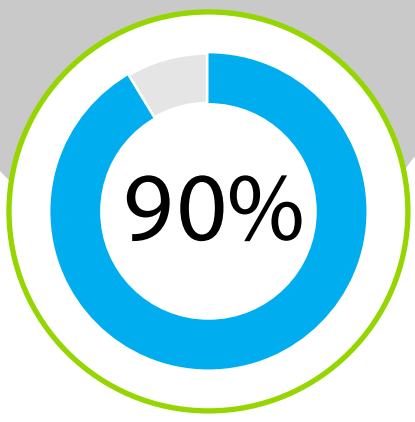
5 WAYS TO HELP YOU AVOID PHISHING ATTACKS



Did you know that 90% of modern data breaches now involve a phishing attack?

These attacks usually consist of fake emails designed to look like they're coming from a brand or institution your clients trust.

Their goal is to entice your staff to click a link or download an attachment, which, in turn, puts malicious files on their computer. This can enable hackers to steal end users' identities, breach your clients' systems, and more.

The best way to defend your business against phishing attacks is to train staff to identify phony emails before they click on them.
Training, your staff can and empower them to stay ahead of next-generation threats.

NOTE (We have seen phising attacks from links in SMS as well)

5 EASY WAYS FOR STAFF TO SPOT A FAKE

1 Who's the real sender?

Make sure the organization name in the "From" field matches the address between the brackets. Watch out for addresses that contain typos in the organization name (think mlcrosoft.com - not an i an l).

2 Check the salutation

If you do business with an organization, the first line of the email should always contain your name. Don't trust impersonal introductions like "Dear Client."

3 Use your mouse hover

Hover over an email link to see the full URL it will direct you to. Do NOT click the link—just hover. If the address isn't where you'd expect to go, don't click it. Check all the links—if the URLs are all the same, it's likely a phishing email, sometimes text may be a graphic and will send you via the link to the image.

4 What's in the footer?

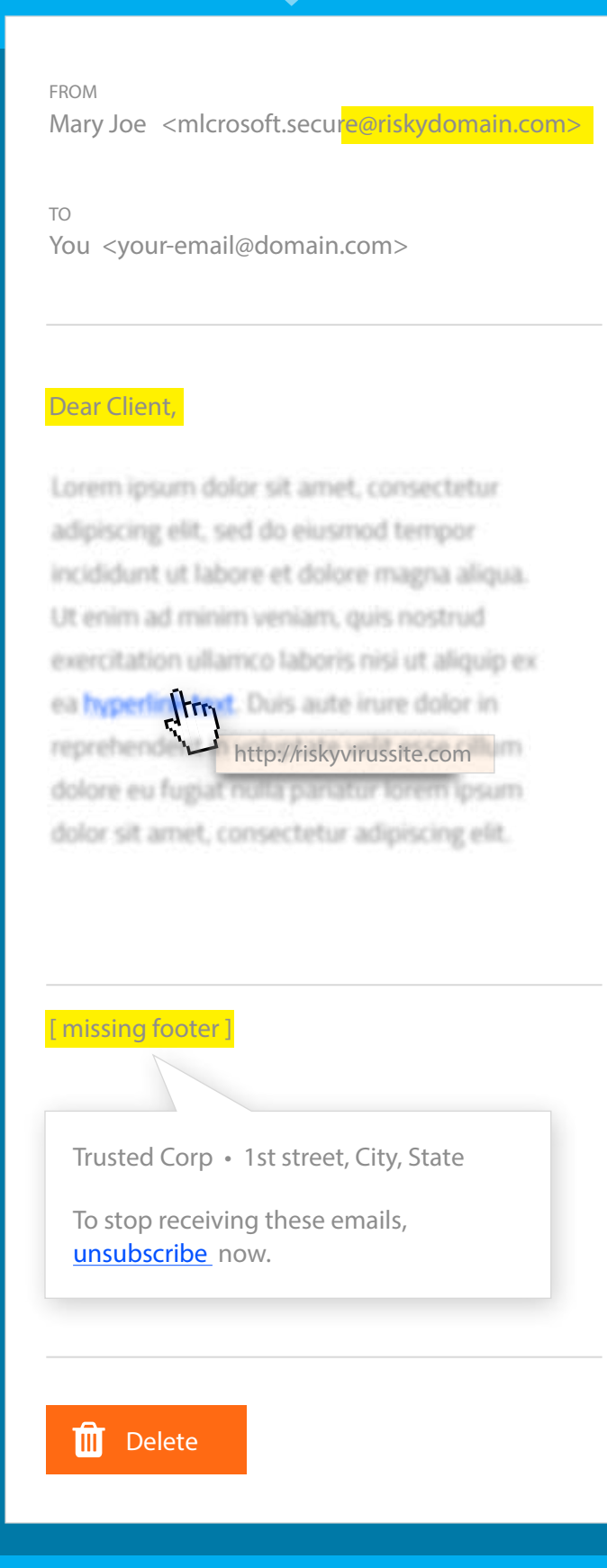
The footer of any legitimate email should contain, at minimum:

- A physical address for the brand or institution
- An unsubscribe button

If either of these items are missing, it's probably fake. Most companys also have a disclaimer in the footer.

5 When in doubt, delete

If you don't know the sender, or even if something seems off, delete the email. If it's not fake, the sender will contact you another way or send the message again, rather be safe than sorry and contact the sender directly to check the validity of the email.



Talk to us to day to see how we can help prevent these types of attacks

sales@whedoit.com | (08) 9467 4367 Perth WA
(02) 8005 8445 Sydney NSW

always online whedo.it