WINSTON & STRAWN LLP

Scam & Fraud Alerts

Like many reputable law firms and global organizations, Winston & Strawn LLP's brand and the names of our attorneys and business professionals are increasingly being used to conduct scam and fraud campaigns. These scams can occur in many different forms and are constantly evolving.

RECENT FRAUD ATTEMPT EXAMPLES REPORTED TO US

- **Copyright Infringement Scam** - Email from a fictitious Winston attorney claiming your website is infringing on copyrighted images/materials. The goal is to scare the potential victim into paying to settle the bogus claim.
- **Invoice Payment Redirection** - Spoofed email from someone claiming to be a Winston attorney requesting payment of an invoice. This typically involves the bad actors using impersonation to hijack an email conversation and redirect payment to a fraudulent bank account.
- **Confidential Business Deal** - Phone call or WhatsApp message from someone pretending to be a Winston attorney requesting assistance with a confidential business deal. The goal is to trick the recipient into clicking a malicious link or attachment and obtaining access to the person's computer or accounts.
- **Fake Job Positing –** Job board positing advertising a fictitious open position using the firm's name. The goal of the scam is to lure someone into providing their personal or financial information.

WHAT YOU CAN DO

Be vigilant and exercise caution when it comes to any unusual or unexpected communications. **Genuine emails from Winston & Strawn will only originate from the "@winston.com" or "@winstonls.com" domains**. Be particularly cautious communicating with anyone claiming to a Winston attorney using a personal email domain (e.g., Gmail, Yahoo, Hotmail).

If you receive a communication which purports to be from one of our attorneys or business professionals and are unsure as to its authenticity, please call your usual Winston contact or email our security team before engaging with the sender. If possible, please provide a copy of the original email (as an attachment, not a forwarded message).

REFERENCES

The SRA publishes scam alerts on its website to warn the public when the name of an SRA-regulated entity is being misused. Visit the SRA's website to learn more.

Additionally, the FBI routinely publishes information about common scams. Visit the FBI's website to learn more.