

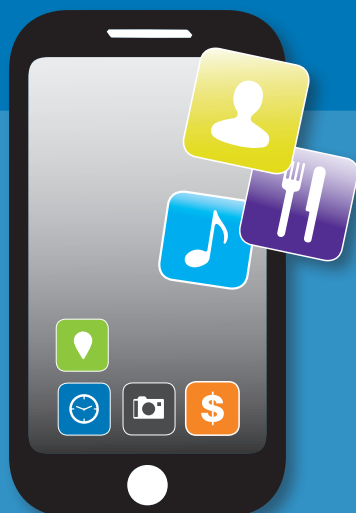


CYBER SECURITY IS OUR SHARED RESPONSIBILITY

PROTECT YOUR SMART PHONE

✓ DO'S

- Make sure the OS and software are up to date at all times
- Download apps from reputable sites and closely review permission requests
- Make sure to check the feedback from other users before installing the program from an app store
- Use a strong, complex password
- Use a security app, if available for your device
- Turn off Bluetooth and other connections when not in use



✗ DON'TS

- Jailbreak your phone
- Download apps from third-party app stores and sites
- Leave your mobile device unattended in public places
- Enable your "Wi-Fi ad-hoc mode"



CYBER SECURITY IS OUR SHARED RESPONSIBILITY

USE SECURE PASSWORDS



**KEEP YOUR PASSWORD SAFE BY FOLLOWING
THESE EASY TIPS:**

DEVELOP strong passwords that use a combination of words, numbers, symbols, and both upper- and lower-case letters

CREATE a password phrase and make it relevant. If you're joining a shopping site for example, think "About to Use Shopping Site" and use "ABT2_uz_\$h0pping"

USE different passwords for every unique account, such as work, banking, and email

DISABLE the "save password" feature in your Internet browser



CYBER SECURITY IS OUR SHARED RESPONSIBILITY

CONNECT WITH CARE



- **Keep your devices updated with the latest system and application patches**
- **Assume that Wi-Fi connections are not secure, since many Wi-Fi hotspots don't encrypt the information you send**
- **Do not log into financial accounts or other sensitive accounts when using public Wi-Fi networks**
- **Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi**



CYBER SECURITY IS OUR SHARED RESPONSIBILITY

DON'T TAKE THE BAIT



- Do not open attachments or click on links from untrusted sources
- Never send personal information in an email
- Keep your firewall and antivirus software updated