How to spot the red flags of a phish

#1. Mismatched URLs:

Often, the embedded URL in a phishing message will appear to be perfectly valid, but when hovering your mouse over the URL, the actual hyperlinked address may appear differently. This is an indicator that the link could be fraudulent.

#2. Poor Spelling/ Grammar:

Large companies often have strict processes in place for reviewing company messages, especially when it comes to grammar, spelling and legality. So, if you receive a message littered with mistakes, there's a chance it may not be from a legitimate source.

#3. Requesting Personal Info:

No matter how legitimate or official an email looks, it's always a suspicious sign when they ask you for personal information. Banks and reputable companies will never ask you to send account or credit card numbers, as they should already know these details.

Others To Look Out For:

- Special offers that sound too good to be true
- 'Responses' from companies you've never contacted
- URLs containing a misleading domain name
- Unrealistic threats, like having your account deleted
- Emails that contain attachments/ website links
- Messages that urge you to act quickly

Tricky subjects. **The Top 10.**

The most common words in **BEC phishing** email subject lines.

Rank	Subject Line	%
#1	"payment"	13.8
#2	"urgent"	9.1
#3	"request"	6.7
#4	"attention"	6.1
#5	"important"	4.8
#6	"confidential"	2.0
#7	"immediate response"	1.9
#8	"transfer"	1.8
#9	"Important update"	1.7
#10	"attn"	1.5