B&C

DO YOU KNOW?

CYBERSECURITY EDITION

SWIPE

Public Wi-Fi USAGE

Do you know public Wi-Fi can expose everything you do online?

SWIPE

Public Wi-Fi networks pose significant security risks for businesses and remote workers due to their open and unencrypted nature. Cybercriminals often exploit these vulnerabilities to steal sensitive data, deploy malware or compromise user accounts.

SWIPE

Whenever you connect to a public Wi-Fi network, your data is transmitted over an unsecured connection, making it easy for hackers to intercept sensitive information such as login credentials, debit card numbers, BVNs, personal details and business data.

SWIPE

B&C

Attackers often exploit device vulnerabilities on public Wi-Fi through **Man-in-the-Middle (MitM)** attacks, malware injections or fake hotspots. Such breaches can even compromise the entire corporate network once an infected device reconnects to the office system.

SWIPE

To protect your data on public Wi-Fi, it is essential to always take necessary precautions. One of the most effective methods is by using a Virtual Private Network as it encrypts your internet traffic, making it difficult for hackers to intercept the data. Additionally, enable Two-Factor Authentication (2FA) for an additional layer of protection, requiring a second form of verification to access accounts.

SWIPE

Lastly, it is crucial to ensure that the websites visited have a secure connection, indicated by "https://" in the URL. Refraining from accessing sensitive information, such as financial data or personal information, while using public Wi-Fi, is also recommended. When possible, use your mobile data or a trusted hotspot instead.