"A DIGITAL STORY FOR INCREASING PUBLIC WI-FI SECURITY AWARENESS AMONG KENYAN SMARTPHONE USERS"

By

Mwaniki Nyaga

+254720207898
mwaniwakinyaga@gmail.com

FADE IN:

INTERIOR, COFFEE SHOP

Slow motion tracking shot pulling into unoccupied table.

NARRATOR

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?

Slow motion pull in to side of subject 1.

SUBJECT 1

Sits with drink and phone in hand. On screen, they scroll through emails. Subject reads one and begins typing a reply.

Camera slow zooms towards phone screen.

NARRATOR

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?

SUBJECT 1

Opens banking app and begins to check transaction history.

NARRATOR

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.

OVERLAID WITH STOCK FOOTAGE OF AIRPORT LOUNGE, HOTEL LOBBY, MALL AND RESTAURANT.

NARRATOR

Although it sounds harmless to browse some news articles, everyday activities that require a login — like checking your social media account, reading e-mail, or checking your bank account — could be risky business on public Wi-Fi.

SUBJECT 1

Browses social media account, opens an article and begins scheming.

INTERIOR, COFFEE SHOP

Slow motion tracking shot pulling into subject 2 sited at a table.

NARRATOR

Data sent through public Wi-Fi networks can easily be intercepted by cybercriminals. What you thought was private could no longer be. A common danger is eavesdropping.

Pan around subject 2's laptop on the table. Go round and behind subject 2.

NARRATOR

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.

Slow zoom towards laptop screen as subject 2 fake types on keyboard. Keep sections of fingers in shot.

STOCK FOOTAGE OF ANIMATED EAVESDROPPING GRAPHIC

NARRATOR

Fake Wi-Fi hotspots trick victims into connecting to what they think is a

legitimate network because the name sounds reputable. Once you connect to this fake Wi-Fi network, everything you do online is monitored by cybercriminals, who scan your activity for banking and social media login information.

STOCK FOOTAGE OF ANIMATED FAKE WIFI PLOT

NARRATOR

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

WRITTEN GRAPHIC

NARRATOR

Luckily, there are ways to stay safe on public Wi-Fi. One, Avoid checking sensitive data. Hold off on logging in to your social media, email, and especially financial accounts while on public Wi-Fi.

WRITTEN GRAPHIC

SUBJECT 1

More shots of browsing; banking, email and socials.

NARRATOR

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.

Camera slow zooms to mobile screen with VPN running in background.

SCREEN RECORDING OF BROWSING WITH VPN ACTIVE

SUBJECT 1

Types in a URL to site on browser. Clicks lock sign once page loads and reads notice.

Camera slow zooms to mobile screen with URL being typed.

SCREEN RECORDING OF URL/HTTPS

NARRATOR

Three, Verify your connection. Ask an employee what the actual Wi-Fi is to avoid connecting to a fake one.

Shot of subject 1 inquiring about the Wi-Fi with wait staff.

NARRATOR

Four, never turn on the auto-connect option for public Wi-Fi. And make sure you turn your Wi-Fi off when you’re done. The Wi-Fi hardware might still be transmitting data with any network in range even without you actively connecting to it.

Camera slow zooms to mobile screen with Public Wi-Fi options being checked.

SUBJECT 1

Opens Wi-Fi settings, unchecks auto-connect option.

SCREENRECORDING OF WI-FI SETTINGS

NARRATOR

Understanding public Wi-Fi risks will ensure your sensitive data doesn’t fall into malicious hands. Follow these tips and reduce your exposure while on public Wi-Fi.

SUBJECT 1

Sips drink while casually browsing, faint smile on their face.

FADE OUT:

THE END