

FISSA+ Privacy & Records Management

Module 6: Staying Safe Online Best Practices

1	Always maintain physical control of your mobile device and be aware of the possibility of your device being snatched out of your hands.
2	It is employees' responsibility to ensure that all of their files and folders have security configurations in place so that only appropriate individuals have access to sensitive information (such as Personally Identifiable Information) stored in their Drive area.
3	Disable WiFi, infrared and Bluetooth when not in use.
4	Use caution when using free charging services for your mobile device.
5	Even legitimate websites can have malware. Think before you click!
6	Configure your mobile device to only use trusted (known) wireless networks, and prompt or ignore when in range of unknown wireless networks.
7	Posts and profiles can be embarrassing, or provide the necessary information for hackers to hijack accounts. Think before you post!
8	If accessing links sent in emails or on websites, verify that the URL for the link is the same as what you think.
9	Use DOI approved cloud storage locations, (currently only Google Drive).
10	Immediately report the loss or potential loss or theft of computers, devices, or any type of media containing sensitive agency information/data (including any Personally Identifiable Information - PII).
11	Wireless networks and devices should be implemented in DOI only with the explicit approval of the executive management of the affected bureau/office and at the Department level.
12	Always be careful about clicking links or attachments in emails, or if you are prompted to log into the same app twice in a single session.