

Don't Fall for a Phishing Attack!



**7 THINGS
TO LOOK
FOR IN EMAIL.**

DEARBORN PUBLIC SCHOOLS



FROM:

- Do I recognize the sender's email address?

Hint: Hover your mouse over the name in Gmail. On a phone, click on name.

- On hover, you should see a picture of the person if that person normally has a photo.

TO:

- Were you CC'd on an email but don't know the other people?
- Was the email sent to an "odd" assortment of people? Maybe people that you know, but wouldn't normally be included in a single email.
- Were you BCC'd only?



DATE:

Was the email sent at an unusual time? (Like 3 a.m.)

HYPERLINKS:

- Be very wary of hyperlinks.
- Hover your mouse over a Hyperlink to see where it is really going (the part after the @sign). On a mobile device, you can long press on link.
- Watch for misspellings. (i.e. bankoramerica, amazan, etc.)
- Watch for long URL that include a misdirection (www.amazon.ripoff.com) (always look for the part right before the .com (or .net).
- Be careful if you are being asked to sign in after clicking a link. You are probably already signed into Google.

Red Flags:

Here are some handy tips to help you prevent a successful phishing attack.

Note that it may not be a single tip, but a combination of factors.

If your instincts say something is wrong, stop and think. Don't act until you consider your choice.

SUBJECT

- Does the subject make sense?
- Is the subject irrelevant to the message?
- Is the message a Reply to something that you didn't send?

ATTACHMENTS:

- Is there an attachment that you weren't expecting?
- Does the attachment end in anything other than .txt?
- Frequently, attachments that end in .doc will contain a virus.
- Attachments that end in .zip are a major problem.
- Attachments are the number 1 way to spread a virus.

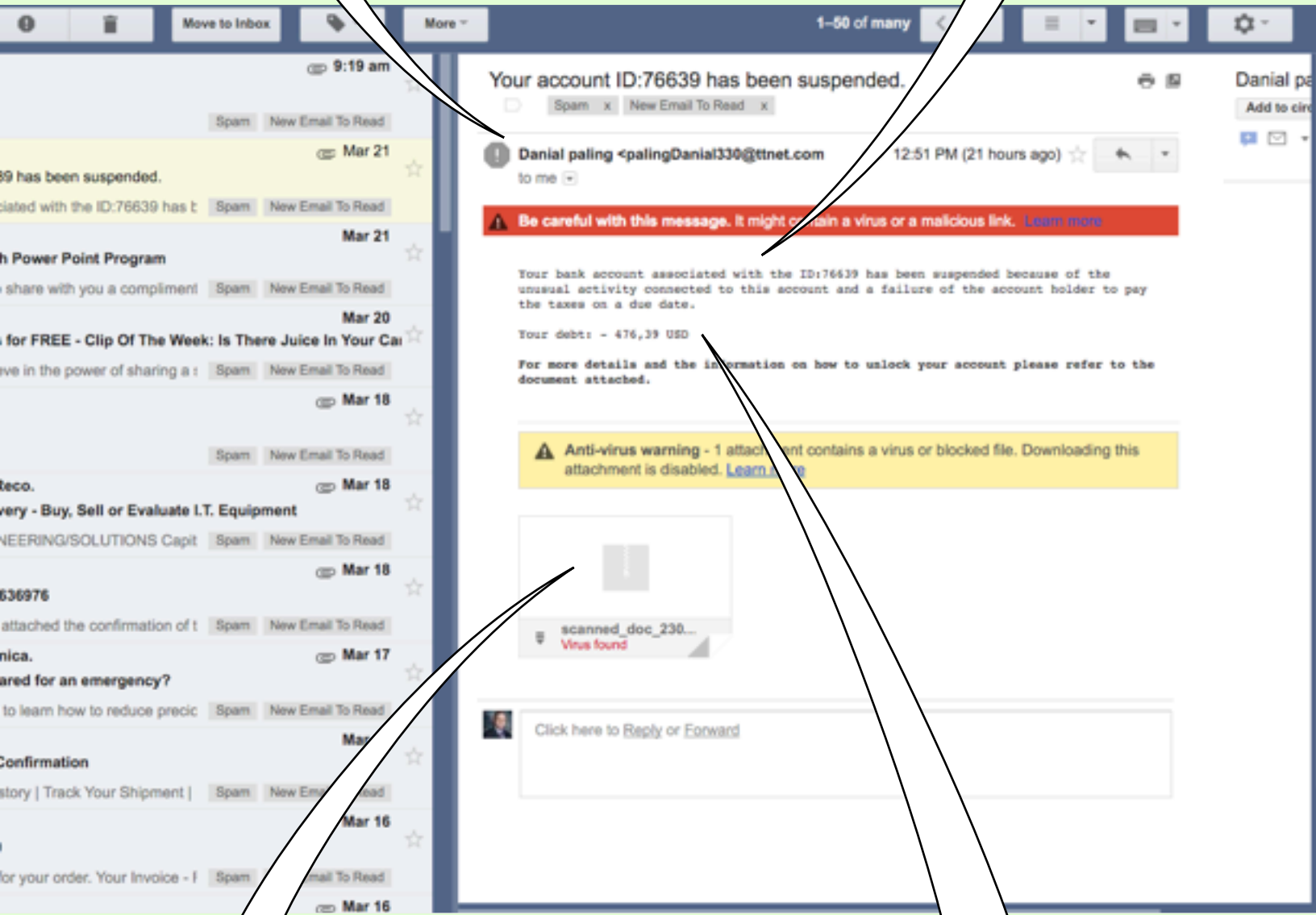
CONTENT:

- Are you being asked to click a link to avoid a negative consequence?
- Does the grammar seem slightly off?
- If you know the sender, does this sound like something that they would send?
- Are there odd letter substitutions? (0 instead of o, 1 instead of l, etc.)
- Are there any subtle threats involved?
- Are you being promised something of value that seems "too good to be true"?

ONE EXAMPLE:

Unknown Person

Threat!



.DOC attachment

Money is written with a comma instead of a period.

This is an example from my Google SPAM folder. This is being used as an example only. Notice that Google has already identified that the attachment contains a virus. There are lots of notices on this one. You should check your SPAM folder occasionally.