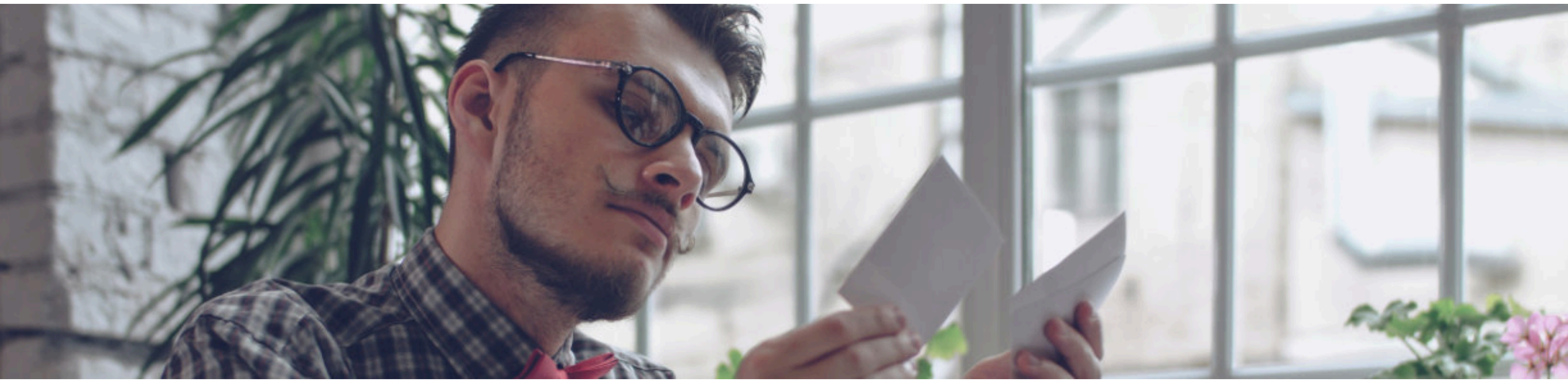
You've Got Junk Mail

How to Spot Scam Emails

DEER
BROOK



As technology evolves and techniques adapt, the age-old method of scouring for typos and misspellings is no longer a go-to strategy for spotting scam emails.

But even so, not all hope is lost. There's still ways you can check to see if messages are the real deal or not.

Signs of a Scam Email

The Email Creates Panic

Fake emails almost always try to induce panic, masquerading as a service like Amazon, FedEx, or even Apple, where the scammers can leverage the company's products or services to create urgency.

The idea here is that scammers are dropping an email to you out of the blue and trying to ruin your day with some "urgent" matter. Whatever it may be, it requires your immediate attention.

They hope that you start to panic, lower your guard, and start clicking on links, opening attachments, or start replying to the emails without giving it a second thought.

The Email Preys on Curiosity

Scammers like to prey on people's curiosity, whether that's in the form of the classic "Nigerian Prince" scam or a more subtle romance scam.

Malicious attachments with vague names, clearly not meant for the recipient, are also another way they try to lure victims in.

They hope that these emails are enticing enough for a potential victim to click into and investigate, even if in some cases it looks like a misdelivered email.

Checking a Scam Email

Ask Yourself These Questions

The first step to checking if an email is fake is to take a deep breath and relax, and then run down a series of questions like these:

- Do I have an account with this company/organization, or is it reasonable that this person has my contact information?
- Do I recognize the person's name, or the organization that they claim to be?
- Was I expecting this kind of email?
- Do I usually get these kinds of emails?

If you answer 'no' to one or many of these questions, your gut instinct is probably on-point.

Check for Misspellings

Even though misspellings and typos are less common in phishing emails these days, double-check for any unusual punctuation and typos. If you're seeing typos on an email from a notable company, alarm bells should be going off in your head.

No credible organization would allow an email to go out with numerous spelling and grammar mistakes.

Check the Sender's Email Address

Check the domain of the sender's address. If you've gotten previous emails from that person or organization, look at those emails and compare the domains to see if they're the same. If they're not, steer clear.

If they look the same but you're still suspicious, copy the sender's domain and paste it into a Unicode inspector or an ASCII validator to verify the domain doesn't have any lookalike characters.

Check the Sender's "reply to" Address

Check the suspicious email to see if there's a "reply to" address with a different domain, or otherwise looks suspicious in any way.

Sometimes, legitimate email accounts get breached and hackers send emails out from trustworthy domains, but they attach their own email (often using a free service like Gmail or Yahoo) in the "reply to" field for any responses that come in.

Trust Your Gut

If the email address looks accurate and trustworthy but the contents of the message are suspicious, trust your gut. As mentioned before, sometimes legitimate email addresses just get hacked.

Compare the message you’ve received to those in the past: if the subject matter, tone, or anything else feels off in the latest email, disregard it.

Don’t use any of the contact information in the email either. Navigate to the company’s website or other presences yourself, where you can find their contact information and call them yourself. Ask them to confirm whether they sent the questionable email.

Keep Your Cool

When an email is laying out a dire situation and telling you to react immediately, your first reaction might be to panic and click links, log into suspicious websites, or hand over sensitive info that a few seconds of pause might have prevented.

Never open an attachment or click a link from an email you weren’t expecting, and never give your credentials to these emails or any webpages they link to.

When you get a message that induces panic like these, take the opportunity to calm down and assess the situation as objectively as possible.

Just keep cool. Assess the situation and use your tools to double-check the source of any suspicious emails.