# Hiding Web Addresses – Instructions & Suggestions

Using the online tool below (TinyURL), it is possible to hide a given URL (Web address) by replacing it with a fake one. The suggested solution will produce the following results:

1. When users hover their mouse over the link in question they will see the fake rather than the true URL.
2. When users click on the fake URL they will be taken to the content of the true URL.

Similar results can also be accomplished by tools such as
FilesUp: http://www.filesup.info/ and
ShortURL: http://www.hashemian.com/tools/short-url.php
All these tools are concerned less with security and more with convenience (i.e. with providing users with short URLs to pages whose true URL may be inconveniently long).

## TINY URL: INSTRUCTIONS

The instructions assume you know how to enter any links on Blackboard, whether as a Menu button, an "External Link," or a link inside a Blackboard item's "Text" field. If this assumption is incorrect contact one of the instructional design consultants.

1. Go to http://tinyurl.com/
2. Enter the URL you want to hide into the field at the top of the page labeled: "Enter a long URL to make tiny"
3. Enter an optional short word in the field under the label "Custom alias." If you do not, the application will just include some random characters in your new link.
4. Click on the button labeled: "Make TinyURL!"
5. A new page will open with 3 new URLs in bold. The first is your original URL and the second is your new URL (the one you'll use in place of the one you want to hide)
6. Select (i.e. highlight by clicking and dragging your mouse over) this new URL and copy (Ctrl+C on a PC, apple+C on a MAC) and paste (Ctrl+V on a PC, apple+V on a MAC) it wherever you would have entered the original URL.

## CAVEATES

1) Tiny URL
   When using TinyURL, after users click on the "fake" URL they will be eventually taken to your original URL (after all, you want users to get to the final destination).
   When the final destination page opens, the address field of the user's browser will display the final destination URL. This means that, if someone wants to copy the real URL and distribute it they can do so from this window.

   Even if you were to use a special javascript code that forces the destination to open in a browser window that does not include an address field, users would still be able to distribute the fake URL, which may not be revealing the true destination but will eventually take users to that destination.

In short, the sender of an email has no (and cannot have any) control over what this email's recipients will do with the information received.

2) URL Encryption
After further investigation, it has become clear that URL encryption, whether provided through the website sent previously or through another similar service, requires programming on both the user (you) and the server (VoiceThread; Blackboard, etc.) ends. For an example on the type of programming required see a relevant paper by two University of Maryland Computer Science faculty members at http://www.cs.umd.edu/~vibha/10_sazawal_vibha.pdf.
Even if programming itself is not an issue, you will, in most cases, not have access to the server in question (e.g. VoiceThread server) and will therefore be unable to add the necessary encryption/de-encryption code to the server end.

**SUGGESTIONS**

1) Ask students to treat class information with confidentiality and trust that they will do so. This suggestion, similar to what Kelly proposed during Friday's workshop, may be the best way to go. After all, no matter what you do, you cannot stop students who want to do so from, say, i) copying and distributing the comments in a discussion forum or even ii) secretly recording a face-to-face class session and posting it on YouTube. You'll just have to trust that, if you explicitly ask them to maintain the class's confidentiality, students will respect your request.

2) Always use the embed code provided in the VoiceThread handouts to incorporate VoiceThread materials to your Blackboard sites. The problems with this approach are that i) you have little control over the default display size of the resource, which may be too small for many uses and ii) users with some html skill can recover the VoiceThread address in question within the embed code and distribute it as they wish.

3) Limit activities, for which security is a concern, to tools that are included with the Learning Management System (e.g. Blackboard) and therefore share the system's security features.

Until VoicetThread or any other similar system becomes an internal part of Blackboard or of any other secure Learning Management System, the reciprocity between flexibility and security will remain. In other words, tools (such as VoiceThread) that provide sophisticated multimedia features can be used best in contexts where trust can be assumed and/or security is not a major concern.