



WHAT IS A PHISHING?

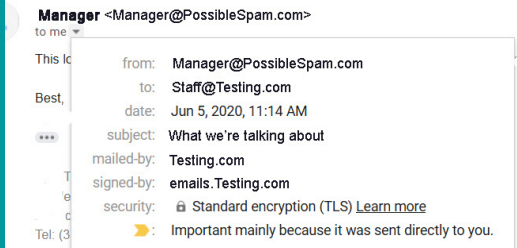
Phishing = The use of malicious emails that cause the recipients to divulge sensitive information or perform a task to bypass security.
Scammers incorporate the use of threats, unrealistic offers and coercion to create a sense of urgency in the user.

WHAT CAN I DO TO AVOID BECOMING A VICTIM?

Check spelling of the sender's email address to ensure its legitimacy

NOTE:

If you do not see enough of the address to determine if it is a spam email, you can click the downward arrow next to "to me" and see the complete sender's information as seen in the example below.



Free iPhone

From: Apple Inc / timcook@app1e.com
To: winner@yahoo.com

Dear Winner,
You have been selected to receive a free iPhone. In order to claim your free iPhone you must respond within 10 minutes.

Claim your phone by clicking below and entering your iCloud username and password.

<https://www.apple.com/free-iPhone>

Note misspelled email address

Are they offering you an expensive gift or saying you won a contest you didn't enter?

Free iPhone

From: Apple Inc / timcook@app1e.com
To: winner@yahoo.com

Dear Winner,
You have been selected to receive a free iPhone. In order to claim your free iPhone you must respond within 10 minutes.

Claim your phone by clicking below and entering your iCloud username and password.

<https://www.apple.com/free-iPhone>

Offer that is too good to be true

What if an email said: 'If you respond to this email in 10 minutes you win a free iPad.'

Would you respond to it? If something seems too good to be true it probably is.

Attackers use methods like this to create a sense of urgency in the recipient.

Look out for requests for sensitive information

DO NOT enter your username and password into unfamiliar websites.

Free iPhone

From: Apple Inc / timcook@app1e.com
To: winner@yahoo.com

Dear Winner,
You have been selected to receive a free iPhone. In order to claim your free iPhone you must respond within 10 minutes.

Claim your phone by clicking below and entering your iCloud username and password.

<https://www.apple.com/free-iPhone>

Request for sensitive information

Do not click on hyperlinks or download attachments in unexpected emails from an unknown sender

Free iPhone

From: Apple Inc / timcook@app1e.com
To: winner@yahoo.com

Dear Winner,
You have been selected to receive a free iPhone. In order to claim your free iPhone you must respond within 10 minutes.

Claim your phone by clicking below and entering your iCloud username and password.

<https://www.apple.com/free-iPhone>

Hyperlink in an unexpected email

Mouse over hyperlinks to see where the link will take you (Do not click on the link unless you know it is legitimate)

As you see by the "From" email example the address could be slightly misspelled and your brain would fill in the blanks.
Chances are the hyperlink will be similarly disguised.

Typical tricks are switching "m" and "n", using "l" for "I", swapping letters around in words such as "bnak" for "bank" - be alert for those methods.

Free iPhone

From: Apple Inc / timcook@app1e.com
To: winner@yahoo.com

Dear Winner,
You have been selected to receive a free iPhone. In order to claim your free iPhone you must respond within 10 minutes.

Claim your phone by clicking below and entering your iCloud username and password.

<https://steal-your-password.com>

<https://www.apple.com/free-iPhone>

Use a secondary verification method (ex: phone call or text message)



Do not respond to a questionable email, or forward it, without checking its validity! Rely on your IT Department for assistance.

Notify the IT Department of any suspicious requests

Expressing your concerns as soon as possible can help the rest of the team from falling prey to a phishing email.

Let your IT professionals investigate any communications you have concerns about.



Need Help Securing Your Business?
Contact Anjolen Inc:
Michelle Tuttle: mtuttle@anjolen.com