Script

Portray the chances of a smartphone user becoming a victim of a public WiFi attack.

Picture this. It’s Saturday morning and you’re hanging out at your local coffee shop using the free Wi-Fi to catch up on a few tasks you couldn’t quite get to during your busy week. Sound familiar? This is typical for many of us, but did you know you might be unaware of some threats lurking in the background on public Wi-Fi while you balance your bank account and sip a hot chocolate?

Public Wi-Fi is mostly found in popular public places like airports, coffee shops, malls, restaurants, and hotels — and it allows you to access the Internet for free. Although it sounds harmless to browse some news articles, everyday activities that require a login — like checking your social media account, reading email, or checking your bank account — could be risky business on public Wi-Fi.

Showcase the consequences of using public WiFi so as to show its severity.

Data sent through public wifi networks can easily be intercepted by cybercriminals. What you thought was private could no longer be. A common danger is eavesdropping. Cybercriminals could buy software kits or special devices to help them access everything that you are doing online — from viewing whole webpages you have visited (including any information you may have filled out while visiting a webpage), to even hijacking your accounts.

Fake WiFi hotspots trick victims into connecting to what they think is a legitimate network because the name sounds reputable. Once you connect to this fake wifi network, everything you do online is monitored by cybercriminals, who scan your activity for banking and social media login information.

Explore whether smartphone users are concerned about the use of public WiFi.

In Kenya, 86% of mobile phone users are aware that open public WiFi hotspots may expose personal and financial data, yet 71% still connect to them.

Users perceive they can **control** the occurrence of information security risk and know when to **carry out preventive** measures so as to protect their information towards the perceived benefits.

Luckily, there are ways to stay safe on public wifi.

Cues to action, costs and benefits.

One, Avoid checking sensitive data. Hold off on logging in to your social media, email, and especially financial accounts while on public WiFi.

Two, If you need to check sensitive data like your banking account or work data, use a VPN or go to the website instead and verify it uses HTTPS. Even if a cybercriminal eavesdrops in the middle of your connection, your data will be strongly encrypted.
Three, Verify your connection. Ask an employee what the actual WiFi is to avoid connecting to a fake one.
Four, Never turn on the auto-connect option for public WiFi. And make sure you turn your wifi off when you're done. The wifi hardware might still be transmitting data with any network in range even without you actively connecting to it.

If the perceived benefits outweigh the costs.
Understanding public WiFi risks will ensure your sensitive data doesn't fall into malicious hands. Follow these tips and reduce your exposure while on public WiFi.