BEWARE OF RANSOMWARE

There are many ways bad guys are trying to get your money; phishing, spam, malware, virus, etc. The latest method is called RANSOMWARE. When you click on a bad link, it takes over your PC, encrypts your files and puts a message on your desktop stating to get your files back, you must send $$$.

It happened to local Habitat for Humanity.

BEWARE OF RANSOMWARE

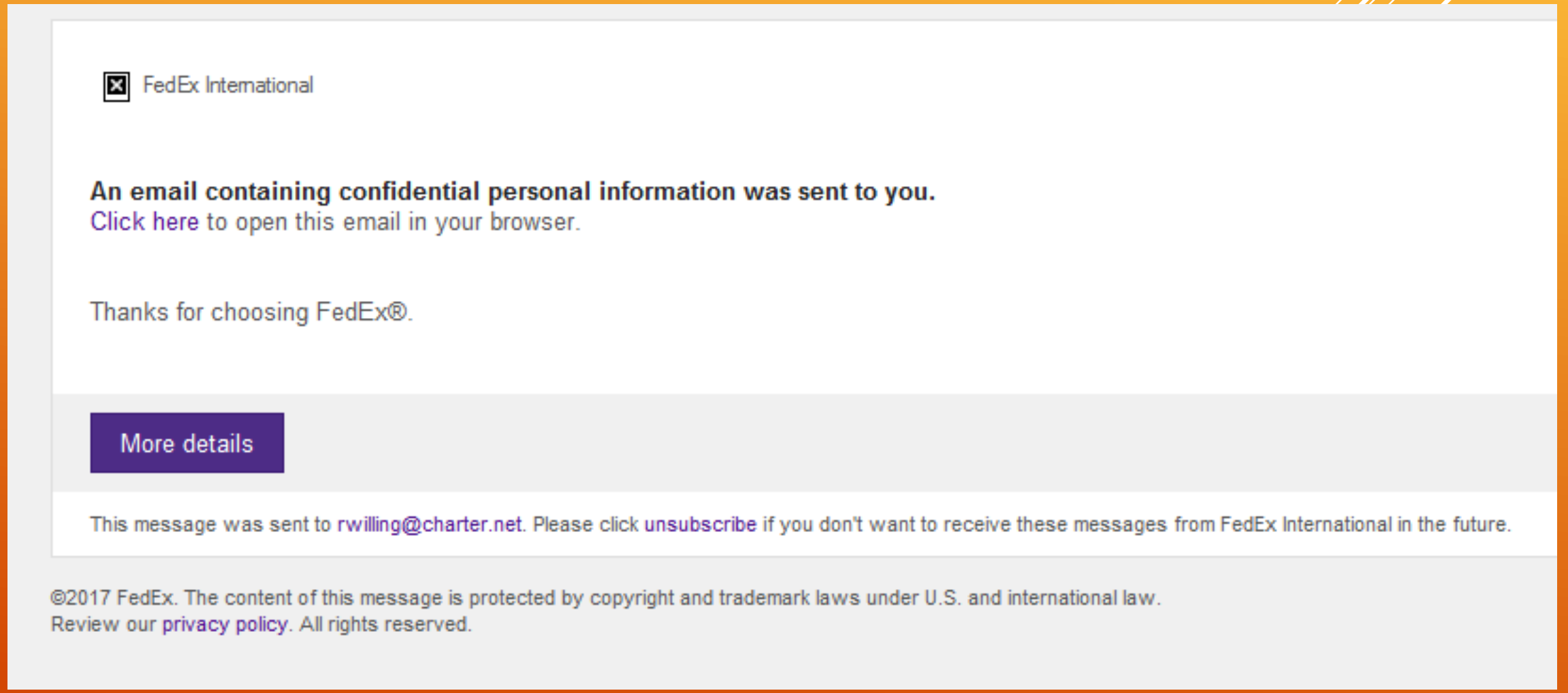
I have received several emails from "FedEx" saying they need more information so they can deliver an email or package. Note: there were never any notes or messages left on my door which is the normal process.

Real questions – Why is FedEx sending me a email with confidential/personal information??????
Why is it not in my inbox???????

The following slides show how to prove the email ***IS NOT*** from FedEx.

BEWARE OF RANSOMWARE

Actual email below – Looks real!



FedEx International

An email containing confidential personal information was sent to you.
Click here to open this email in your browser.

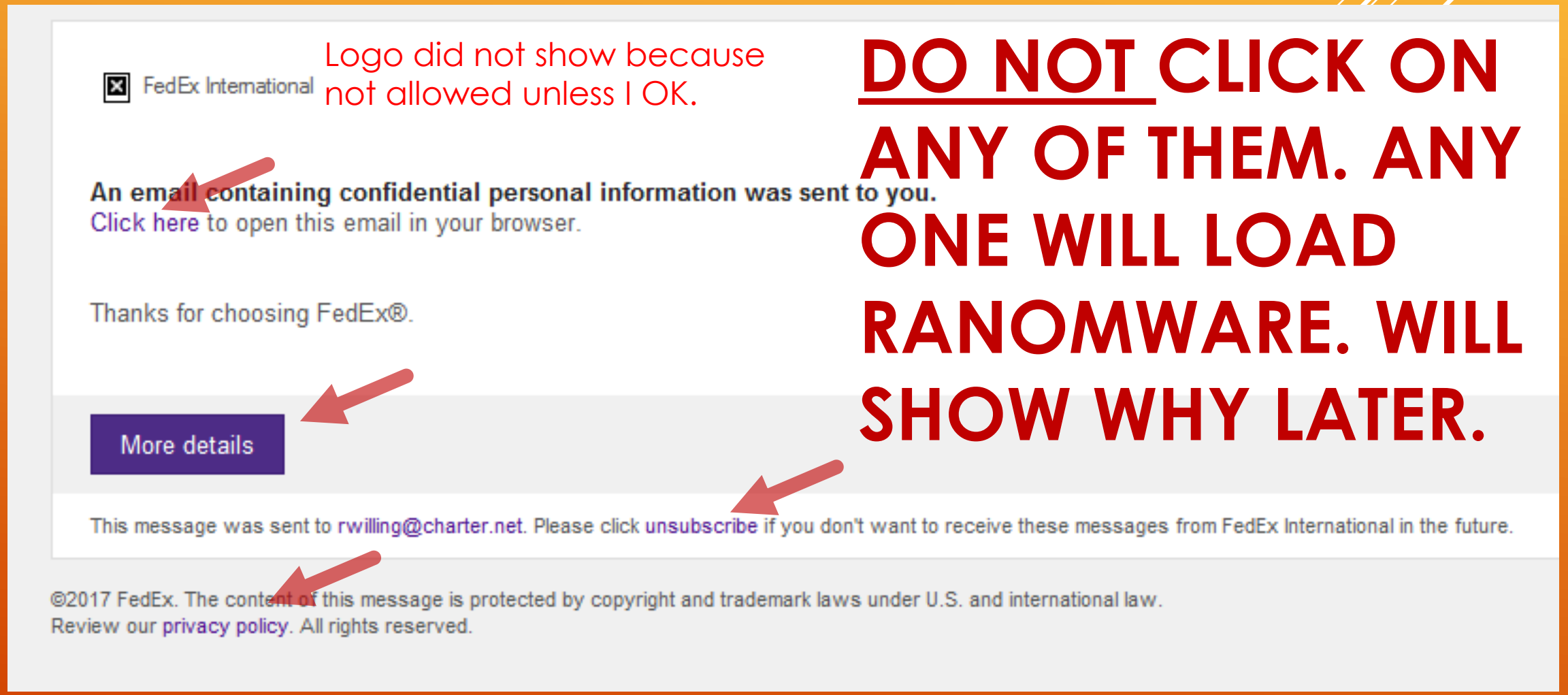
Thanks for choosing FedEx®.

More details

This message was sent to rwilling@charter.net. Please click unsubscribe if you don't want to receive these messages from FedEx International in the future.

BEWARE OF RANSOMWARE

Actual email below – note all the link points - see arrows



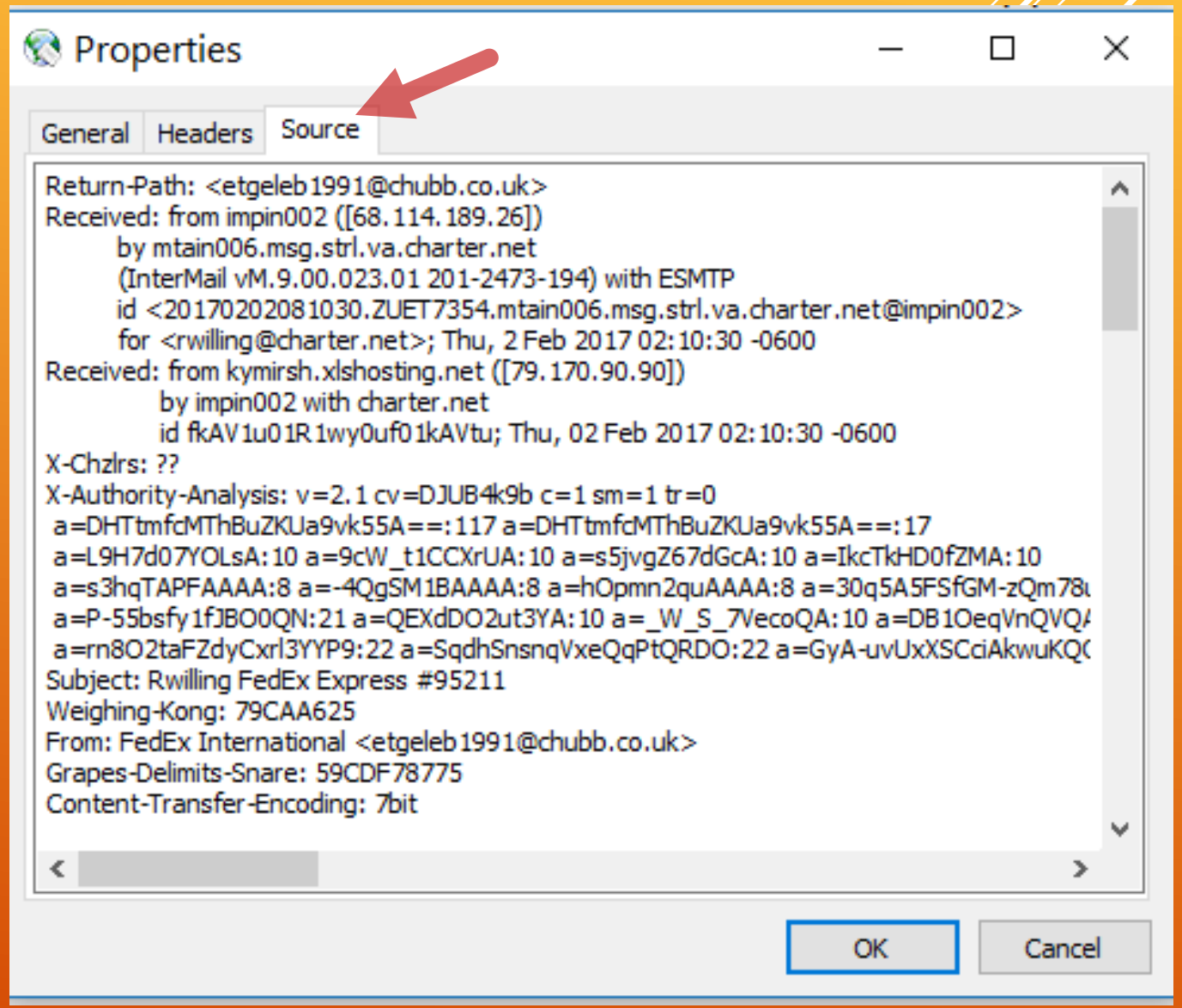
BEWARE OF RANSOMWARE

Next view the message source, the normal process is to;

Right click on the message then click on Properties

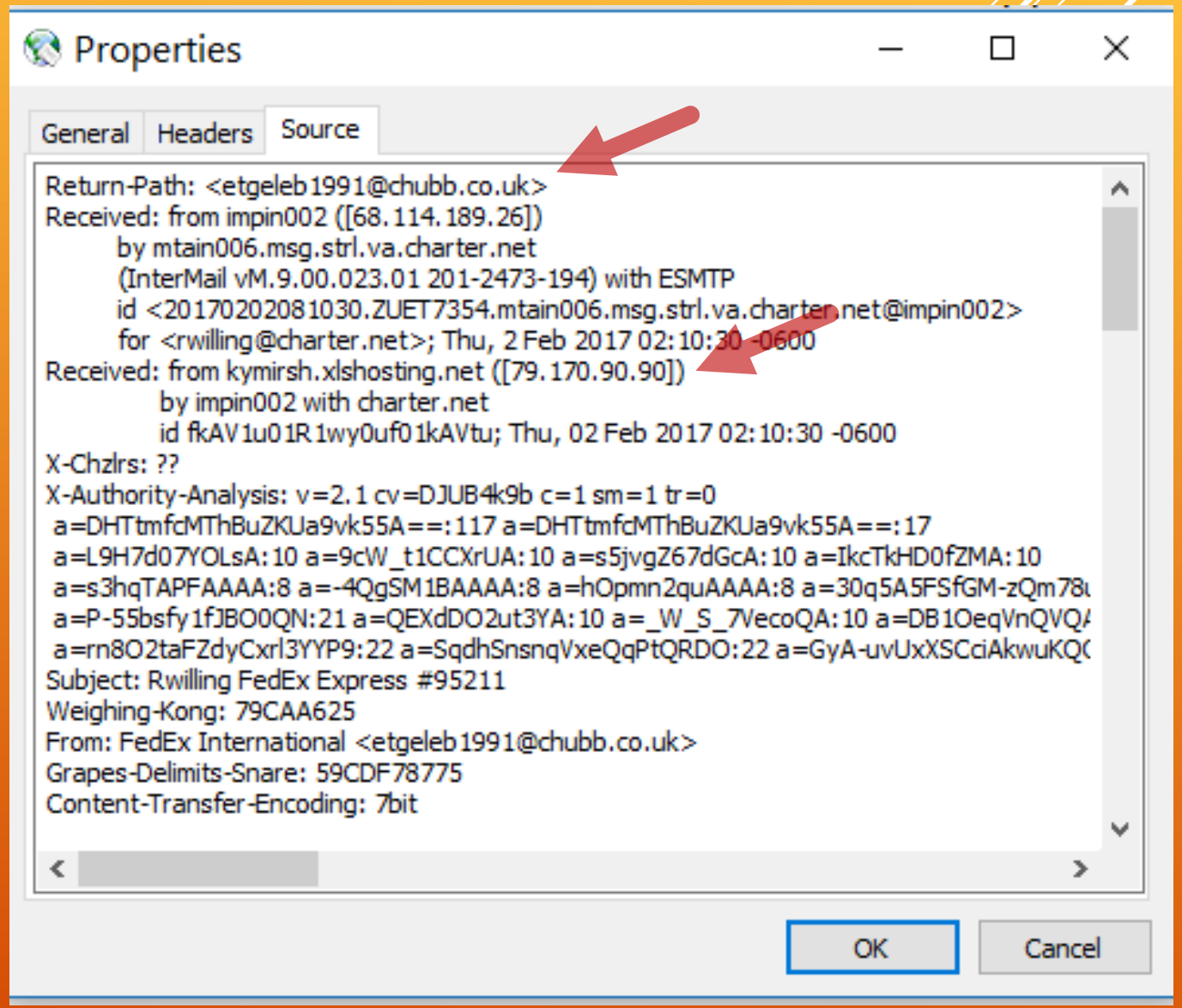
Click on the Source tab

You should see a view like this.



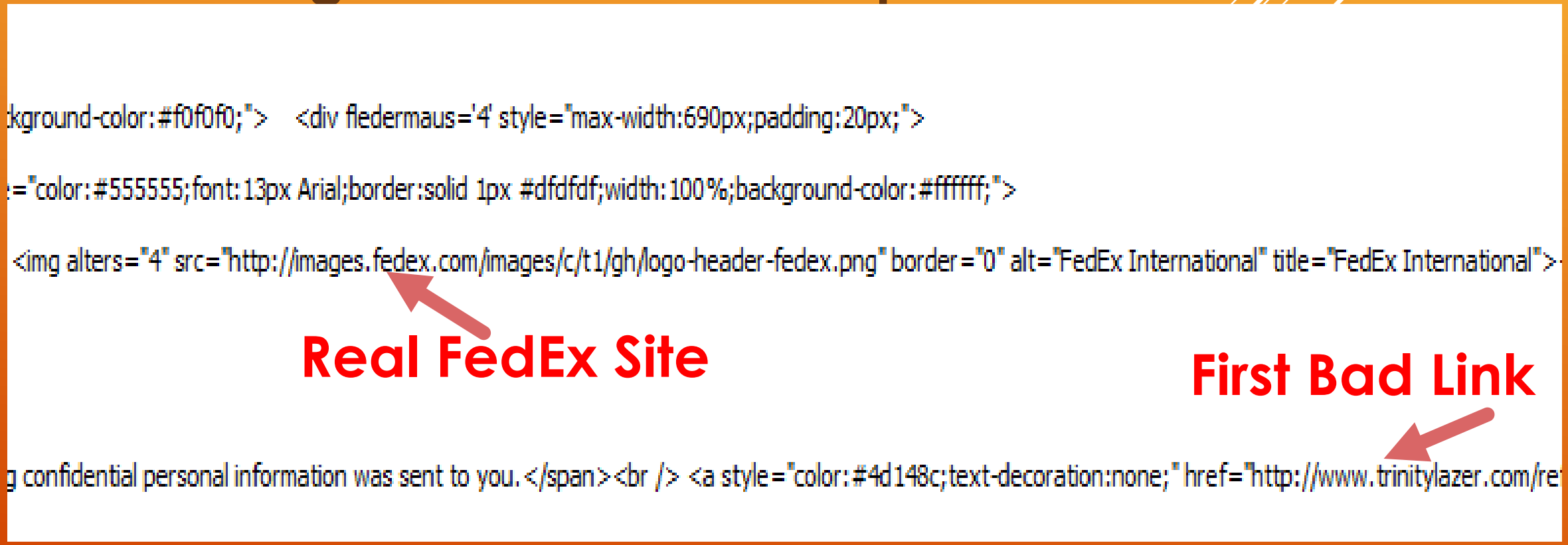
BEWARE OF RANSOMWARE

Looking at the source, you will see the return email address. Note it's origin. NOT FEDEX!! This is though a real website for a UK insurance company. Do you think FedEx would be sending a message from United Kingdom if they were trying to deliver an email or package in the U.S.?



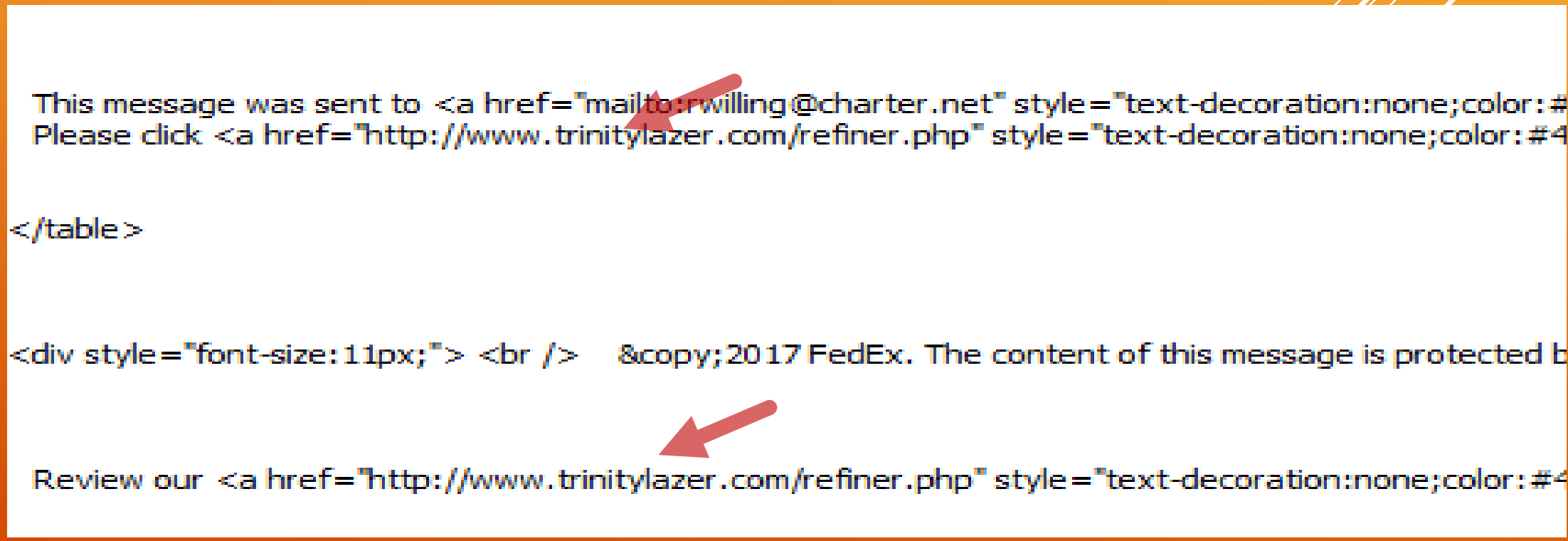
BEWARE OF RANSOMWARE

Looking more at the source, you will see they actually used a REAL FEDEX logo from the actual FedEx web site!! That is being creative and deceptive.



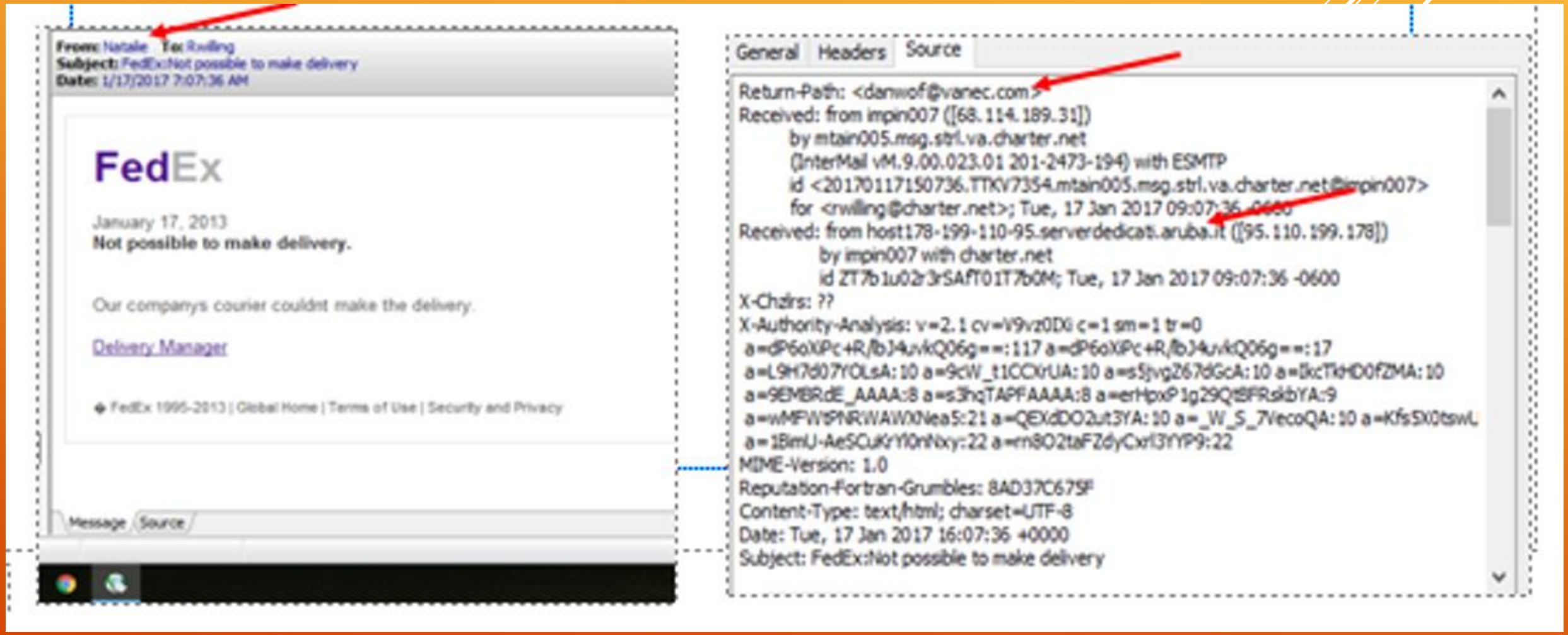
BEWARE OF RANSOMWARE

More looking at the source, you will see EVERY link is pointing to the same web site – the location of the RANSOMWARE. You will see this site as you position your cursor over EVERY link in the original email. DO NOT CLICK!!



BEWARE OF RANSOMWARE

Another actual “FedEx” email below – Note Aruba!



BEWARE OF RANSOMWARE

There are several government agencies that try to help protect users from the bad guys. Some are listed below.

* *ftc.gov/complaint* - Federal Trade Commision
  - ID theft, Fraud, Debt collection
* *consumerfinance.gov/complaint* - Consumer Finance Protection
  - shady business, others same as FTC
* *ic3.gov/complaint* – Internet Crime
  - scams, hacking, phishing, auctions, investment
* *donotcall.gov or 888/382-1222*

Another web site from AARP may help you stay current to threats.
aarp.org/fraudwatchnetwork Don't seem to have to be a member.

Report bad emails looking like FedEx to abuse@fedex.com

BEWARE OF RANSOMWARE

One of the best things you can do to be prepared if this does happen is to keep all files and system backed up to a removable device, e.g. a thumb or hard drive. Your loss would be only those items created since last backup.
See Galen's backup video on our website "Presentation Handouts" page that shows how to make file histories. I have put more information on page 10 of the Jan '17 club newsletter on the website under "Newsletter" that covers additional backup options.
This presentation is on the"Presentation Handouts" page.

Galen's video http://www.rascal.cc/files/Download/filehistory.mp4
Newsletter http://www.rascal.cc/files/Download/nl1702.pdf

Do it soon and be better protected from the bad guys.

BEWARE OF RANSOMWARE

What else can we do to help protect our files and system?
Use free or fee programs that the experts recommend.

A few free programs;

Virus	AVG, AVAST…
Malware	Malwarebytes, Spybot Search & Destroy, Microsoft…
Firewall	ZoneAlarm…
Ransomware	Cybereason RansomFree…

Do a web search for the experts latest recommendations, evaluations and reviews. This is a dynamic area and the top ones change often because new threats occur almost daily.