3 Everyday Ways to Practice Information Security:

1) **Utilize Multifactor Authentication.**
   This security control is offered on nearly every platform you interact with and is extremely effective at keeping your information confidential. Even though it may not be required for your account on certain platforms, it is best practice to "go the extra mile" and enable MFA. This simple feature allows for your password to be compromised and still maintain confidentiality and integrity of your data. Major information breaches occur regularly and most of those are outside of your control. Using MFA allows you to take back control, since you are the only person able to authenticate by providing the second factor information at that moment.

   Additional resources:
   Multifactor Authentication, CISA

2) **Update your software regularly.**
   In 2022, over 26,000 new IT security vulnerabilities and exposures (CVEs) were reported. Many of these vulnerabilities were mitigated by applying software patches. Some ways to ensure you are up to date with the latest patches are setting your software or devices to automatically apply the latest software releases. If that is not an option, then utilize your software's built-in feature that can check for updates and perform this task at least monthly. Don't forget to include your phones and tablets as well! Taking a few minutes to update your devices can prevent major incidents that last days or months from occurring.

   Additional resources:
   CISA Known Vulnerabilities Catalog

3) **Know WHO you are communicating with in emails.**
   Phishing attempts and impersonations are the most common tactics used by malicious actors. A simple way to defeat many of these attempts is to check who sent you an email or who is being replied to with your information.
   For example, when you send and receive an email, you have email addresses displayed in the "To / From" lines that show an abbreviation of email addresses. Clicking on this abbreviation may reveal that the "sender" or "recipient" is not who you believed it to be or reveal that there is a fraudulent address impersonating someone legitimate after closely examining the email address.
   You are looking for misspelled words, names, or additional characters to make the address look similar in the abbreviated form. A quick check on who you are communicating with can help identify and report malicious actors while saving you from any harm.