



Cyber security training tools for the nuclear energy sector

Vu Pham ¹, Clifford Glantz, and Ying-Chen L Milbrath ²

1. Sacramento State University, 6000 J Street, Sacramento, CA 95819

2. Pacific Northwest National Laboratory, 902 Battelle Blvd, Richland, WA 99354



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Introduction

Cybersecurity is a critically important problem facing the nuclear and energy sector. A wide arrange of adversaries with varying attack tools threaten critical infrastructure. The **National Nuclear Security Administration (NNSA)** has tasked Pacific Northwest National Laboratory with developing eLearning modules for cybersecurity. The modules are designed to increase cybersecurity knowledge and awareness for nuclear facility decision makers, regulators, workers, and stakeholders. The modules are designed along the lines of a university curriculum. There are foundation course (100 level), and three more in-depth courses (200 – 400 level). This summer, I participated in the development of three 200 level courses that cover the subjects of cybersecurity threats, vulnerabilities, and consequences. I developed interactive educational products to reinforce presented information. This poster describes one of the products that I had developed.

Method

I used **Storyline 2™ software** to develop interactive educational products. Storyline allows a developer to insert graphics, sounds, and videos that make the course more interesting! In this poster I will present one useful product, named “Gearhead”.

Gearhead

Gearhead is a product that puts the user into the shoes of an attacker. It illustrates some of the steps they might take to acquire information on the control systems used at a hypothetical nuclear facility, *Plant Alpha*.

Gearhead

In the start of Gearhead, the learner is given their assignment.

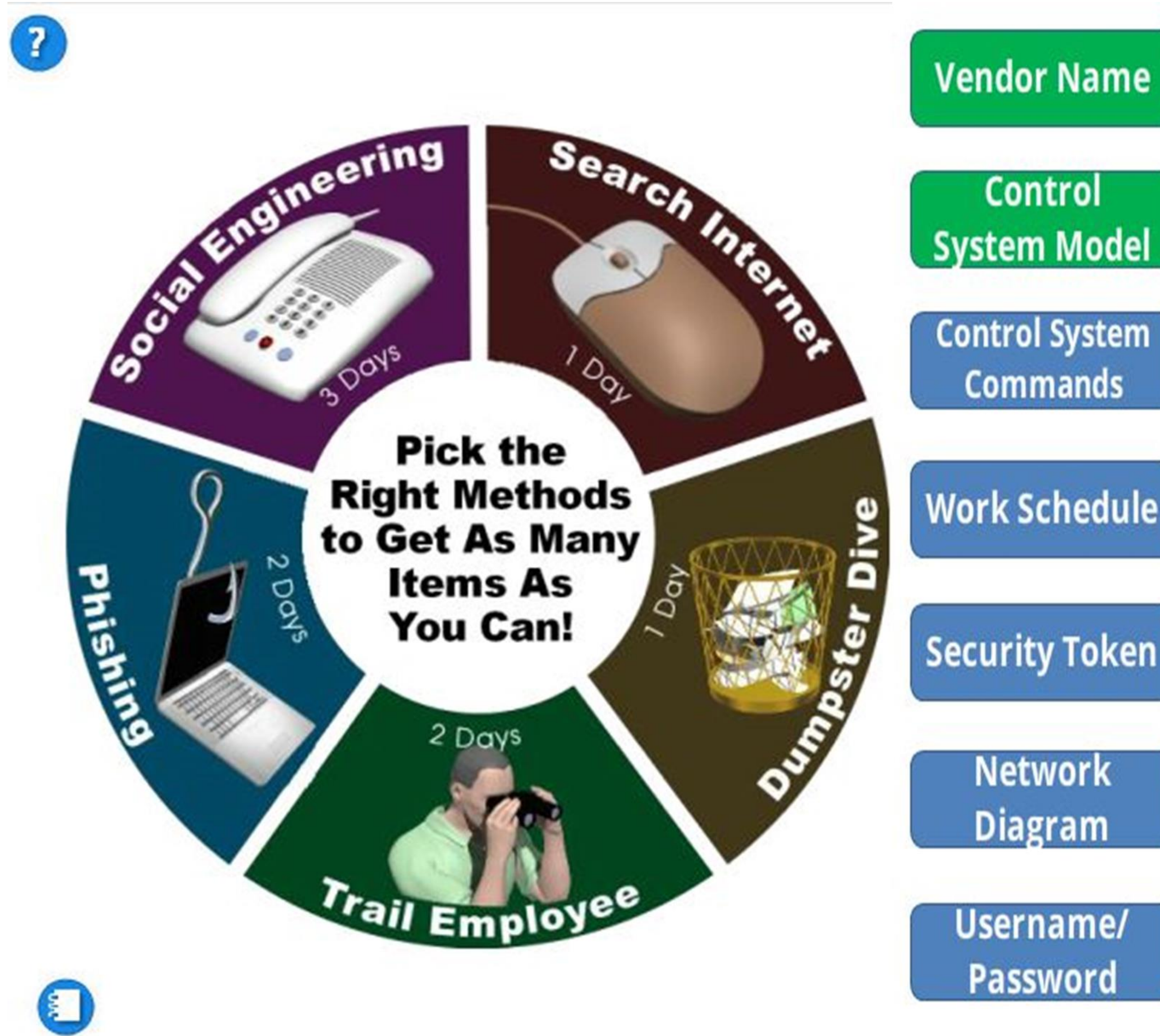
“Here’s a list of the information and products we could use to break into Plant Alpha and install malware. Our programmers will design that malware to cause the facility to shut down when the time is right and we issue our commands.”



You must obtain at least 5 of these items about Plant Alpha:

1. Vendor Name
2. Control System Model
3. Control System Commands
4. Work Schedule
5. Security Token
6. Network Diagram
7. Username/ Password

The learner has the choice to explore many different paths to complete their assignment; giving them control over their learning experience.



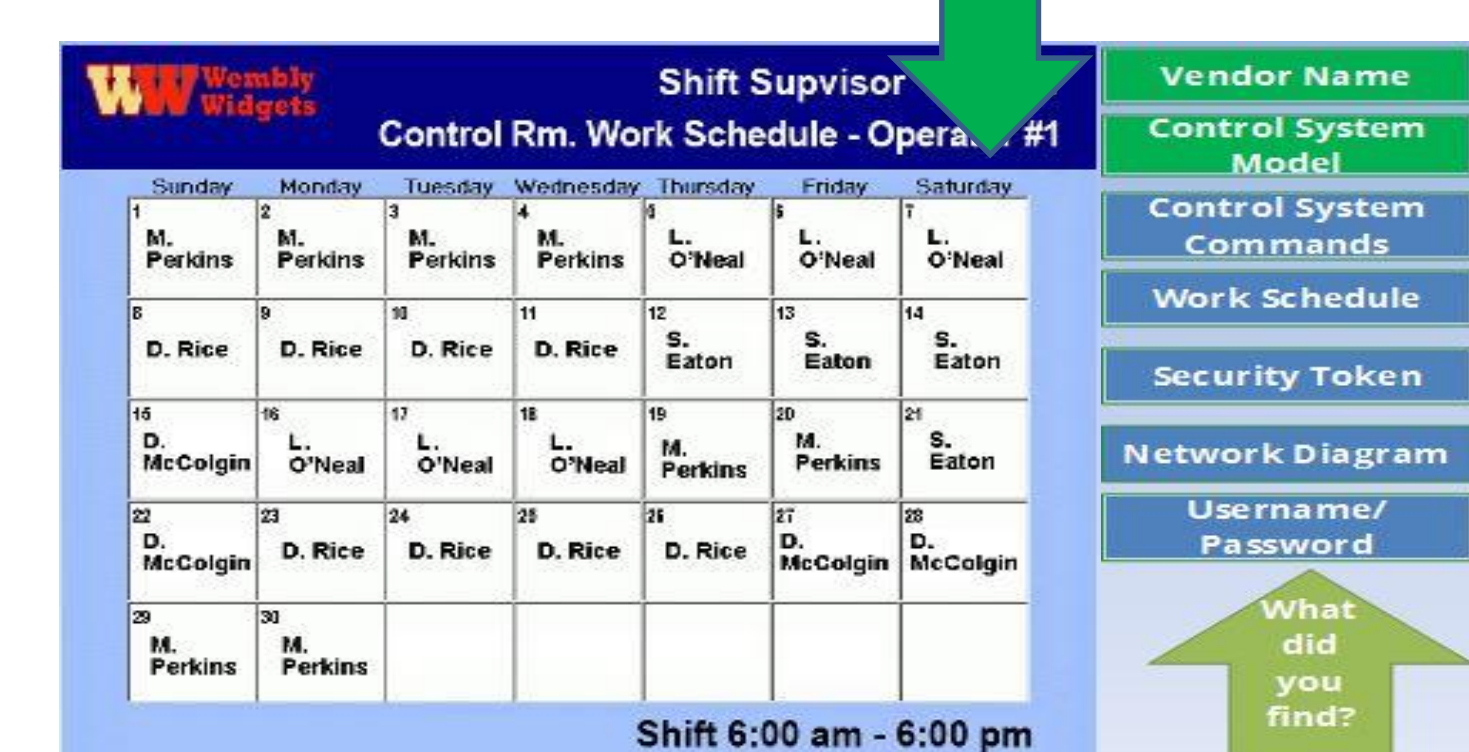
In this example, the learner takes on the assignment to “dumpster dive” at a Plant Alpha staff member’s home and outside the Plant Alpha office building to acquire potentially useful information. Just as the name applies, “dumpster dive” refers to searching a garbage bin for discarded information that could be useful to the attacker.

Gearhead

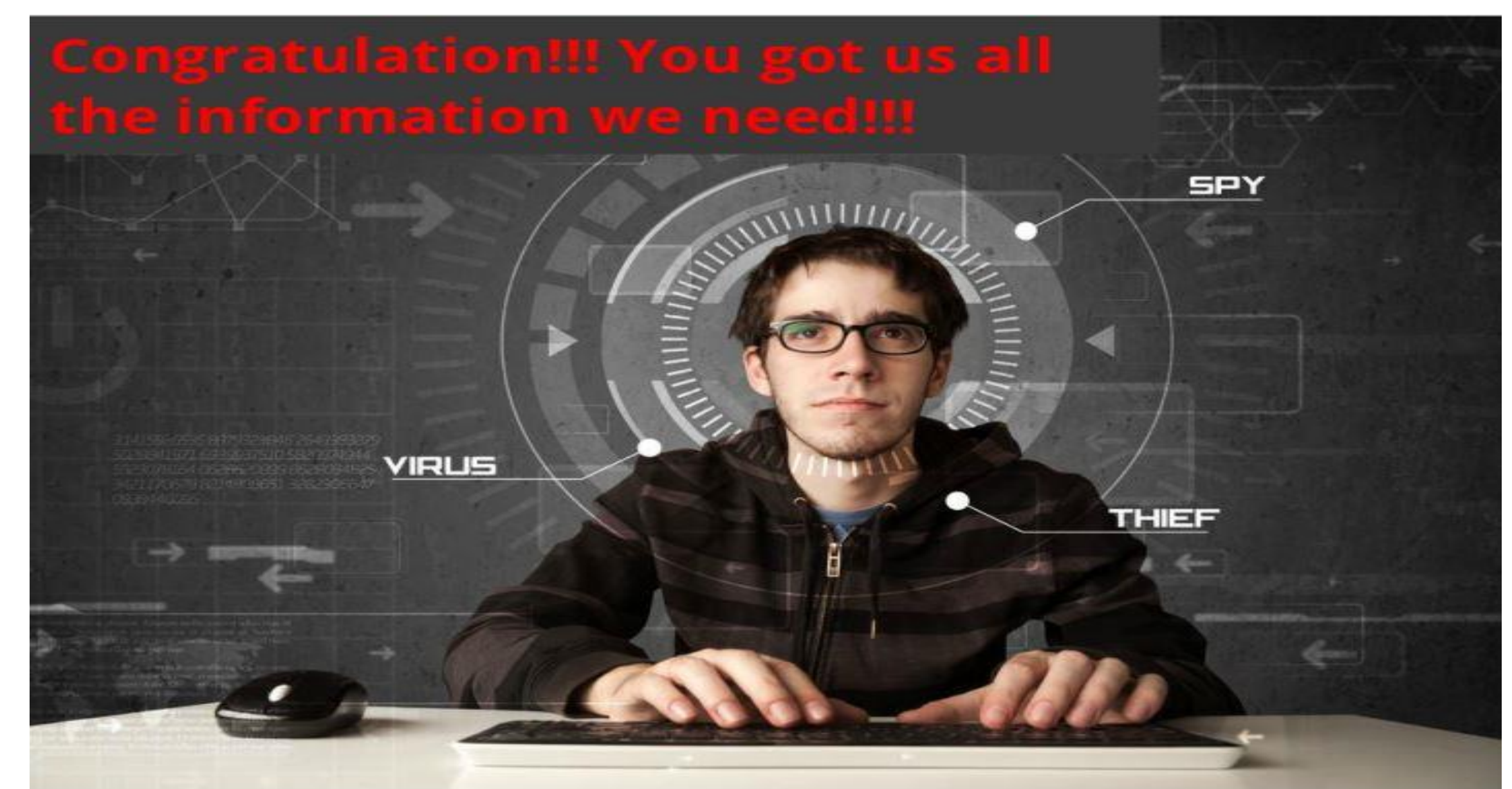


Engineering Home Plant Alpha

Click on Engineering’s Home and Plant Alpha to complete this activity! When you finish both of them, click “Next” to move on!



If the learners acquires all the items needed to mount a successful cyber attack, they are congratulated for their accomplishment.



Conclusions

Storyline 2 is an effective tool for inserting interactive exercises in eLearning modules. Interactive exercises maintain learner attention and reinforce learning during remote training.

ABOUT

Pacific Northwest
National Laboratory

The Pacific Northwest National Laboratory, is a U.S. department of Energy Office of Science laboratory that solves complex problems in energy, national security, and the environment, and advances scientific frontiers in the chemical, biological, materials, environmental, and computational sciences. The Laboratory employs nearly 5,000 staff members, has an annual budget in excess of \$1 billion, and has been managed by Ohio-based Battelle since 1965.

For more information on the science you see here, please contact:

Clifford Glantz
Pacific Northwest National Laboratory
P.O. Box 999, MSIN: K9-30
Richland, WA 99352
(509) 375-2166
cliff.glantz@pnnl.gov