



Telework IT Security Guide

Practice	Do 	Don't 
Wi-fi & Public Networks	<ul style="list-style-type: none"> Secure your home network with a strong password or passphrase Use passwords for all devices on your network 	<ul style="list-style-type: none"> Use public or unsecured networks Allow unknown devices to access your network
Personal Use	<ul style="list-style-type: none"> Keep work data on work devices only 	<ul style="list-style-type: none"> Use work devices for personal use Allow non-employees to use work devices (even for simple tasks)
Physical Security	<ul style="list-style-type: none"> Secure devices with a strong password or passphrase Lock devices while unattended Always know the location of your device Be aware of your surroundings; e.g. can someone see your screen over your shoulder or through a window? 	<ul style="list-style-type: none"> Write down passwords Leave your device in a vehicle unless necessary Leave hard copy documents unattended or in plain sight
Data	<ul style="list-style-type: none"> Follow all record management policies Save data to OneDrive or a commonwealth network shared drive Close unused files and applications before sharing your screen in meetings 	<ul style="list-style-type: none"> Not use a thumb drive or personal storage device to store work data Save data on your hard drive or desktop
Social Media	<ul style="list-style-type: none"> Follow all agency and commonwealth guidelines on social media Be aware of misinformation 	<ul style="list-style-type: none"> Share or allow access to personal information such as birthdays, addresses or phone numbers
Reporting	<ul style="list-style-type: none"> Report suspicious activities to: OA-SecurityIncidents@pa.gov Report phishing emails to: CWOPA_Spam@pa.gov 	<ul style="list-style-type: none"> Open potential spam or phishing emails Assume someone else has reported a phishing email