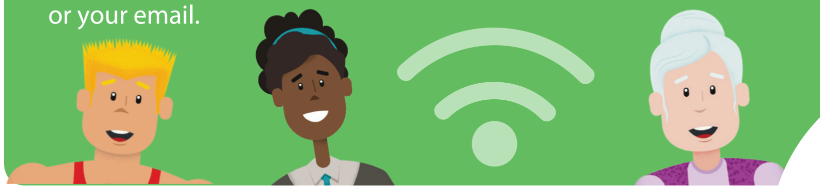
Protect IT. IT's up to you.

OWN
SECURE
PROTECT
IT.
OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

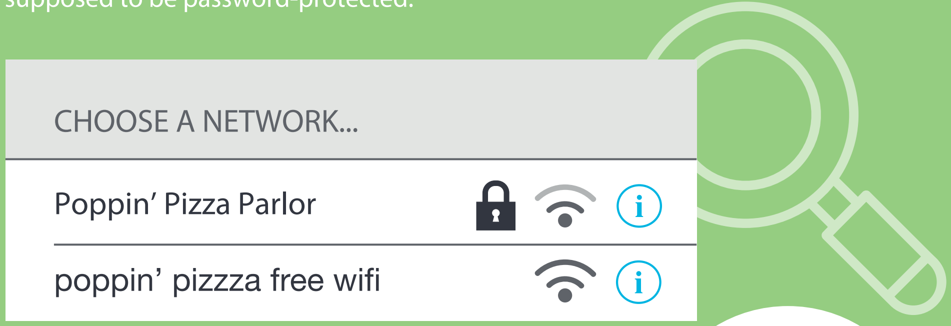
Public has **no privacy**

Using **public networks is always a risk.** When using a public network, such as in a coffee shop or an airport, never access private information like your bank or your email.



Spot the copycat

Hackers will sometimes create copycat networks with the same or similar names to existing, legitimate networks. These copycats will lack password protection to entice people into using them. When connecting to a network run by a person or a business, **always confirm** exactly which network is theirs and whether it's supposed to be password-protected.



CHOOSE A NETWORK...

Poppin' Pizza Parlor 🔒 ⓘ

poppin' pizzza free wifi ⓘ

Auto-connect is **not correct**

Having a device automatically connect to known and remembered networks is a fast ticket to malware. **Disable auto-connect** and carefully choose the network you want.

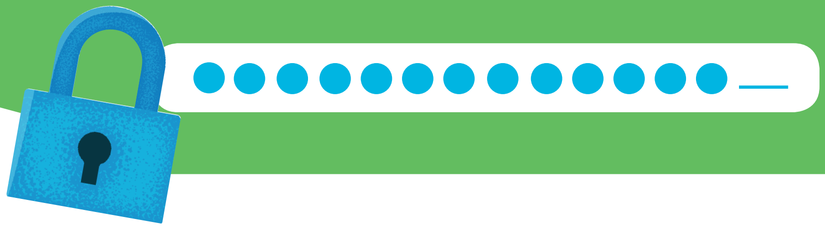
Bob's Cafe - FREE WIFI

Forget This Network

Auto-Connect ○

Password **preferred**

Public, unprotected networks are more likely to be run by hackers looking for an easy target. When working remotely, always **use the password-protected networks** controlled and monitored by the business owner.



Berkeley Information Security Office

More information at
https://security.berkeley.edu/ncsam-2019