Tips for Avoiding Being a Social Engineering Victim

# Consider the source

* That USB stick you just found might contain malware.
* That text or email from your bank could be spoofed and not from your bank at all.
* Be suspicious of links and attachments.

# Slow down

* Social Engineers want you to act without questioning or thinking.
* It might be a scammer behind that email, phone call or face-to-face request.
* Take time to question if something is fishy.

# If it sounds too good to be true

* How likely is it that you are some lost relative of a prince or earl?
* If your cousin, nephew or grandchild is requesting money, it most likely is a scam.

# Install antivirus or a security suite

* Keep your security software up to date.
* Make sure you have the latest operating system software running on all your devices.
* Keep operating system updated

# Use your email software to filter out junk mail

* Let your spam filters work for you – set it to high to weed out as much junk as possible.

Social engineering is everywhere, online and offline. Your best defense against these kinds of attacks is to educate yourself so that you are aware of the risks — and to stay alert.