Gone phishing

Description

Phishing is the top attack method for social engineers – it's how they steal data, defraud people of money, and spread malicious software. Always think before you click!

Do you know how to spot a phishing attack? Here are five easy questions to ask yourself to avoid being caught on a cybercriminal's hook.

1. Does it push a sense of urgency?
2. Does it feature threatening language?
3. Does it offer unrealistic promises?
4. Does it contain suspicious links or attachments?
5. Does it come from a sender you don't know or didn't expect?

If the answer is yes to one, some, or even all these questions, there's a high likelihood you're being phished.


HACKING///
LOADING

Spot a phishing scam

Links: On a computer, you can identify a malicious link by hovering your mouse over it to reveal the full URL. If it looks odd or suspicious, or you're not sure, don't click!

Attachments: Never open an attachment unless you are certain it is from a trustworthy source.

Email addresses and URLs: Keep in mind it's easy to steal real company logos or create email addresses that appear to come from a legitimate source. Always thoroughly inspect the "from" address for any changes (e.g. Amazom.com where Amazon is spelled incorrectly).

Phishing is a dangerous attack that combines manipulation and deception. Remember to slow down and stay alert to avoid being scammed.

At work, report phishing attacks immediately and always follow our data and cybersecurity policies. Report Phishing by clicking the Phish Alert Button.

Category

1. Our Knowledge Centre