

Mobile BYOD + Zero Trust

Safeguard Every Device



Why Zero Trust?



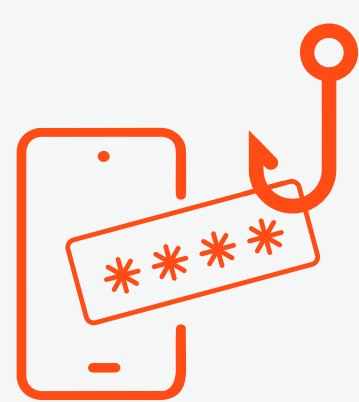
Always verify:
No automatic
"safe zone".

82% of companies rely on personal devices for work.

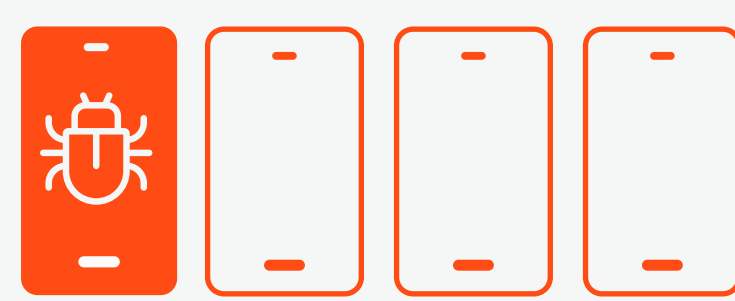
5M phishing attacks reported in 2023.



Common Mobile Threats



Phishing (Mishing):
83% target mobile.



Malicious Apps:
1 in 4 devices hit by malware.

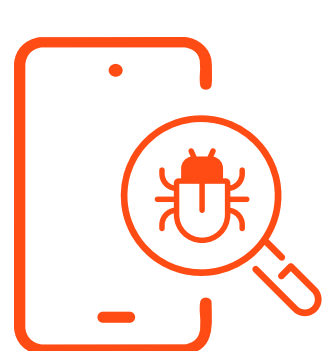


Shady Wi-Fi:
13% face man-in-the middle hacks.



Juice Jacking:
Public USB chargers can infect phones.

How Mobile Threat Defense (MTD) Helps



On-Device Scanning:
Blocks threats in real-time.



Privacy Protection :
Keeps personal and work data separate.



Continuous Health Checks:
Stops risky devices from accessing data.



Quick Tips for BYOD Safety



Set and enforce Clear Rules (Passwords, OS updates).



Use MTD Tools (like Zimperium).



Train Teams (spot phishing, avoid shady chargers).

Implement BYOD in a Zero Trust World



Continuously Verify Devices:

Use on-device threat defense to ensure each device meets security standards.



Strengthen Access Controls:

Combine device health checks with identify and access management.



Segment Your Network:

Limit what a compromised device can access and reduce lateral movement.