Teaching Security Lesson 2: Authentication

Activity: Building Strong Passwords

Part 1: Choosing New Passwords

Websites will sometimes require that new passwords meet certain requirements. Some websites just set a minimum length, but others have many requirements. For example, Chase Bank requires that new passwords meet these requirements:

✓ Must be 8-32 characters long
✓ Must include at least two of the following elements:
  o At least one letter (upper or lowercase)
  o At least one number
  o At least one special character from the following: # $ % ’ ^ , ( ) * + . : ! = ? @ / ] \ _ ; { } ~
✓ Must be different than your previous five Passwords
✓ Must not match your User ID
✓ Must not use the name of the financial institution (for example: JPM, MORGAN, CHASE)
✓ Must not be a commonly used password (for example: password1)

1. Why does Chase require that passwords be at least 8 characters long? Why are longer passwords better?

2. Why does Chase require that the password have at least one letter, one number, and one special character?

3. Make up 5 new passwords that meet the requirements and write them in the first column on page 2. (Then come back here for Question 4!)

4. Make up a password that meets these requirements but would still be easy for someone to guess. (For example: Think of one that someone who knows a little bit about you could guess.)
Part 2: Measuring Password Strength

What does it mean for a password to be “strong”? The requirements from Part 1 are designed to prevent you from choosing a weak password. Some websites also have a “password meter” to tell you how strong your password is before you submit it.

A. Go to this website: https://cups.cs.cmu.edu/meter/
B. Check the box to “Show Password”
C. Carefully type each password from Column 1 into the password field and complete Columns 2 and 3

<table>
<thead>
<tr>
<th>Password (Part 1)</th>
<th>What color was the bar? (e.g. gray, red, dark green)</th>
<th>What was the detailed feedback?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Part 3: Passing It On

In 2-3 sentences, what advice would you give to someone about choosing a password?