

Staying Safe on Text & WhatsApp

Text messages and WhatsApp are now prime targets for smishing and phishing attacks over SMS or messaging apps. Attackers exploit trust and urgency to trick people into clicking links or sharing sensitive information.



How Attacks Happen:



Impersonating Companies

Messages may claim to be from delivery services, banks, or tech providers. A common trick: "Your Amazon package is delayed, click here to reschedule." Clicking the link can lead to a malicious site designed to steal your login info.

Tip: Don't click links in unexpected texts. Always check messages through official apps or websites.



Urgent or Scary Language

Attackers use pressure to make you act fast: "Your account will be locked in 24 hours, act now!" Urgency reduces the chance you'll pause and think, which is exactly what scammers rely on.

Tip: Be suspicious of urgent language. Real companies rarely pressure you like this.



Requests for Codes

Some attacks ask for login or multi-factor authentication (MFA) codes, pretending they need them to "verify your identity." Scammers may even pose as IT support or a friend in need.

Tip: Never share MFA codes with anyone, not even people claiming to be from your bank or IT team.