

Tuesday TechTip:

Think before you click!

It's easy to click on a link, whether in an email or on a website, out of curiosity. Break this habit - keep your computer and personal information safe! Always pay close attention to the URL (Uniform Resource Locator; an address that specifies the location of a file on the Internet), more commonly known as the address. There are 3 parts to a URL:



After the `http://` (or `https://`) and before the first forward slash (`/`) is the **Domain**, the most important section in determining whether the URL points to the legitimate site or not.

1. *Before clicking on a link*, place your mouse over the link. The URL displays. Often in fake emails, the URL will be different than the named link. Check the URL to see if it is legitimate.
2. Don't trust URLs with all numbers in the domain name.
3. Don't let your eyes fool you. Often fake domain names are spelled exactly as the real domain, except for one single letter (or maybe two). For example:
 - a. VWesternunion.biz and b. Westernunion.biz

The first address (item a) is an example of a hoax, or fake, address. Notice that it's very hard to tell the difference. Item a is actually two capital V's (VV vs. W). Depending on the font it can be even more deceiving, remember social engineers can be quite sly, be aware!

4. Be familiar with legitimate URLs. For example: `http://www.ccis.edu/` is not the same as `http://www.ccis.org/` or `http://www.ccis.net/`
5. Don't be fooled by domains that contain the correct information, but then go beyond with additional information. Example fake domains may be `http://www.ccis.edu.com/eServices`, or `http://www.ccis.edu.eg/eServices`, etc. Notice the highlighted area is *not* part of the legitimate CCIS address.
6. In emails, look at the sender of the email and verify the sender's address is legitimate. Continue to scan the message for any fake URLs or suspicious statements asking for personal information. When in doubt, ignore and delete.

NOTE: Any URL collecting sensitive information like credit card numbers, social security numbers, user names, passwords, etc. *should start with the `https://` prefix*, if it doesn't, get away from it as far as possible. The 'S' after `https://` stands for Secure.