SOCIAL ENGINEERING is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
(Google definition)

These hackers try to learn enough about you to make educated guesses about your passwords, pins, and security questions. To counter these types of attacks:

- Do not open attachments or links from untrusted sources.
- Do not trust strangers with your personal information or your devices.
- Lock your laptop/computer.
- Use anti-virus software.
- Never email or text your credit card information, social security number, or bank account number to anyone.

Want to learn more about digital privacy?

Introduce yourself to the Library Freedom Project at https://libraryfreedomproject.org/resources-01/privacytoolkit/

Read up on identity theft at https://www.consumer.ftc.gov/topics/privacy-identity-online-security (website also available in Spanish)

Watch a TED talk on Internet security, https://www.taylordigital.com/blog/5-ted-talks-internet-security/

Ask a reference librarian at LBCC library!

Linn Benton Community College Library

https://library.linnbenton.edu/home
Phone: 541-917-4638
Email: libref@linnbenton.edu

Psst . . . Can we talk about passwords?

A quick checkup

Test your email
https://
haveibeenpwned.com

At this website you can enter an email address and see a list of all known data breaches tied to that email address.

You can also sign up for a "Notify Me" service so that you will be notified about future breaches.

Password security basics

Create a strong password
—use at least 12 characters
—include numbers, symbols, caps, and lower-case letters
—avoid dictionary words
—avoid anything obvious about you (your dog's name, your birthday, etc.)
—substitute numbers for certain letters
—remember that default passwords are NEVER secure

Use different passwords for different accounts
—make even different passwords easy to remember by using the same core password and just adding three letters at the end or beginning depending on the website, ie add AmA for amazon.com, add FB for Facebook

Change passwords on a regular basis
—add the date of change at the end or beginning _02_18

Password generators
Lastpass.com

Password managers
A place to store your passwords online by using a single master password. This allows you to use many different passwords for different sites without having to memorize all of them. One free password manager is Dashlane,
https://www.dashlane.com/

Keep passwords private

Change passwords after a major life change

Check password strength
howsecureismypassword.net

Be careful with public computers and public wi-fi

Two-factor authentication