TSBDE FRAUD ALERT

Unfortunately, stakeholders often receive fraudulent calls or emails purporting to be from The Texas State Board of Dental Examiners (TSBDE). If you suspect a telephone call or correspondence from our agency is fraudulent, please notify us by emailing fraud.alert@tsbde.texas.gov or calling 512-305-7724.

Please visit the Consumer Protection section of the Texas Office of the Attorney General to learn about common scams and how to report scammers here.

FRAUDULENT PHONE CALLS

TSBDE urges you to be on the lookout for unexpected scam phone calls from anyone claiming to be from our office.

A caller from the TSBDE office will ALWAYS:

Introduce himself or herself as a TSBDE employee.

Be able to verify specific details on prior notices or historical account information.

Explain your licensing or compliance fees.

Encourage you to call the telephone number(s) on our website if you have any questions about the process: TSBDE Agency Contacts

FRAUDULENT PHONE CALLS

A caller from the TSBDE office will NEVER:

Threaten to bring in local police, FBI, immigration officers or other law-enforcement to have you arrested for not paying.

Pressure you to make a payment.

Ask for personal information not directly related to an agency transaction.

Ask for money outside of routine transactions made through Texas.gov or our secure vendors.

Ask for bank account information.

If you are unsure that the person calling you is from the TSBDE office, please hang up and call the appropriate number on our website:
TSBDE Agency Contacts.

SPOOFED EMAILS/ RECENT PHISHING ATTEMPTS

Cybercriminals have attempted to send spoofed (impersonated) emails — appearing to be from the TSBDE office. Our office, like other companies and government agencies, has unfortunately been the subject of a number of recent email fraud attacks, including:

Spoofed emails claiming to be from our office but using a domain not associated with the agency, urging recipients to click on a “secure message” but the attachment is malicious, intended to steal usernames and passwords.

Emails should come from someone with a TSBDE domain: jsmith@tsbde.texas.gov.

Spoofed emails purporting to be from our office but using a fake agency email domain telling recipients to click on an attachment and sign in to receive a message. The attachment contains a fraudulent link designed to steal your log-in credentials.

Spoofed emails purporting to be from an authorized TSBDE email service but using a comcast.net email domain. The attached PDF instructs users to click on a “View Information” link which is designed to steal login credentials.

SPOOFED EMAILS/ RECENT PHISHING ATTEMPTS

Please be advised that as a licensee of TSBDE, some of your practice information is published to the public. Be wary of this when someone claims to be from TSBDE. To see what information is available, you may visit here.

Phone Scam Attempts

Licensees have reported that a person called them purporting to be from TSBDE pressuring them about TSBDE investigations and requesting money.

TSBDE will never pressure you for money over the phone. If you owe licensing or other fees to TSBDE, we have official channels to collect that money and will work with you if you have any questions. These cybercriminals are putting your information at risk and trying to damage good customer relationships. That is why we are expanding our efforts to fight fraud and keep you safe and secure.

Please be advised that as a licensee of TSBDE, some of your practice information is published to the public. Be wary of this when someone claims to be from TSBDE. To see what information is available, you may visit: https://tsbde.texas.gov/resources/public-license-search/.

SPOOFED EMAILS/ RECENT PHISHING ATTEMPTS

Phone Scam Attempts

If you are suspicious about an email or phone call that claims to be from the TSBDE office, follow these tips:

Question whether the information should be requested via email or telephone.

Be wary of links and attachments. Consider the context of the email, look for red flags such as poor grammar and/or sentence structure, and when in doubt– don’t click.

Use an email spam filter and up-to-date virus software and avoid public Wi-Fi.

When suspicious, do not respond to the original email. Use independent sources to verify sender details and establish a new channel of communication to confirm with the sender.

If you suspect any communication from our agency is fraudulent, please notify us by emailing fraud.alert@tsbde.texas.gov.