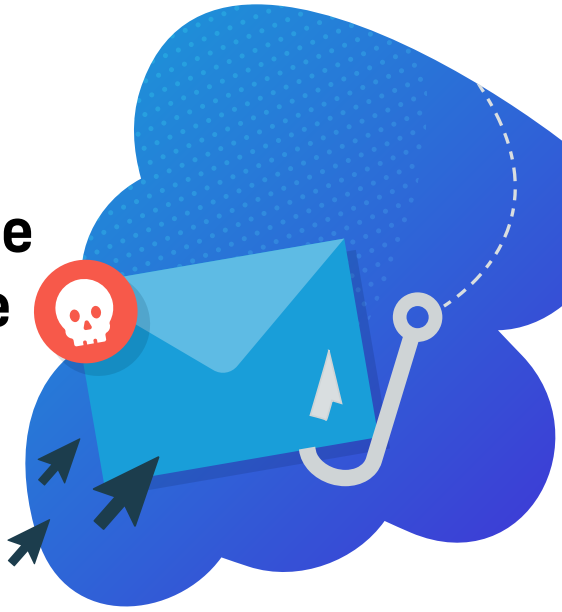
datto

# Phishing Attacks: How to Recognise Them and Keep Business Data Safe



Cybercrime is on the rise, and hackers are using any opportunity to take advantage of an unknowing victim to gain access to personal information for financial gain. One commonly used tactic is phishing. Phishing messages are crafted to deliver a sense of urgency or fear with the end goal of capturing a person's sensitive data and can result in wire transfer fraud, credential phishing, malware attachments, and URLs leading to malware spraying websites.

**Phishing scams are getting more sophisticated on a daily basis, thus harder to detect and avoid.**

## Here are five different types of phishing attacks to avoid:

### 1. Spear Phishing

Attackers pass themselves off as someone the target knows well or an organisation that they're familiar with to gain access to compromising information (e.g., credentials or financial information), which is used to exploit the victim.

### 2. Whaling

Whaling is a form of spear phishing with a focus on a high-value target, typically a senior employee within an organisation, to boost credibility. This approach also targets other high-level employees within an organisation as the potential victims and includes an attempt to gain access to company platforms or financial information.

### 3. Mass Campaigns

Mass phishing campaigns cast a wider net. Emails are sent to the masses from a knock-off corporate entity insisting a password needs to be updated or credit card information is outdated.

### 4. Ambulance Chasing Phishing

Attackers use a current crisis to drive urgency for victims to take action that will lead to compromising data or information. For example, targets may receive a fraudulent email encouraging them to donate to relief funds for recent natural disasters or the COVID-19 global pandemic.

### 5. Pretexting

Pretexting involves an attacker doing something via a non-email channel (e.g., voicemail) to set an expectation that they'll be sending something seemingly legitimate in the near future only to send an email that contains malicious links.

## What to do if you think you've received a phishing email?

First, to help identify it as a phishing email, check to see if the signed-by field was generated by a DomainKeys Identified Mail (DKIM) or a service. For example, if you received an email from name@datto.com, you would see a DKIM in the signature that looks like this: datto-com.20150623.gappssmtp.com. This is how all emails through a domain are processed.

Emails shared through a service (e.g., Drive, Calendar, Dropbox, Box, etc.) do not have a DKIM. Instead, you would see the signature of the provided service (i.e., signed-by dropbox.com).

If you receive a file, and it is not signed by google.com, gmail.com, dropbox.com, it is likely phishing - delete it immediately. It's important to remain vigilant and proceed with caution in these circumstances.

**Be careful!** Phishing scammers are impersonating file sync and share platforms and sharing fake documents or folders in an attempt to infect your computer.

**Education and cyber security training** can mean the difference between compromised credentials and a failed attempt by a hacker.

LEARN MORE →