INFORMATION SECURITY TRAINING COURSE

---------- WEEK 5 REFERENCE SHEET: Social Media ----------

-

MAIN IDEAS	NOTES
Social Media Threats	Two of the big threats to you via social media: • Clickjacking • Social Engineering Social Media has made the world a more connected place. All those connections also create unprecedented access to people's and business' information
What is Clickjacking?	Clickjacking is an attack method, also known as User Interface Redressing, because it is set up by disguising (or redressing) a link with an overlay that tricks the user into doing something different than he or she thinks.
What is Social Engineering?	Social engineering is the art of manipulating people so that they give up confidential information. Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software
BEST PRACTICES	
Social Media Security Best Practices	1. Shutdown unattended social median accounts 2. Protect your passwords • Avoid using personal information such as date of birth, pet's name, child's name, etc. as login passwords. • Don't use the weak password. If you can't remember the complex one, then use a password manager. • Begin using **2 Factor Authentication**. 3. Turn on login alerts • If you enable this feature, you will be notified by e-mail if your account is accessed from a new device and/or location. 4. Protect your computer and smartphone with strong, up-to-date security software
2FACTOR AUTHERNTICATION	
What is 2 factor authentication?	2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information.
Second factor could come from one of the following categories:	Something you know: This could be a personal identification number (PIN), a password, answers to "secret questions" or a specific keystroke pattern. Something you have: Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token. Something you are: This category is a little more advanced, and might include biometric pattern of a fingerprint, an iris scan, or a voice print.