Phish Phinder

Tell-Tale signs of a (*potentially*) successful Email Phishing Scam

Hackers use Phishing Emails to obtain your:

- Usernames
- Passwords
- Credit Card #

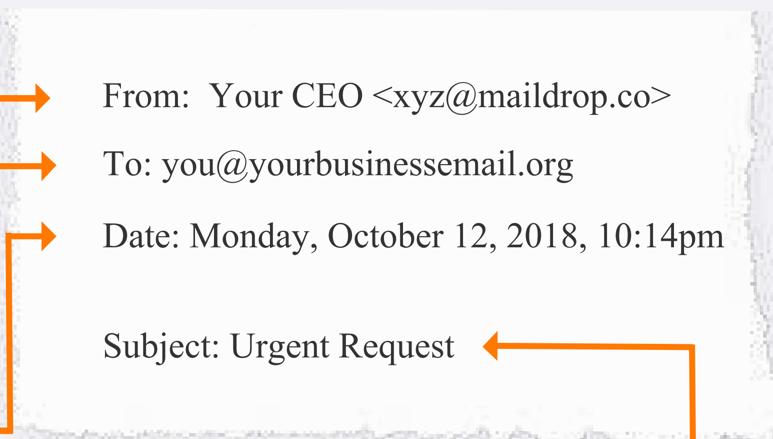
All it takes is for you to take the bait by

- Opening an attachment
- Clicking a malicious link
- Entering sensitive information

Anatomy of a Phishing Email

Look for any of the following suspicious elements when opening your next email.

THE HEADER



From: Your CEO <xyz@maildrop.co>

To: you@yourbusinessemail.org

Date: Monday, October 12, 2018, 10:14pm

Subject: Urgent Request

- Does the name match the sender?
- Have you received an email from this address before?

- Is the email directed at *undisclosed-recipients*?
- Was it sent to several addresses?

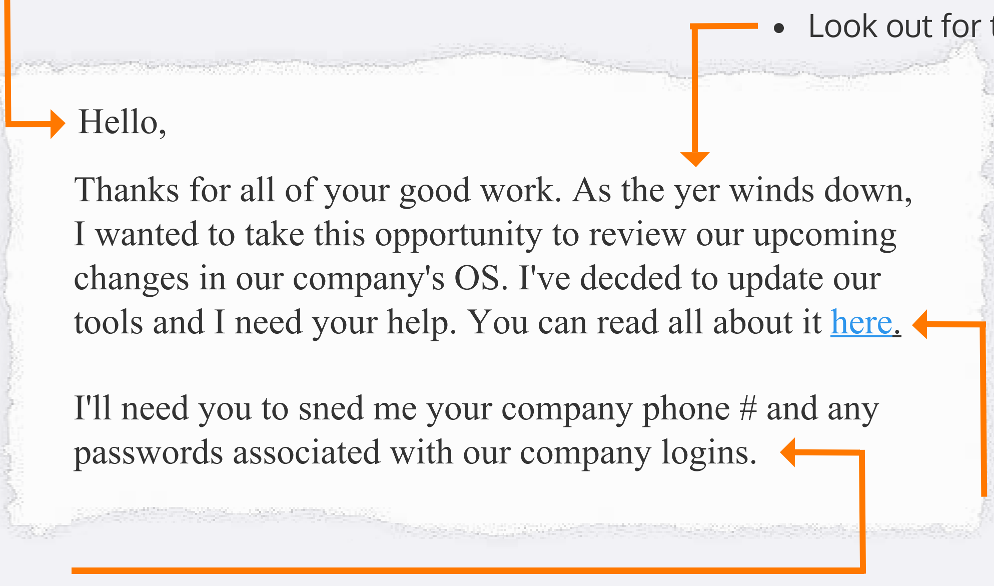
- Is this a normal time/date for this sender to have emailed you?

- Is the subject something relevant to my relationship with the sender?
- Is the subject line requesting my immediate response or promising me a reward?

THE BODY

- Is this the senders usual greeting?

- Look out for typos.



Hello,

Thanks for all of your good work. As the yer winds down, I wanted to take this opportunity to review our upcoming changes in our company's OS. I've decded to update our tools and I need your help. You can read all about it here.

I'll need you to sned me your company phone # and any passwords associated with our company logins.

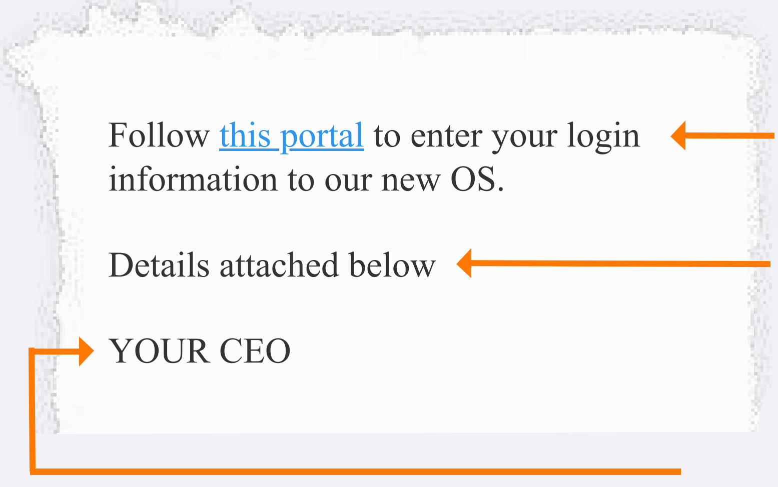
- Hover over a link before clicking.
- Does the URL look right?
- Has a letter been omitted?
- Are they using **.net** when it should be **.com**?

- If the sender is asking for private information you should immediately flag it.

Other Red Flags

- Is the content relevant to your relationship with the sender?
- Is the issue really as urgent as the sender is implying?

THE FOOTER



Follow this portal to enter your login information to our new OS.

Details attached below

YOUR CEO

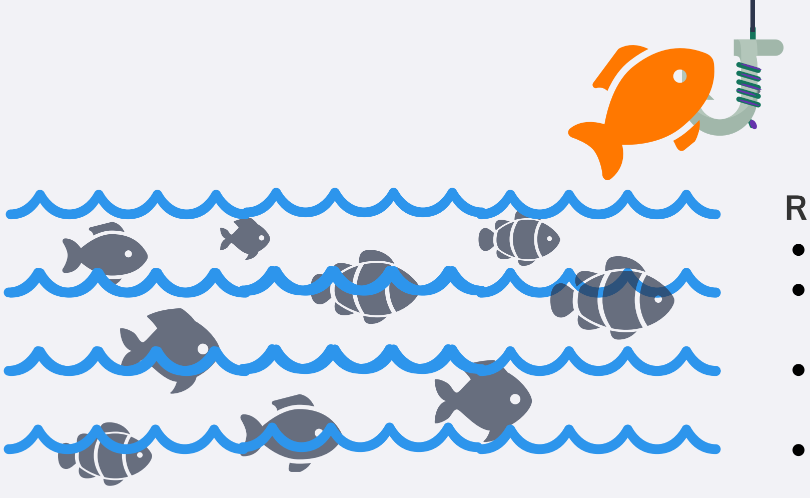
- Never offer your login information into a portal, especially if unsolicited.

- Do not open unexpected attachments, especially when the file type is a **.pif**, **.scr** or **.exe**.

- Does the salutation match the sender?
- Is this how they usually sign off?

Don't Take the Bait

1 in 10 Phishing Emails Succeed



REMEMBER:

- A little scrutiny goes a long way
- Be aware of the warning signs and don't ignore them
- If it doesn't look right, it probably isn't. Take a closer look before taking action
- Even the most savvy can still get caught.

Keep your anti-spam or anti-virus software up to date, and **SECURE YOUR NETWORK TRAFFIC** to mitigate phishing risk at your company!

avast business
powered by AVG and Avast