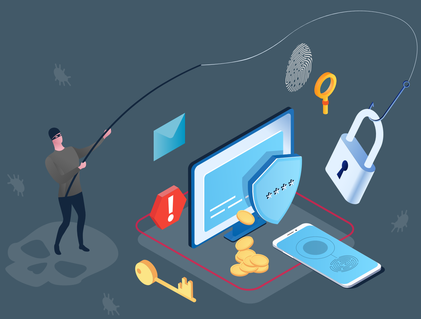
mailguard



6 Ways To Spot An Email Scam

Email scams are getting sneakier and more complex everyday – so what can you do to avoid being the victim of one?

To help, we've drafted an infographic of red flags that are typically present in a malicious email. Share this with your team, friends and colleagues – you might just save your company from being a victim of a scam email and from suffering huge losses.

1 The email doesn't address you directly

Does the email address you by generic words like "Dear Customer"? If so, beware. Legitimate emails are more likely to use your first name or full name.

2 Bad grammar

Nobody likes to read bad grammar. Emails with poor spelling and punctuation should raise alarm bells.

3 Distorted images

Do the graphics look a bit shabby? A legitimate notification from an established company is less likely to send emails with blurry images.

4 Instructions to click a link

Take note when an email asks you to perform an action. If there's a link, hover over it to see where you're being directed to before you click.

5 Weird origins

Always check where the email came from. Even some Hotmail, Gmail & MailChimp addresses could be scams. Company addresses are usually more trustworthy.

6 A sense of urgency

When the email is rushing you to do something, beware. If it's asking you to pay money by a due date, it could be a fraud.

Learning how to spot email scams helps protect your business. But sadly, it doesn't give you full protection. Talk to us about how MailGuard can proactively secure your business.

Email info@mailguard.com.au
or call at 1300 304 430.

www.mailguard.com.au