A friend of mine from another university was visiting recently and told me about a peculiar situation at work.

His institution is experiencing financial difficulties, so his department decided to reduce expenses by eliminating the extensive full-color brochure they had published for many years to entice students and parents into considering their program. Instead, they would publish a much simpler, less expensive brochure and put lots of exciting information on the departmental Website. This plan would also offer the opportunity for including links to each professor’s personal Web page, where the faculty could post valuable and impressive materials such as their curriculum vitae, list of publications, photos and so on.

Then he hit a brick wall.

The IT security officer at the university flatly disallowed all external links from the main departmental Web page. University policy precluded such links. “Why?” asked my friend. They would, said the security administrator, “compromise the security of the institutional Web site.” And that was it: end of discussion. The impression was that the security officer would have said, “Go away and stop bothering me” had my friend not been a faculty member.

My friend asked me about the security implications of having external links. Was it true, he asked, that they could allow an attack on the university’s Web site?

Well, no, not it the normal sense of the word “attack.”

Hyptertext transfer protocol (http) is a system for giving client systems (the computer running a browser) an address that can be translated into a numerical Internet Protocol (IP) address using the Domain Name System (DNS). An address in Hypertext Markup Language (HTML) is simply a string that is usually formatted in a particular way (e.g., underlined and in a particular color) according to the settings on the client system. As far as the Website is concerned, an HTML page that contains only Universal Resource Locators (URLs) is just a bunch of text.

Note that I am not discussing active content here; there are certainly ways to open holes in a Web site using URLs that are dynamically generated. For example, URLs that contain detailed that are interpreted by the Website as instructions or as user identification codes and authentication sequences can easily by abused from the outside. A specific example is some mailing list administrators’ (or spammers’) practice of giving members (or victims) URLs like this to remove themselves (or believe that they remove themselves) from the list:

http://www.something-or-other.domain/account=12345abc8910
People who are irritated by spammers have been known to generate lots of similar URLs and automatically cause mass removals from the lists using this vulnerability.

In the next article in this two-part sequence, I’ll discuss a related issue: links to embarrassing Web sites.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.