BEC Quick Guide
for Dental Teams

1

We got an email from our dentist asking for a payment to a new vendor...how do I know if it's legit?

If something feels off, don't second-guess yourself...verify it. Call or talk to the dentist in person before sending any money or updating account info. BEC scams often impersonate familiar names with small changes you might miss at a glance.

2

What does a BEC scam actually look like in a dental office?

It could be an email that looks like it's from your supply rep or lab asking you to pay an invoice—but the bank account has changed. Or it could be a message from your "dentist" saying they need a wire transfer urgently. These emails usually look professional and believable.

3

Wouldn't our antivirus software catch something like this?

Not always. Most BEC scams don't include malware or suspicious links. That's what makes them so dangerous...they're designed to fly under the radar of traditional security tools by using real email accounts or carefully spoofed ones.

4

Our team is busy and wears a lot of hats...how can we spot scams quickly?

Teach your team the basics:

- Always double-check any requests involving money or account changes.
- Look closely at email addresses (like @dentalc0rp.com instead of @dentalcorp.com) and not just the name (like Dr. Baker – drbaker@adbdental.com instead of Dr. Baker – companyemail5623@gmail.com).
- Slow down when something feels urgent. Urgency is a common red flag in scams.

We recommend regular 5-minute huddles or quick lunch-and-learn sessions to keep everyone sharp.

5

What should we do if we think we've already fallen for one?

Don't panic, but act fast:

1. Notify your dentist or practice manager immediately.
2. Call your bank/credit card company and try to stop the transaction.
3. Contact your IT provider or cybersecurity partner (like Pact-One) ASAP.
4. Change any affected passwords.
5. Report the incident to the FBI's Internet Crime Complaint Center (IC3).