How to spot phishing emails

Do you know the sender and is that their actual email address? If you don't recognize the sender of the email you've received, proceed with caution. Check if the display name differs from the actual email address, since the former can be customized by the sender.

Are there any attached files and if yes, were you expecting any? Beware of attached files, especially when not expecting any. Check the type of file that is attached and if it's an archive file (e.g. ZIP), do not open it. However, even a typical PDF or Word file can be rigged with a malicious payload.

Are you pressured to act in a certain manner or to act quickly? Hackers want their victims to act quickly so that they can't take the time to think rationally. If you are asked to act as soon as possible or to act in a manner that is suspicious (e.g. do not tell anyone about this), something isn't right.

Has the sender provided other means of contacting them? Look at the email signature of the sender for a phone or fax number that would allow you to verify the legitimacy of the message. Also, check if the sender is named individually rather than as part of group or team as the latter would be more suspicious.

Are there any spelling or punctuation errors? The presence of grammatical errors and poor formatting should warn you to treat the email carefully. Hackers are becoming more careful in drafting their messages, especially when targeting someone in the C-Suite (e.g. CEO, CFO, COO, etc.).

Are there links in the email to click on and where do they lead you to? Since adding a malicious link in emails is the most common attack vector for hackers, you should be very careful clicking on any links. Hover you mouse over the link to see where it would actually take you. If any different than what you expect, do not click on it.

Are you asked to provide personal or other sensitive information? No legitimate institution would ask you to submit sensitive information via email. If asked about username and password, account number, or anything similar, you should know better that you are being phished.

Is there a greeting in the beginning and is it specific to you? Since hackers target many recipients at once, likely the greeting won't be specific to you but rather something like "dear user". The lack of personalized greeting should raise an eyebrow and make you more cautious when checking the rest of the email.

Are you asked to send funds or pay a fee or fine to anyone? A prevalent tactic used by hackers because it brings profit. Every request or demand to send funds, made through an email, should be reviewed very carefully, especially if the manner is uncommon. Even if email is coming from an authorized user (e.g. CFO), it could be the case of hacked email address. Stay vigilant!

Does the email and its contents make sense to you? Sometimes, you just know something is wrong when you see it. Consider the example of receiving an email from a known sender but something about it makes your head tilt (different nature of the request, tone, choice of words, etc.).

Alliance for Healthier Communities
Alliance pour des communautés en santé