HOW TO DECODE A WEB ADDRESS

Does that link belong to Lehigh?

About this tutorial

- This quick guide is intended to make it easy for you to spot fraudulent web addresses, which frequently occur in phishing e-mail messages.
- It is not a complete guide to everything there is to know about web addresses—the objective is simply to help you answer the questions “where does this link go?” and “does it go to Lehigh (or to the place it claims to go)?”
- To answer these questions, you just need to know where to look, and learn to ignore the stuff that’s irrelevant.

Links: Where do they go?

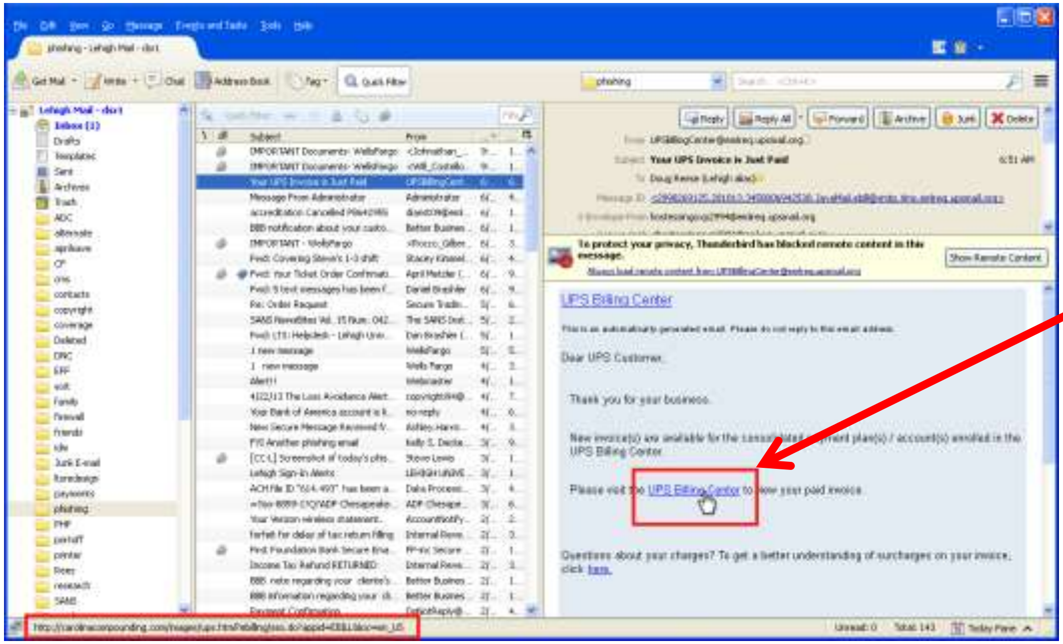
- All links have two parts:
  - The link text, which is what is displayed (often, but not always, this is in blue and underlined).
  - The link address, which is the address of the page where the link will take you (you don’t immediately see this).
- For example: Click here. (The link text is the word “here”; the link address is http://www.lehigh.edu)
- It is important to note that the link text can *look* like a web address (we’ll see an example shortly), but even if it does, link *text* doesn’t affect where you go—the link *address* does.

Links in email

- In an all-text email message, many browsers will automatically display any web address as a link (where the link text and the link address are the **same**).
- For example: http://www.lehigh.edu (the link text is the same as the link address).
- Phishing messages will exploit this fact to try to fool you—they will often have links whose **link text** looks like a safe and familiar web address, but the **link address** points somewhere else.

Seeing the link address

When you hover the cursor over a link (point, but don't click), the status area at the bottom of the window will usually display the link address.



From: UPSBillingCenter@wdreq.upsmail.org

Subject: **Your UPS Invoice is Just Paid** 6:51 AM

To: Doug Reese (Lehigh alias)

To protect your privacy, Thunderbird has blocked remote content in this message.

UPS Billing Center

This is an automatically generated email. Please do not reply to this email address.

Dear UPS Customer,

Thank you for your business.

New invoice(s) are available for the consolidated payment plan(s) / account(s) enrolled in the UPS Billing Center.

Please visit the UPS Billing Center to view your paid invoice.

Questions about your charges? To get a better understanding of surcharges on your invoice, click here.

http://carolinacompounding.com/images/ups.htm/ebilling/ssn.do?appid=EBILL&loc=en_US

web address appears here

Hover here, over the link

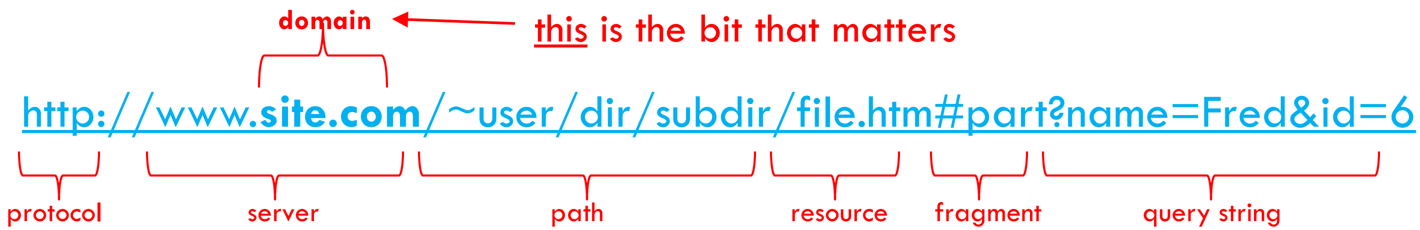
This works in many email programs and web browsers.

Always check the address

- Remember: even if the part of the link that you see (the link text) *looks* like a web address, always hover over the link to check the actual link address; it might be different.
- Note: if it *is* different, that fact by itself indicates that the message is probably fraudulent.
- **The point is, you don't need to click on a link to see where it goes.**

Parts of an address

- A web address has several parts: the protocol, the server name, the path, the query string, the fragment identifier, and so on.



domain

this is the bit that matters

http://www.**site.com**/~user/dir/subdir/file.htm#part?name=Fred&id=6

protocol

server

path

resource

fragment

query string

- **However**—there is only one thing you *really* care about: does this link point to a web site that belongs to the organization it says it does?
- For this, what you need to know is the **domain.** This is the last part of a **server name** (for example, at Lehigh, this is always **lehigh.edu**).

The server name

- In a web address, the server is specified in the same place every time.
- It starts after the double slash ("//") near the beginning of the address, and it ends at the very next slash.
- So, for example, in http://mysite.**myco.com**/bingo, the server name is mysite.myco.com.
- The domain in this example is myco.com. Since the domain is not lehigh.edu, this is not a Lehigh site.

Domain names

- Domain names indicate who the site belongs to.
- Universities and other educational institutions have domain names that end in .edu (Lehigh owns the domain lehigh.edu).
- Many corporations own domain names that end in .com (mcdonalds.com, bestbuy.com, homedepot.com).
- Domains ending in .gov or .mil are government or military, respectively.
- Domains ending in two letters (like .us or .ca) indicate countries (the US and Canada, in this case).

Domains and servers

- The server part of the web address contains the domain (always at the end).
- So Lehigh has servers like:
  - portal.lehigh.edu
  - coursesite.lehigh.edu
  - cf3.cc.lehigh.edu
- Notice that they all end in **lehigh.edu**
- So a Lehigh web address might look like: https://confluence3.cc.**lehigh.edu**/display/LTSCAS/CrashPlanPro+Backup+Server

Examples of valid web addresses

- http://www.**irs.gov**/pub/irs-pdf/f1040.pdf
  (this is a link to a PDF of a tax form at the IRS—the domain is **irs.gov**).
- http://www.dmv.state.**pa.us**/centers/vanityPlate.shtml
  (this is a link to an information page at the Pennsylvania Department of Motor Vehicles—the domain is **pa.us**)
- http://support.**microsoft.com**/ph/2514/en-us
  (this is a link to a Microsoft knowledge base item—the domain is **microsoft.com**)

Phishing and web addresses

- A lot of phishing messages are very straightforward—they don’t expect you to check where the address goes. So many web addresses in phishing messages look nothing at all like what they should. Links that are supposed to go to Lehigh web sites don’t even mention Lehigh anywhere.
- BUT, phishing message creators are getting cleverer, and they are starting to use web addresses that seem to be Lehigh-related, even though they aren’t.
- As long as you are careful to check the domain, you can spot these too.

Trying to fool you

- In a phishing email message, link addresses may have extra information that is designed to try to fool you.
- For example, the server name may be extra long, and mention Lehigh (or even lehigh.edu!) near the beginning. But if the domain (the end) isn't lehigh.edu, it isn't a Lehigh site.
- Example:

  http://lehigh.edu.myform.**myco.com**/go.html

  the domain is myco.com, not lehigh.edu—this is **not** a Lehigh address. (lehigh.edu is not at the end of the server name)

Dirty tricks

- □ Or something that looks like a Lehigh server name may appear, but not in the place a server name should.

- □ Example:
  http://site.**myco.com**/webmail.lehigh.edu/go.cfm
  again, the domain is myco.com, not lehigh.edu—this is **not** a Lehigh address (the lehigh.edu is in the wrong place—it's not in the server name at all).

- □ Example:
  http://site.**myco.com**/show.html?go=www.lehigh.edu
  once more, the domain is myco.com, not lehigh.edu

Dirtier tricks

- □ Or the domain may be almost lehigh.edu, but not quite.

- □ Example:
  http://services.**my-lehigh.edu**/gethelp.php
  the domain is my-lehigh.edu, not lehigh.edu (the parts are separated by periods and must match exactly).

- □ Example:
  https://portal.**leigh.edu**/secure/login.php
  the domain is leigh.edu, not lehigh.edu (spelling counts, and almost isn't good enough).

Read it right

- Remember:
  - Only look at the server name (the part between // and the next /).
  - Only look at the last part of the server name (something-dot-something).
  - If it isn't **lehigh.edu**, it isn't a Lehigh site. (Likewise, if it isn't irs.gov, it isn't the IRS, and so on).
- Always check to see where a link points before you click on it. Stay safe.

Contact

If you have questions, contact the Help Desk at 610-758-4357, or get in touch with me:

Doug Reese
LTS Help Desk
610-758-4357
dsr1@lehigh.edu