SECURITY INSIGHTS:

How Scammers Are Exploiting Public Records to Steal Your Money

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

You're in the middle of a zoning application for a new office build-out. An email lands in your inbox from what appears to be a city planning official - complete with the county seal, your permit number, and the correct property address. It says you owe a processing fee and warns that delays will follow if you don't pay promptly. You've been going back and forth with the planning department for weeks, so this feels routine. You click to pay. Except that email didn't come from city hall - it came from a scammer who just walked away with your money.

The FBI recently issued a public warning about this exact scheme. Criminals are impersonating city and county planning and zoning officials to collect fraudulent permit fees from people with active applications. What makes this scam particularly convincing is the level of detail. The emails reference real permit numbers, actual property addresses, and sometimes even the names of legitimate government employees. None of that information is stolen from a database breach - it's all pulled from publicly available permit records that local governments post for transparency.

The timing is the real weapon here. These emails arrive while applicants are actively communicating with their local planning office, so a message about fees doesn't raise an eyebrow. The invoices look professional, with itemized statements and formal language about regulatory compliance and hearing agendas. But buried in the details are the tells: the sender's email comes from a non-government domain - something like "@usa.com" instead of an official ".gov" address - and the payment methods are wire transfers, peer-to-peer apps, or cryptocurrency. No legitimate government office asks you to pay permit fees in Bitcoin.

There's another clever trick. The emails specifically instruct recipients to communicate only by email-not by phone -claiming it's necessary for an "audit trail." That's designed to keep you from picking up the phone and calling the actual planning office, which would immediately expose the fraud.

For anyone in the title, real estate, or property development, this one hits close to home. You're regularly involved in permitting, zoning applications, and municipal processes. A convincing invoice tied to an active project could easily slip through - especially during a busy closing week when dozens of legitimate payment requests are already in motion.

TAKEAWAYS

- **Verify every payment request by phone.** If you receive an invoice related to a permit or zoning application, call the city or county office directly using the number on its official website-not the number provided in the email.
- **Inspect the sender's email domain.** Government emails end in ".gov." If the address uses a commercial domain like "@usa.com" or "@gmail.com," it's not coming from a government office, no matter how official the letterhead looks.
- **Treat urgency as a red flag.** Legitimate planning departments don't threaten immediate consequences over email if you don't pay within hours. Pressure to act fast is a hallmark of fraud.
- **Never pay permit fees via wire transfer, peer-to-peer apps, or cryptocurrency.** Real government offices accept payments through their official website portals or in person. If someone directs you elsewhere, stop.
- **Alert your team.** If your office handles permitting or development work, make sure everyone involved knows this scam exists. One informed colleague can prevent a costly mistake.

Public records are meant to keep government transparent - but scammers are turning that openness into an attack vector. When an invoice arrives with your permit number, the instinct is to trust it. That instinct is exactly what they're counting on.