



# PUBLIC WI-FI

## WHAT YOU NEED TO KNOW

Although public Wi-Fi has made our life easier, it does pose a security risk.

brought to you by the  
**ICTC**  
INFORMATION AND COMMUNICATIONS TECHNOLOGY CENTER  
#techtips #cybersecurity

### UNSECURED



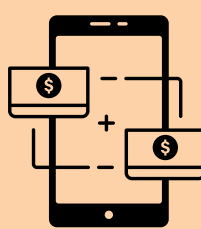
Users can connect without a password or login.

### SECURED



Requires a login and acceptance of legal terms.

## DON'T



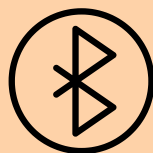
Access personal bank accounts or sensitive data on public Wi-Fi.



Leave your phone or laptop unattended in a public setting.



Shop online when using public Wi-Fi.



Leave your Bluetooth on. Hackers can look for open Bluetooth to gain access to your device.

## DO



Turn off automatic connectivity. It can make your device vulnerable.



Choose **secured** over **unsecured** networks when possible.



Limit airdrop and file sharing.



Use your cellphone as a hotspot if you have the data to support it.

A public Wi-Fi network is inherently less secure than your personal, private one because you don't know who set it up or who else is connecting to it. The best way to avoid security issues is to avoid public Wi-Fi, but if you must use it, take the steps above.

## NEED HELP?

✉ helpdesk@dlsud.edu.ph

☎ 3225

INFORMATION AND COMMUNICATIONS TECHNOLOGY CENTER

De La Salle University - Dasmariñas

+63 (46) 481.1900 Local 3225

✉ ictc@dlsud.edu.ph