“Is This Email a Trap?”
Phishing Awareness Checklist

Spot the Red Flags

- Does the email use urgent or threatening language?
- Is the sender’s address slightly “off” or unfamiliar?
- Are there unexpected attachments or links?
- Is it asking for payment, login credentials, or sensitive data?
- Does something just feel off?

Think Before You Click

- Pause and verify before clicking links or opening attachments.
- Hover over links to preview the actual URL.
- Never share passwords or patient data over email.

Reporting

- Always flag weird emails...no blame, no shame.
- Follow your incident response plan if something occurs.

Make Training a Habit

- Run quarterly phishing simulations.
- Host quick monthly refreshers or cybersecurity tips.
- Reward “threat spotters” on your team.

Cyber-Smart Culture

- Appoint a “Cybersecurity Champion” on your team.
- Remind your team that staying safe is everyone’s responsibility.
- Partner with a dental IT expert like Pact-One for extra protection.