Avoiding Dangerous Links

Handling Email Scams

Recognise common email traps and avoid dangerous links

Learning Objectives

When you complete this section, you'll be able to:

- Describe why attackers use links in email scams
- Recognise fraudulent URLs
- Describe four ways in which attackers manipulate links
- Examine suspicious email links without clicking on them

What Are the Dangers of Email Links?

Links aren't really dangerous until you click on them.

Attackers send emails with links to:

- Verify that your email is valid (and consequently send you more dangerous emails)
- Trick you into visiting a fake website and entering your credentials for a well-known website
- Exploit your web browser to take control of your computer or download malicious code (like ransomware)

How URLs Work

URLs are the complete addresses to specific websites.

www.dailydelicious.net/recipes/spider-cookies/

How Links Work

Links point to a specific URL. Links make URLs clickable.

Links can point to URLs in clickable text.

Links can also be displayed in full: https://www.cabrini.com.au

Links can even be graphics or buttons:

[v22.2.1]

How Domains Work

http://www.wombank.com

In a URL, the domain name—in this example, *wombank.com*—works like an online home address for a website.

Attackers Manipulate URLs to Trick Users

Manipulating a URL goes beyond using the right words to trick you. Attackers will often change links in other ways to look like valid URLs.

Let’s take a look at some examples …

Shortened URLs

Shortened URLs are forwarding addresses for longer links. Attackers use link shortening tools on the Web to conceal a link's true destination.

If you suspect you've been given a shortened URL, you can search the web for a URL expander. Copy the URL and paste it into the tool to find out where the URL really goes.

Number-based links

Companies like to use words, not numbers, in their domain name.

Avoid links that contain four sets of numbers separated by dots after the ://.

Scammers can use number-based URLs to hide malicious sites. If you don't know exactly where a number-based URL goes, do not click it.

Look-alikes

Attackers will deceive users by substituting letters and numbers to make a URL appear identical to a legitimate site. For example, 0 (the number) and O (the letter), l (lowercase L) and I (uppercase i), or vv (as w).

Here's an example of a look-alike:

www.gigarnartonline.com

www.gigamartonline.com

At first glance, these two domains look almost identical, making it easy to overlook the substitutions (rn for m).

Cabrini

Hyphens

Attackers often add hyphens to official brand domains, creating malicious links.

Note: Some legitimate sites use hyphens in their domain name, but don't click on the URL if it doesn't look like the one you know and trust.

Don’t Ignore the Domain

Carefully examining a URL can help you determine if the domain is a scam or legitimate. If you want to know where a URL really goes, look at the part of the URL after the **://** but before the first /. Read this part from right to left, starting at the first /.

http://perchaseonline.verifier-sure.com/myAccount/index.html

Read Between the Dots

http://essexhealthsystem.shandite.com

You can also start with the text to the right of the first dot after the ://—*shandite.com* is the true domain. It's the site you'd visit if you click on the link

What to Do Instead of Clicking

Only click on email links if you're expecting them (such as a product confirmation order).

If you trust the name of the organization who sent the email, type the URL you know and trust into your browser or use your bookmark. This way you can see if there's something that needs taking care of without the risk of navigating to a dangerous site.

Make hovering over links a habit. Rest your cursor over the link and read the URL that appears, but do not click the link.

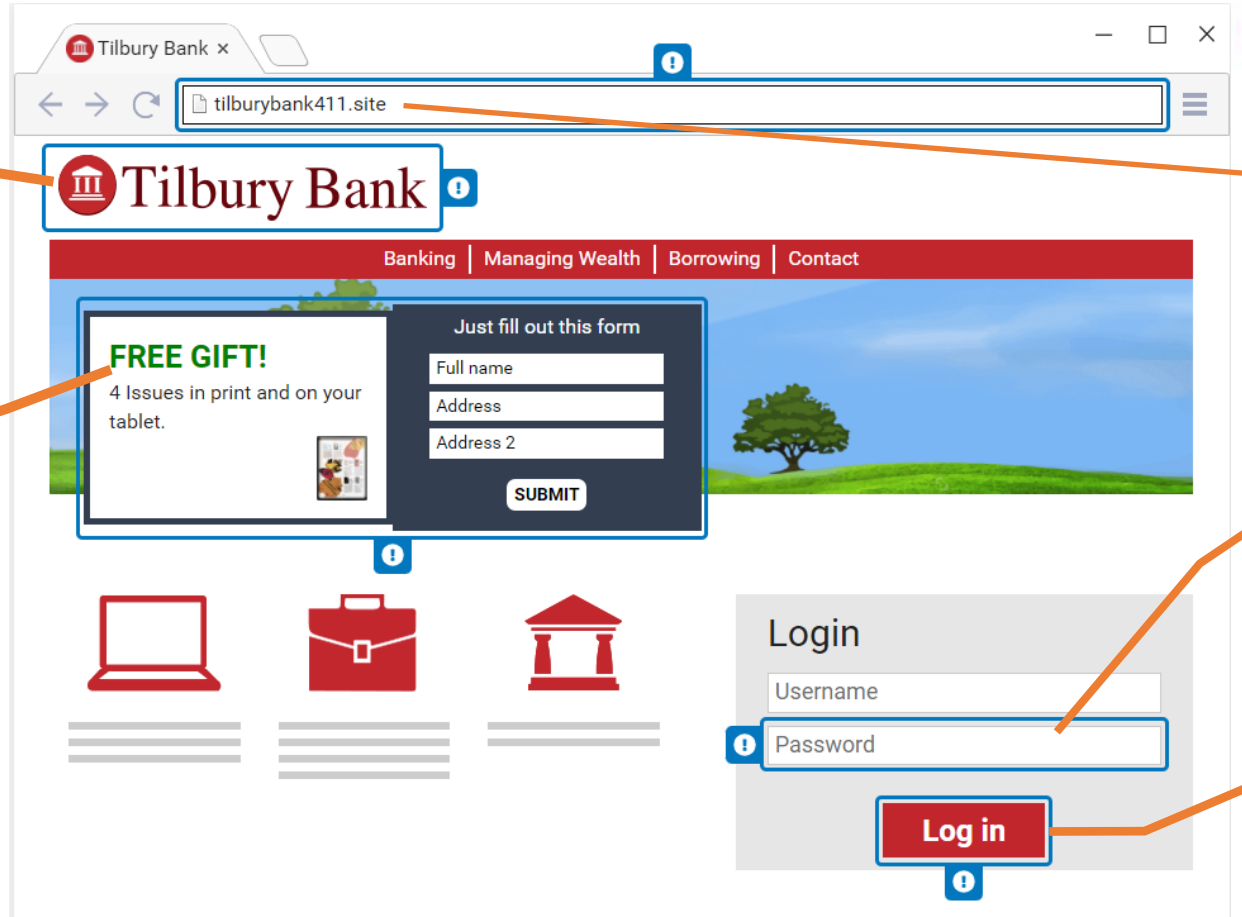
Use your favorite search engine to verify the site. When you search for a fraudulent domain, the top result's domain should match what you've entered.

What If I've Clicked the Link?

...and I think I'm on a dangerous website.

Don't interact with it until you verify the website is legitimate. Is this the website you expected?

Be cautious of pop-ups or error messages



Look for https or a lock symbol but beware if you receive a secure certificate warning

Do not enter any credentials or personal information.

If you still don't know, contact your security team..

Please complete the Declaration that you have read and understood the module.

End of module