# Activities/ Resources for Outcomes

## Password Scenarios

**Scenario 1**:

Password: brian12kate5

"I doubt anyone could guess my password! It's my kids' names and ages. Who else would know that?"

Problem:

Solution:

.

**Scenario 2**

Password: w3St!

"My password is so simple! It's just the beginning of my street address with a few extra characters."

Problem:

Solution:

**Scenario 3**

Password: 123abccba321

"My password follows a simple pattern, so it's easy to remember and type on my keyboard."

Problem:

Solution:

**Scenario 4:**

Password: BrAveZ!2

"I use the same passwords for all my accounts. This way, I only have to remember one password!"

Problem:

Solution:

## Password Scenarios and Solutions

**Scenario 1**:

Password: brian12kate5

"I doubt anyone could guess my password! It's my kids' names and ages. Who else would know that?"

Problem:

Solution:

**Problem:** This password uses too much personal information, along with common words that could be found in the dictionary.

**Solution**: A stronger version of this password would use symbols, uppercase letters, and a more random order. And rather than using family names, we could combine a character from a movie with a type of food. For example, Chewbacca and pizza could become chEwbAccAp!ZZa.

**Scenario 2**

Password: w3St!

"My password is so simple! It's just the beginning of my street address with a few extra characters."

Problem:

Solution:

**Problem**: At only five characters, this password is way too short. It also includes part of her address, which is publicly available information.

**Solution**: A stronger version of this password would be **much longer**, ideally more than 10 characters. We could also substitute a nearby street name instead of her current address. For example, Pemberly Ave could become **p3MberLY%Av**.

**Scenario 3**

Password: 123abccba321

"My password follows a simple pattern, so it's easy to remember and type on my keyboard."

Problem:

Solution:

**Problem:** While patterns like this are easy to remember, they're also some of the first things a hacker might guess when attempting to access your account.

**Solution:** Remember that random passwords are much stronger than simple patterns. If you're having trouble creating a new password, try using **a password generator** instead. Here's an example of a generated password: #eV$pIg&qf

NOTE: If you use a password generator, you may also want to create a **mnemonic device** to make the password easier to remember. For example, **H=jNp2#** could be remembered as **HARRY = jessica NORTH paris 2 #**. This may still feel pretty random, but with a bit of practice it becomes relatively easy to memorize.

**Scenario 4:**

Password: BrAveZ!2
"I use the same passwords for all my accounts. This way, I only have to remember one password!"

Problem:

Solution:

**Problem**: There's nothing really wrong with this password, but remember that you should never use the same password with different accounts.

**Solution**: Create a unique password for each of your online accounts.

# Filling in Your Footprint

**Individual Brainstorm**:
On the flip side of this page, fill in the outline of a footprint with some information about you that is available on the Internet (for example, name, address, friends you're connected to).

- If a particular piece of information is easily accessible to many other people online (in other words, very exposed), write it in bigger letters.
- If a piece of information is accessible to relatively few people, write it in smaller letters.

**Group Discussion**:
When the time is up, discuss the following questions with your group:

1. What are some similarities/differences between the footprints of the different people in the group?

2. Which of the items listed could be used to uniquely identify you? Which combinations of items could be used?

3. Are there any items you listed that you wish weren't available online? (In other words, that you wish weren't part of your information footprint?)

4. What could you do to reduce the exposure of some items in your footprint?