HOW TO STAY SAFE ON PUBLIC WI-FI

HOUSEKEEPING

Q&A

- Ask ANY questions you have, we have time after the webinar content to answer them live

Survey

- There will be a survey after the webinar. Please fill it out as we want to make these better for you!

Replay/slides

- We will send a replay and slides next week via email, keep an eye on your inbox!

WHAT WE'LL COVER

- What we mean by public networks
- The best thing you can do
- the cybersecure mindset
- Technical and non-technical tips to keep you safe

WHAT DO WE MEAN BY PUBLIC NETWORKS?

WHAT DO WE MEAN BY PUBLIC NETWORKS?

Networks where you don’t know their security level

- **Guest Wi-Fi**
- **Hotel Wi-Fi**
- **Your local coffee shop (eg. starbucks, etc.)**
- **Open Wi-Fi networks (#TELUS, ShawOpen, etc.)**

THE BEST THING YOU CAN DO

THE BEST THING YOU CAN DO

The best thing you can do to protect yourself on public networks is:

1. **Not use them in the first place**
    a. **Use data/LTE on your mobile device**
    b. **Hotspot yourself**

THE CYBERSECURE MINDSET

THE CYBERSECURE MINDSET

ANY device you own is at risk of being compromised: phone, laptop, tablet, etc.

The networks available to you COULD be set up by a cybercriminal

When you connect to a network, you have decided the benefits outweigh the risks

NON-TECHNICAL TIPS

NON-TECHNICAL TIPS

ASK FOR THE INFORMATION

- **Don’t guess the network**
- **Ask the person at the counter for the Wi-Fi information**

CHECK WHAT YOU’RE SIGNING UP FOR

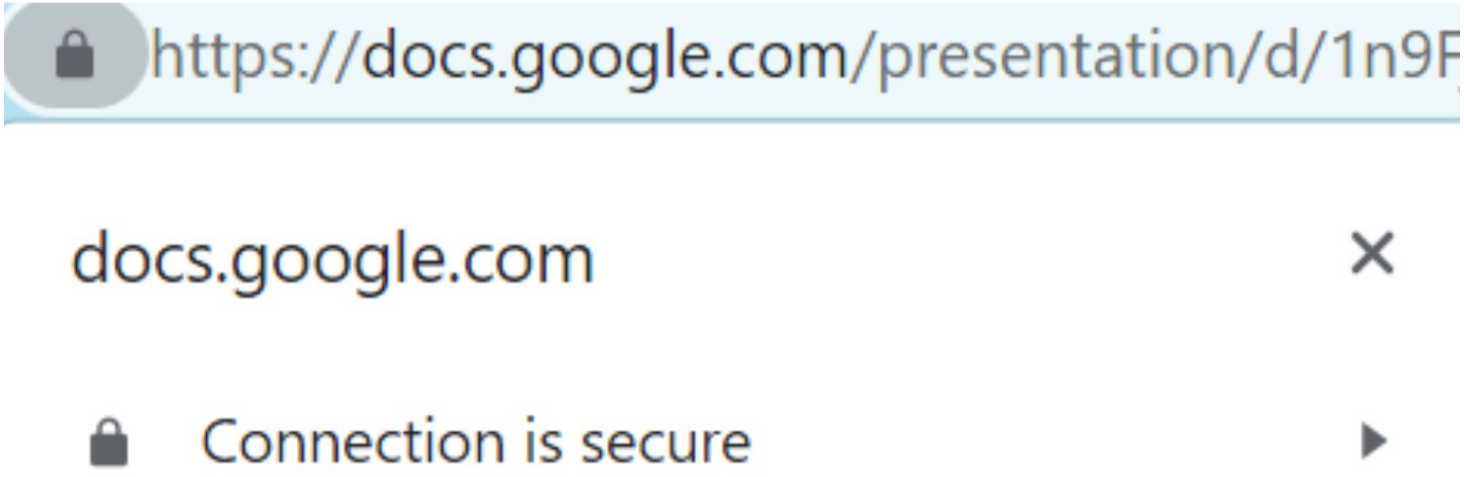
- **Ever had to enter your email to access a public network?**
- **Ever wondered WHY your email was needed to sign in?**
- **Read the Terms of Use/Terms and Conditions**

TECHNICAL TIPS

TECHNICAL TIPS

CHECK YOUR CONNECTION IS SECURE

- **Google lets you know if a website is using encrypted HTTPS**



TECHNICAL TIPS

While on a public network AVOID sites that require/hold important information

- **Don’t access personal or financial information**
- **Don’t use the same password on different websites (see our last webinar)**

TECHNICAL TIPS

Use a VPN

- **VPNs encrypt data by default**

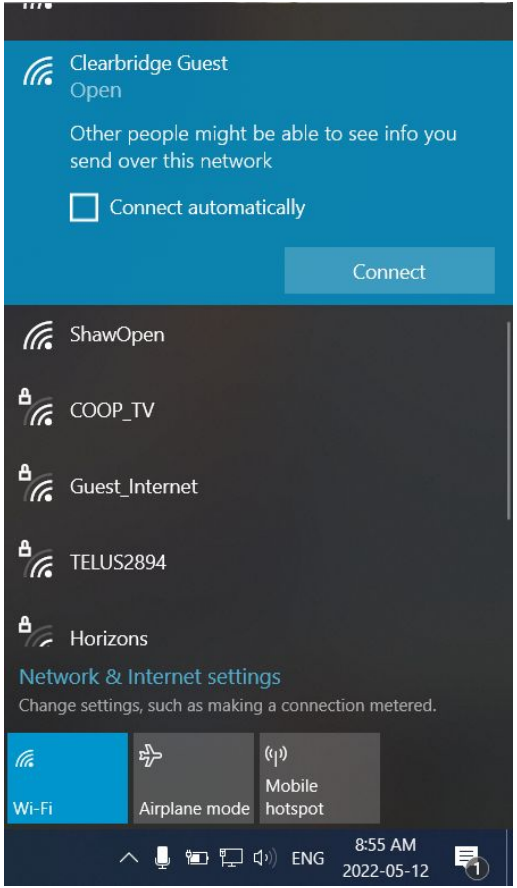
TECHNICAL TIPS

DO NOT UPDATE/UPGRADE/DOWNLOAD SOFTWARE TO YOUR DEVICE

- **Don’t click popup windows asking you to install/download software for you to access public wifi**
- **Don’t download anything from the web**
- **ALWAYS avoid doing system updates/upgrades on public wifi**

TECHNICAL TIPS

Disable Connect Automatically to Public WiFi networks



LET’S RECAP

LET'S RECAP

Public networks are networks where you don't know their security level
- **These include guest networks, coffee shop wifi, hotel wifi, etc.**

The safest thing to do is use your own data/LTE/hotspot

The cybersecure mindset believes: ANY device is at risk of being compromised

If you need to connect to a public network, double-check it's the right one
- **Non-technical**
  - **Ask the person at the counter**
  - **Check what you're signing up for (question why they need info from you)**
- **Technical**
  - **Check your connection is secure**
  - **Avoid sites that require important information (eg. banking)**
  - **DO NOT UPDATE/UPGRADE/DOWNLOAD SOFTWARE**