CENTRIPETAL

Social Engineering

THINK BEFORE YOU CLICK!

Too Good To Be True

Skillfully crafted phishing emails often leverage psychological triggers to prompt you to click.

Phishing Patterns

Cyber attackers frequently exploit current events such as tax seasons, major sporting events, and health crises like the COVID-19 pandemic to launch phishing campaigns.

Email Tone

Phishing messages manipulate emotions, using greed, urgency, curiosity, and fear as powerful motivators.

Unsolicited Emails

Avoid clicking on links or opening files from suspicious, unsolicited emails. Always verify with the supposed sender through a phone call.

Deceptive Prompts

Be particularly cautious when prompted to enter usernames and passwords on external websites, as these can be deceptive and highly realistic.

Impersonal Phrases

Watch out for impersonal phrases in emails. Generic greetings may indicate a phishing attempt.

Sender Address

Check the sender's address for anomalies. Ensure it aligns with the name of the purported reputable company.

URL too Short?

Be cautious of shortened URLs, as criminals often use them to hide the true destination. Hover over links to reveal the underlying URL.

Phishing Awareness

Promote phishing awareness by conducting regular simulation campaigns for employees.

Configure Mailbox

Configure your mailbox to label external emails with a warning like "External Email."

Double check with your contacts

Double-check requests for payments or updates to payment information, especially in Business Email Compromise (BEC) attacks.

Received a suspicious email?

If you receive a suspicious email, report it to your IT department and follow their guidance. In case of accidental clicks or downloads, contact your IT department immediately for proper remediation.

Contact Us: Website: https://www.centripetal.ai/, **Email:** sales@centripetal.ai