CYBERSECURITY

Creating Strong Passwords

Passwords play an foundational role in people's digital lives. A common mistake people make is using short, easily remembered passwords, which are likely to cause data breaches and identity theft. ***Strong passwords*** are essential to **protecting personal information and identity**.

1 Avoid using personal information

Most personal information can be easily retrieved from Internet searches or social media sites. AVOID:

- Name
- Phone Numbers
- Family Member' Names
- Dates of Birth
- Common Usernames
- Documented Hobbies

2 Use a long password

A password should have at least 8 to 10 characters, but 16 to 20 characters is ideal.

- Numbers
- Symbols
- Uppercase & Lowercase Letters

Use a combination of numbers, symbols, and case letters.

Beyonce123

gina14michelle3

n0rTh!

Favorite celebrity and consecutive numbers

Using family members' names and ages

Using a street name or favorite locations

To create stronger passwords, mix up the numbers, symbols, and case letters. EX. d35tiny&c4i1d

3 Avoid reusing passwords and using patterns

Strong passwords should be used, but don't repeatedly use the same passwords.

- Avoid consecutive letters (ex. abc)
- Avoid consecutive numbers (ex. 123)
- Avoid using the same password for different accounts

Password Generators

Use a password generator to create strong passwords with letters, mixed case, punctuation, and numbers to avoid identity theft.

****

Password Managers

Use a password manager to generate and/or keep track of passwords in a secured location.

****

References:

- GCF Global. (n.d.). Creating strong passwords. https://edu.gcfglobal.org/en/techsavvy/password-tips/1/
- Security. org. (n.d.). *How secure is my password?*. https://www.security.org/how-secure-is-my-password/

PURDUE UNIVERSITY | College of Education

Project TIME — Teaching Innovations in Multimodal Education, a GEER grant initiative of Learning Design & Technology