CyberGuard Technologies

Avoid becoming the victim of a PHISHING ATTACK

1. Hover over any links in the email to check the URL - if it doesn't look right, don't click it!
2. Check the sender – is the email address correct and in the right format, do you recognise it?
3. Don't open attachments that you weren't expecting
4. Don't open attachments in file types that you don't normally receive, for example HTML or EXE files
5. Never enter personal information into a form you open via an email link unless you are sure it is legitimate

USE CAUTION

If you weren't expecting an email but it looks like it came from a known sender, however you believe it could be suspicious, call them on their usual number (not the number in the email) and validate it first.

Report anything suspicious to your IT team.