Securing Your Assessments

Excerpt from Section 9 of the Carnegie Mellon *Best Practices Guide for the Design and Development of SCORM Assessments*

Original Publication 07/31/2006

Bill Blackmon

whblackmon@gmail.com

Introduction

Many content developers are afraid that learners could look at the source code for assessments to determine the correct answers to test items. This quick tip provides a simple way to provide a measure of security for your assessments when they are delivered through a SCORM-compliant LMS.

The Problem

A SCO is typically composed of a set of static HTML and other files stored on a web server and delivered to a learner. A savvy learner may view the source for the HTML file and reverse-engineer your assessments to discover the correct answers.

Simple Security Measures

A simple way to secure your assessments is to put each assessment into another HTML file and store the name of the file as SCO launch_data. The name of the file will only be retrieved during the running of the SCO, and a learner will not be able to discover the name of the file by viewing the HTML source files.

In your content package, you specify the name of the file using the dataFromLMS field:

```
  <item identifier="ITEM-1"
identifierref="RES-1">
    <title>Sample Assessment</title>

<adlcp:dataFromLMS>hidden_assessment.html<
/adlcp:dataFromLMS>
  </item>
```

Then, when the learner is ready to take the test, the SCO gets the name of the file using the cmi.launch_data element:

```
  <frameset rows="*">
    <script language="javascript">
      var assessment_file = doGetValue(
"cmi.launch_data" );

      document.write( "<frame src=\""
        + assessment_file
        + "\" name=\"mainFrame\" />" );
    </script>
  </frameset>
```

Use this simple strategy to make your assessment SCOs secure so you will not have to re-create new assessments just because learners gained access to the answers.