

Phishing

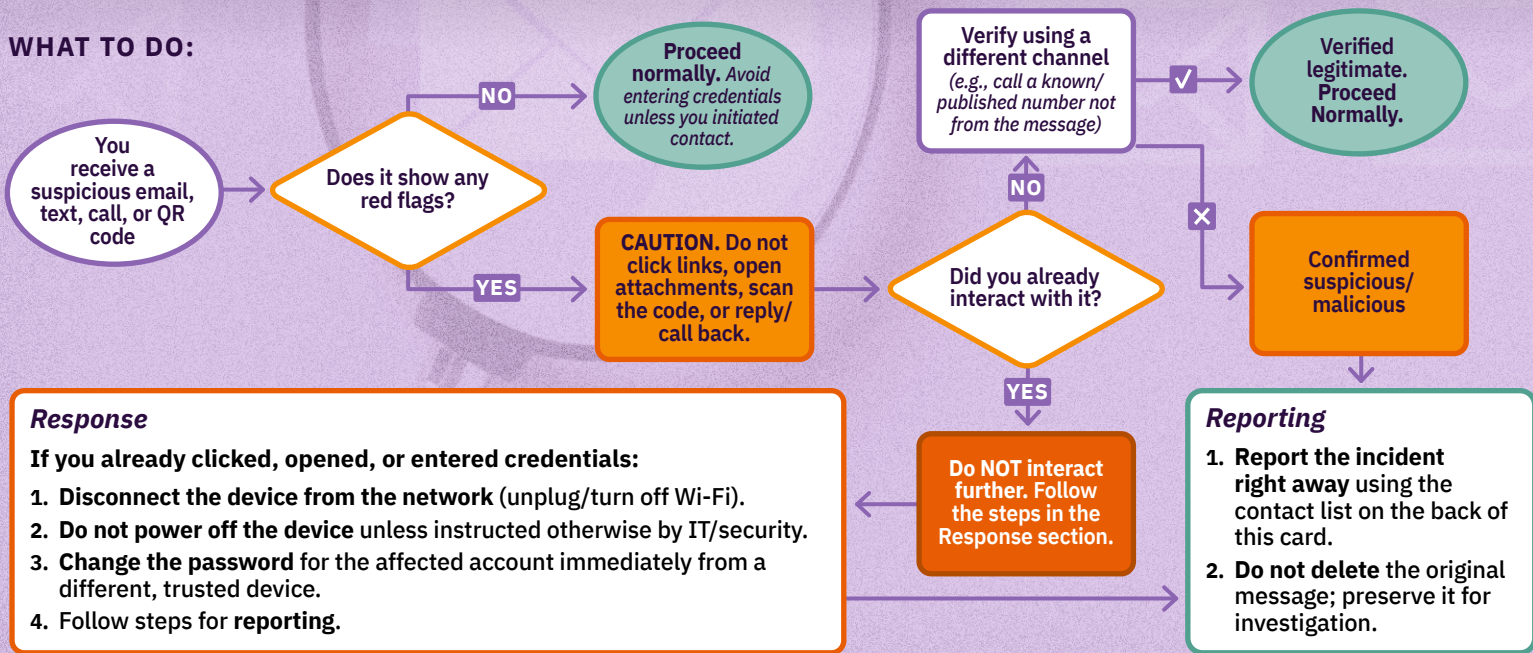
Quick Reference Guide for Suspicious Emails, Texts, and Calls



SPOT THE RED FLAGS

- Message creates urgency or pressure to act
- Address or domain is off (e.g., .com vs. .gov, misspelled)
- Generic greeting instead of name ("Dear Customer")
- Awkward phrasing, poor grammar, misspelling
- Link preview doesn't match the site it claims
- Unexpected attachment or file type doesn't match icon/extension
- Request for credentials/access via QR, text or unfamiliar caller

WHAT TO DO:



Key Contacts & Resources

JURISDICTION:

ROLE	NAME	PHONE	EMAIL
IT Support/ Security Team			
County/Local Election Office			
State Election Security Lead			
State or Local Law Enforcement (<i>Cyber</i>)			
Other:			
Other:			

JURISDICTION NOTES & LOCAL PROTOCOL

ADDITIONAL RESOURCES:

- CISA: Report Phishing and Other Cybersecurity Incidents
- CISA Insights: Actions to Counter Email-Based Attacks on Election-Related Entities
- Election Security Exchange: Phishing Threats
- MS-ISAC/EI-ISAC

Access these
resources
and more:

