

What does Phishing look like?



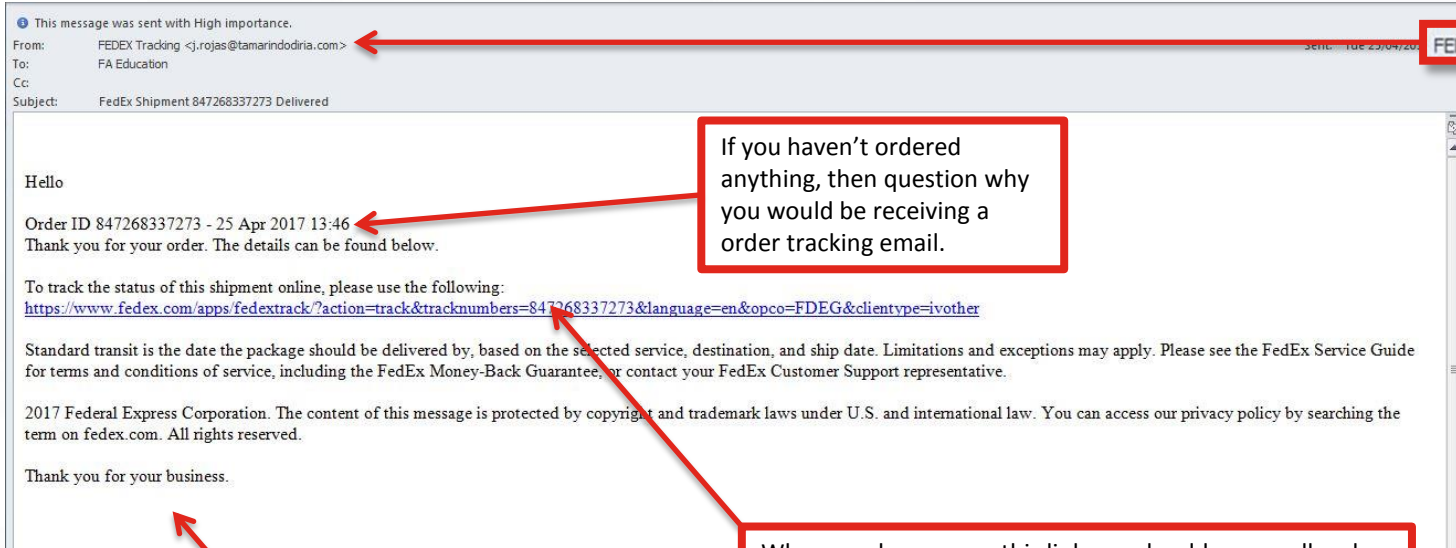
What does Phishing look like?

This PowerPoint will show you 5 different phishing emails that have tried to access the FA network.

There will then be descriptions on each one showing you what to look out for when trying to identify a phishing email.



Email 1



FEDEX Tracking <j.rojas@tamarindodiria.com>

If you haven't ordered anything, then question why you would be receiving a order tracking email.

Even though it states that it is from *FEDEX Tracking* the actual email address has nothing to do with FedEx, so always double check the email source.

When you hover over this link you should see a yellow box indicating which web address you are going to. Make sure this corresponds with the blue underlined address.

No corporation branding can sometimes be a sign that the email is not legitimate.



Email 2

From: Martin Burnell <Martin.Burnell@thefa.com> Sent: Mon 24/04/2017
To:
Cc:
Subject: aw

Clearly this is not a real subject title and therefore should make you question how legitimate the email is.

This is more tricky as it is coming from an FA account, if you do not deal with this person on a regular basis then perhaps question it.

Your ticket is pending for acceptance from you for its closure. Please review and accept/reject modification thereafter. Please click on the link provided below to accept the resolution.

Click here to Accept or Reject this resolution<<https://owawebapp.000webhostapp.com/>><<http://www.connetedtomicrosoft.citymax.com/outlookhelpdeskx.html>><<https://owawebapp.000webhostapp.com/>><https://leidos.service-now.com/survey_login.do?jvar_login_goto_url=nav_to.do?uri=expert_shell.do%3Fsysparm_sys_id%3De75514511f0020005a3637b8ec8b7006%2526EV%3Asysparm_task_survey%3D8701f7d90fe03600707cda40f1050eae>

Additional details about this ticket are:
Incident Number : INC0143872<<https://owawebapp.000webhostapp.com/>><https://leidos.service-now.com/email_login.do?jvar_login_goto_url=gbp/incident_detail.do%3Fsysparm_name=incident.do?sys_id=6a5f63d90fe03600707cda40f1050e41>
Created : 2017-01-25 17:18:23
Summary : Reset IE Home Page

Please do not reply to this automated message

Thank you,

Service Desk Team

From past experience emails with links in them do not look like this. They will normally just be one web address, but as you can see this has < and > placed in between. Also if you haven't heard of the website that you are being pushed towards the maybe do a bit of research before clicking the link.

This email has a different signature to who you received the email from. Again this should be a red flag.



Email 3

If the person contacting you does not work in the technology sector then they wouldn't be contacting you with information relating to it.

From: Martin Burnell <Martin.Burnell@thefa.com>
To:
Cc:
Subject: IT Newsletter

Dear colleagues, Chers collègues,

The fact that the email is in French should immediately raise your suspicions.

To keep you abreast of ICT developments of the Organization and to keep your technical skills up to date, the latest IT Newsletter issue is now available at <https://owawebapp.000webhostapp.com/>

The technology team never refer to themselves as ICT when communicating with the business, so we wouldn't use that terminology.

We also do not run a IT Newsletter here at the FA and if we do launch one you would hear about it, rather than just getting it in a sentence on an email.



Email 4

From: Martin Burnell <Martin.Burnell@thefa.com>
To:
Cc:
Subject: ID:431 -Account Reset Notification

Sent: Mon 24/04/2017 15:09

This message is sent from a trusted sender.

Account Confirmation

Dear User,

We received a request from you yesterday to terminate your account permanently and we are working on that now. but first we need to confirm,

If you did not request this, click the button below to cancel the request immediately.

<<https://owawebapp.000webhostapp.com/>>Cancel

Request<<https://owawebapp.000webhostapp.com/>><<http://www.connetedtommicrosoft.citymax.com/outlookhelpdeskx.html>><<http://www.outlookwebappx.citymax.com/help-desk.html>><<http://www.imxprs.com/free/sdfglir/outlook>><<http://ibbqf5e95.ukit.me/>><<http://www.latorredelsole.it/virtualtour/Shop/output/ikm/inbox.htm>>

If you actually request to delete your account, please ignore this email.

Thank you for using Microsoft services . .

Microsoft respects your privacy. To learn more, please read our Privacy Statement <<http://moduletech.no/content/doc.htm>> . <<http://iorionstienda.cl/web/wp-adnim/doc.htm>>

There are tools that will put this sort of statement onto emails, but they will not make it so obvious and it will not likely be the first thing on the email.

If you notice this sentence starts with talking about Microsoft and points you towards their privacy statements. Neither website is a Microsoft address so should not be trusted.

From past experience emails with links in them do not look like this. They will normally just be one web address, but as you can see this has < and > placed in between. Also if you haven't heard of the website that you are being pushed towards the maybe do a bit of research before clicking the link.



Email 5

From: Graham Hill <Graham@thenationalleague.org.uk>
To:
Cc:
Subject: Did you Request for this

If there would be no need for you to communicate with someone from this company then wonder why you are being contacted by them.

We received a request from you yesterday to terminate your account permanently and we are working on that now. but first we need to confirm, If you did not request this, click on:
<http://www.webhelpxx.citymax.com/admin.htm> to cancel the ongoing process n

terminate your account

This email actually looks unfinished and seems to be missing the end of a sentence. Again if the email was this serious they would end it or if it was legitimate they would at least send you an email straight after with the rest of the information on.

Termination of an account is quite a serious situation, so anything that is this important would always come from IT Support.

