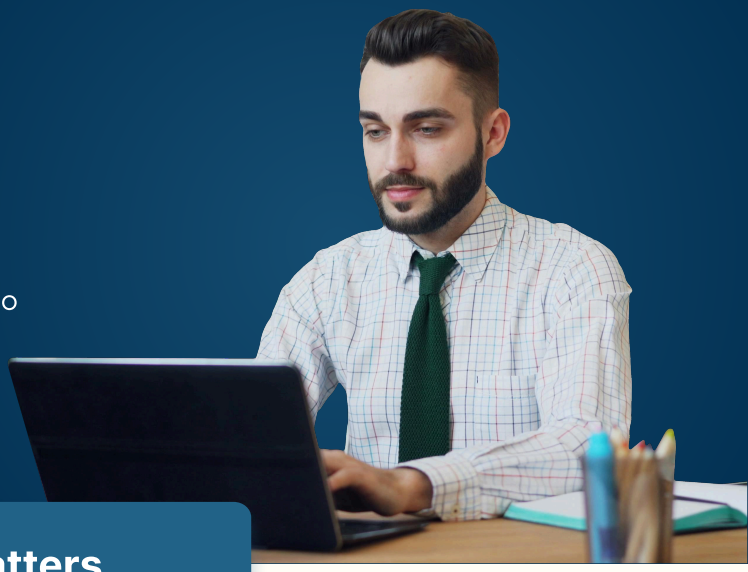
Think Before You Click

One careless click is all it takes to trigger a major cyber incident. Hackers rely on urgency, curiosity, and distraction to trick people into clicking malicious links or opening harmful attachments. Taking a moment to pause and think is the simplest and most powerful defence.



Why It Matters

The First Step in Most Attacks

Phishing emails, fake links, and suspicious attachments are the most common ways hackers break in. Once clicked, they can install malware, steal credentials, or spread ransomware.

Tip: *Always pause and think before clicking any link or opening an attachment.*

Sender Verification

Attackers often spoof addresses or impersonate colleagues to build trust. A quick check of the sender's identity can reveal a scam.

Tip: *Double-check email addresses and question anything that feels unusual.*

Sense Check

If a message feels odd, like a colleague suddenly asking for money or urgent action, it's likely a scam.

Tip: *Ask yourself, "Would this person really ask this?" If not, verify through another channel.*

When in Doubt

Uncertainty is a red flag. Clicking is irreversible, but reporting helps everyone stay safe.

Tip: *If unsure, don't act; report the message to IT or security instead.*