How to Create Strong Passwords That You Don’t Need to Memorize
No agenda or lecture
This will be an exercise
I will help you create a personal strategy
Strong passwords will be an outcome of this strategy
Memory is intrinsic to humans
Repetition and reference assist memory
The variables in this strategy are unique to you
You have a leg up on the process if you know words from a language other than English 😊
Tools needed for this exercise

- A Pen
- Paper
- Your creativity
Let’s assume that you want to create a strong password for a grocery store website.

Step 1: Pick the name of a grocery store you visit
   Safeway

Step 2: Reverse the name
   Yawefas

Step 3: After the first letter, insert a ‘!’
   Y!awefas

Step 4: Substitute letters, be unconventional. Say my ‘w’s are always the number ‘4’
   Y!a4efas

Step 5: Add a nonsensical phrase or combination of letters
   Y!a4efas tral
Let’s try it again with another website or provider’s page

Step 1: Pick the name of a pharmacy’s website that you visit
Walgreens

Step 2: Reverse the name
Sneerglaw

Step 3: After the first letter, insert a ‘!’
S!neerglaw

Step 4: Substitute letters, be unconventional. Say my ‘w’s are always the number ‘4’
S!neergla4

Step 5: Add a nonsensical phrase or combination of letters
S!neergla4tral
Some more examples

Lyrics:
Promisemeson
P!r3m3s3m3s3n

Poems:
Ihavepromisestokeep
I!h2v2pr2m2s2st2k22p

Phrases:
Mansionyogurtgold
M!nsi2ny2gurtg2Id
Strong passwords help in these 3 instances

- **Dictionary** – scripts that go down the list of words in the dictionary
- **Brute force** – scripts that try different combinations
- **Guessing or Inferring** – deducing from bits of information about the person or just guessing

**People-Process-Technology**
Some more tips and tricks

- Use songs, phrases, substitutions
- Passwords made up of word combinations, phrases in a language other than English (for example: ‘chardinkichandani’ is a combination of 4 words in Hindi and not easy to guess or broken by using a script)
- Your password retrieval email account should be non-descript (not related to your name or identity)
- Whenever possible, use two-step authentication (such as your bank uses)
- Use two-factor authentication (for example: An RSA token) whenever possible
- Your challenge question responses don’t need to be truthful
- Close accounts that you don’t use
- Change your passwords once every quarter and change the ‘key’.
- Never use your browser to save passwords or write them down
- If your account is compromised, notify the IT Support Center (or appropriate tech support) immediately and reset the password/s unless otherwise directed by the law enforcement
- www.ShouldIChangeMyPassword.com
- Putting your Password to the Test at http://www.passwordmeter.com
- If a breach occurs, do not try to do damage control by yourself. Reach out to the GW IT Support Center at 202-994-4948 and/or the GW University Police Department
If your password looks like one of these, please change it

**SplashData**’s Worst Passwords of 2012

<table>
<thead>
<tr>
<th>#</th>
<th>Password</th>
<th>Change from 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>password</td>
<td>Unchanged</td>
</tr>
<tr>
<td>2</td>
<td>123456</td>
<td>Unchanged</td>
</tr>
<tr>
<td>3</td>
<td>12345678</td>
<td>Unchanged</td>
</tr>
<tr>
<td>4</td>
<td>abc123</td>
<td>Up 1</td>
</tr>
<tr>
<td>5</td>
<td>qwerty</td>
<td>Down 1</td>
</tr>
<tr>
<td>6</td>
<td>monkey</td>
<td>Unchanged</td>
</tr>
<tr>
<td>7</td>
<td>letmein</td>
<td>Up 1</td>
</tr>
<tr>
<td>8</td>
<td>dragon</td>
<td>Up 2</td>
</tr>
<tr>
<td>9</td>
<td>111111</td>
<td>Up 3</td>
</tr>
<tr>
<td>10</td>
<td>baseball</td>
<td>Up 1</td>
</tr>
<tr>
<td>11</td>
<td>iloveyou</td>
<td>Up 2</td>
</tr>
<tr>
<td>12</td>
<td>trustno1</td>
<td>Down 3</td>
</tr>
<tr>
<td>13</td>
<td>1234567</td>
<td>Down 6</td>
</tr>
<tr>
<td>14</td>
<td>sunshine</td>
<td>Up 1</td>
</tr>
<tr>
<td>15</td>
<td>master</td>
<td>Down 1</td>
</tr>
<tr>
<td>16</td>
<td>123123</td>
<td>Up 4</td>
</tr>
<tr>
<td>17</td>
<td>welcome</td>
<td>New</td>
</tr>
<tr>
<td>18</td>
<td>shadow</td>
<td>Up 1</td>
</tr>
<tr>
<td>19</td>
<td>ashley</td>
<td>Down 3</td>
</tr>
<tr>
<td>20</td>
<td>football</td>
<td>Up 5</td>
</tr>
<tr>
<td>21</td>
<td>jesus</td>
<td>New</td>
</tr>
<tr>
<td>22</td>
<td>michael</td>
<td>Up 2</td>
</tr>
<tr>
<td>23</td>
<td>ninja</td>
<td>New</td>
</tr>
<tr>
<td>24</td>
<td>mustang</td>
<td>New</td>
</tr>
<tr>
<td>25</td>
<td>password1</td>
<td>New</td>
</tr>
</tbody>
</table>
Questions?

Presented by:

Noor Arohi
Senior Analyst - Risk and Compliance
GWIT Information Security and Compliance Services
infosec@gwu.edu
703-726-3664