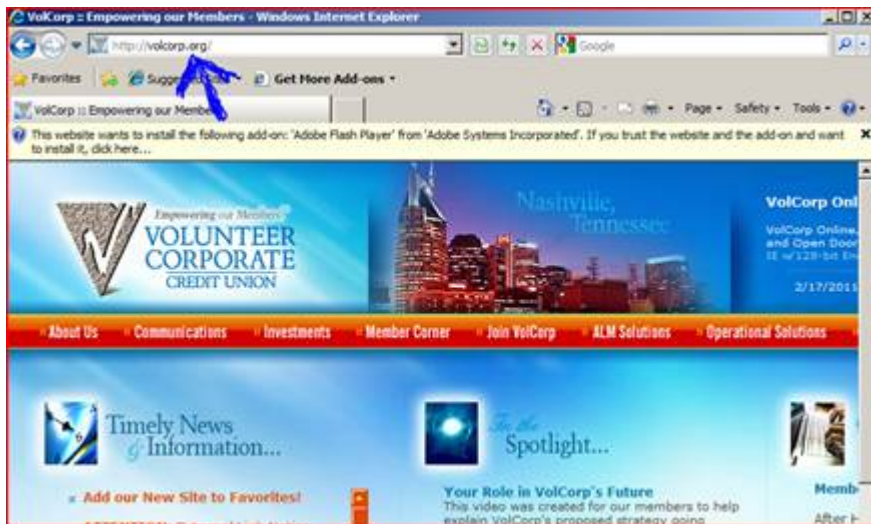


Security Awareness: A game of links

Have you ever noticed the address bar in your web browser? Do you think you can distinguish bad links from good links? Try this quiz to find out. For each question, try to identify the safer link. This will demonstrate some of the techniques that criminals use to trick people and some of the ways you can protect yourself. The answers are at the bottom of the page.

If you don't know where the address bar is, here is where to look:



Which link is safer?

- #1 A:
- B:
- #2 A:
- B: Volunteer Corporate Credit U...
- #3 A:
- B:
- #4 A:
- B:

- #5 A: <http://www.somebank.org/>
B: <http://www.somebank.org/login.php?user=jdoe&pass=s3cr3t>
- #6 A: <http://www.somebank.org/index.php?lang=%3c%73%63%72%69%70%74%3e%64%6f%63%75%66>
B: <http://www.somebank.org/index.php?page=main>
- #7 A: 
B:  <http://www.adobe.com/>
- #8 A: <http://www.somebank.org.bop.ru/>
B: <http://www.somebank.org/>
- #9 A: <http://www.google.com/>
B: <http://www.google.com/>

S
C
R
O
L
L

D
O
W
N

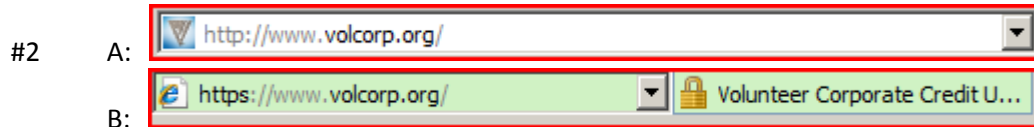
F
O
R

A
N
S
W
E
R
S

Answers



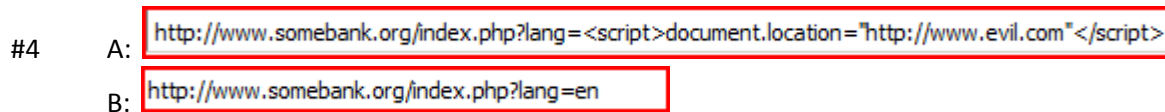
#1A is less dangerous. In example 1B, the letter “l” in Volcorp has been replaced with the number 1. Criminals will often register websites that closely resemble legitimate sites so they can trick the users.



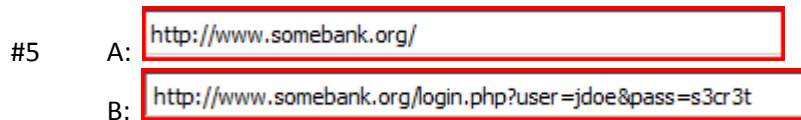
#2B is less dangerous. Both links go to the legitimate site but, example 2B uses https instead of http. The https means the connection between your computer and the web site is encrypted.



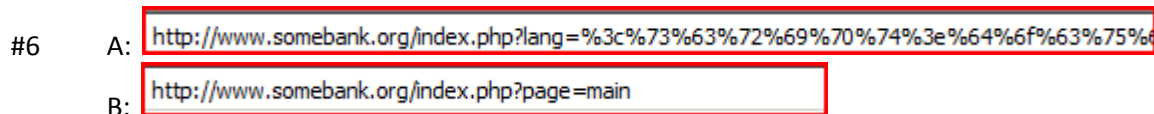
#3B is less dangerous. Both links include other web pages into the main web page. In 3B, the file is on the same server. In 3A, the file is from another (remote) website. Including remote pages is not always bad but, you should pay attention to what is being included. Keep in mind, the bad guys will probably not name their website “evil.com”




#4B is less dangerous. The example in 4A includes the “<script>” tag in the address bar. If you see this, there is a very good chance you have clicked on an evil link or the website has been compromised.



#5A is less dangerous. Example 5B is passing the username and password in the address bar. Your userid and password can be seen by the casual observer that sees your computer screen, or recorded in computer logs.



#6B is less dangerous. Example 6A is the same as example 4A but using encoding to hide the “<script>” tags. If you see numbers like this in the address bar, you should reconsider going to the site. This is not always “evil” but it has a high probability of being evil.

 Click here to install the following ActiveX control: 'Adobe Flash Player' from 'Adobe Systems Incorporated'...

#7

A:

B:  <http://www.adobe.com/>

#7B is less dangerous. If you go to a web site that says you need to upgrade the Flash Player, do not click the link on the website. The website could have been compromised. Instead, go directly to Adobe.com to upgrade the flash player.

#8

A: <http://www.somebank.org.bop.ru/>

B: <http://www.somebank.org/>

#8B is less dangerous. Web site names read from right to left, not left to right. Example 8B would be "Somebank" under the "org" domain. Example 8A would be the "BOP" domain under the "RU" (Russia) domain. [The word bop is Russian for "Thief"]

#9

A: <http://www.google.com/>

B: <http://www.google.com/>

#9 This is a trick question since both links are the same. Not seeing an obvious problem with the link is no guarantee the site is safe.