DETECT, DEFLECT, DEFEND
CYBER EVIDENT

Your digital safety matters to us—
reach out anytime!

helpline@cyberevident.com

DETECT

1. Urgent Requests: “Act now!” or “Your account will be locked!”
2. Unfamiliar Senders: Check the email address or phone number carefully.
3. Requests for Sensitive Info: Asking for passwords, PINs, or personal details.
4. Too Good to Be True: Promises of lottery wins or unexpected situations.

DEFLECT

1. Verify with the Source: Contact the company directly via official channels.
2. Ask Questions: Scammers often stumble when challenged.
3. Refuse Suspicious Payments: Never pay via gift cards, cryptocurrency, or wire transfers.
4. Hang Up or Delete: If it feels wrong, end the interaction immediately.

DEFEND

1. Enable Multi-Factor Authentication (MFA): Add an extra layer of security to your accounts.
2. Monitor Your Accounts: Check for unauthorized activity regularly.
3. Regular Updates: Keep your devices and apps updated to avoid vulnerabilities from trusted sources.
4. Report Scams: Notify your bank, telecom provider, or a local cybercrime agency.

Call Now

IF IT FEELS TOO URGENT, TOO PERSONAL, OR TOO GOOD TO BE TRUE, PAUSE AND THINK. SCAMMERS RELY ON YOUR REACTION —DON’T GIVE THEM THE CHANCE!