


Phishing Identification Checklist



Email addresses can be spoofed, or forged, to make messages appear to come from legitimate sources. Victims are much more likely to cooperate when they believe they are communicating with someone they know, which is even more reason to fully scrutinize all requests for sensitive info or money! If you check any of these boxes, beware! You could be under attack!

☐ Does the email contain poor spelling or bad grammar?

☐ Is the email awkwardly worded or nonsensical?

☐ Is the "from" address unrecognizable or just plain weird?


☐ Does the email promise large sums of money or other unbelievable offers?

☐ Does the email use threatening language?

☐ Does the email contain a sense of urgency?

☐ Does the email have a call-to-action such as clicking a link?

☐ Does the email contain an unexpected attachment or request for money?



As always, follow our organization's policies and report security incidents, such as potential phishing attacks, immediately. If you have any questions, please ask!