Effective Computer Security Training Cheat Sheet

by [deleted] via cheatography.com/2754/cs/8953/

Introduction

One fundamental problem is that most awareness programs are created and run by security professionals, people who were not hired or trained to be educators. These training sessions often consist of long lectures and boring slides—with no thought or research put into what material should be taught and how to teach it. As a result, organizations are not getting their desired results and there's no overall progress.

To solve this puzzle, it's important to step back and understand how people most effectively learn subject matter of any type.

From start to finish, inside a PayPal Phishing scam

The science of learning dates back to the early 1950s, and its techniques have been proven over time and adopted as accepted learning principles. Applied to information security training, these techniques can provide immediate, tangible, long-term results in educating employees and improving your company's overall security posture.

Creidt: http://www.csoonline.com/article/2131688/security-awareness/ten-commandments-for-effective-security-training.html

1. Serve small bites

People learn better when they can focus on small pieces of information that the mind can digest easily. It's unreasonable to cover 55 different topics in 15 minutes of security training and expect someone to remember it all and then change their behavior.

Short bursts of training are always more effective.

2. Reinforce lessons

People learn by repeating elements over time—without frequent feedback and opportunities for practice, even well-learned abilities go away. Security training should be an ongoing event, not a one-off seminar.

3. Train in context

People tend to remember context more than content. In security training, it's important to present lessons in the same context as the one in which the person is most likely to be attacked.

4. Vary the message

Concepts are best learned when they are encountered in many contexts and expressed in different ways. Security training that presents a concept to a user multiple times and in different phrasing makes the trainee more likely to relate it to past experiences and forge new connections.

5. Involve your students

It's obvious that when we are actively involved in the learning process, we remember things better. If a trainee can practice identifying phishing schemes and creating good passwords, improvement can be dramatic.

Sadly, hands-on learning still takes a backseat to old-school instructional models, including the dreaded lecture.

6. Give immediate feedback

If you've ever played sports, it's easy to understand this one. "Calling it at the point of the foul" creates teachable moments and greatly increases their impact. If a user falls for a company-generated attack and gets training on the spot, it's highly unlikely they'll fall for that trick again.

7. Tell a story

When people are introduced to characters and narrative development, they often form subtle emotional ties to the material that helps keep them engaged. Rather than listing facts and data, use storytelling techniques.

8. Make them think

People need an opportunity to evaluate and process their performance before they can improve. Security awareness training should challenge people to examine the information presented, question its validity, and draw their own conclusions.

9. Let them set the pace

It may sound cliche, but everyone really does learn at their own pace. A one-size-fits-all security training program is doomed to fail because it does not allow users to progress at the best speed for them.

10. Offer conceptual & procedural knowledge

Conceptual knowledge provides the big picture and lets a person apply techniques to solve a problem. Procedural knowledge focuses on the specific actions required to solve the problem.

Combining the two types of knowledge greatly enhances users' understanding. For example, a user may need a procedural lesson to understand that an IP address included in a URL is an indication that they are seeing a phishing URL. However, they also need the conceptual understanding of all the parts of a URL to understand the difference between an IP address and a domain name, otherwise they may mistake something like www4.google.com for a phishing URL.