FEDERAL BUREAU OF INVESTIGATION

Public Service Announcement

Alert Number: I-030926-PSA | 09 March 2026
Criminals Impersonating City and County Officials in Phishing Emails for Planning and Zoning Permits

The FBI is warning the public about an emerging phishing scheme by criminals impersonating city and county officials to solicit fraudulent payments for city and county planning and zoning permits. The criminals leverage publicly available permit information to identify potential victims and increase the legitimacy of the scam. Victims of this scam have been identified nationwide.

How The Scam Works

Individuals and businesses with active applications for land-use permits are being targeted by criminals impersonating city and county planning and zoning board officials, fraudulently requesting fees associated with these permits. Victims receive unsolicited emails citing their permit information, zoning application numbers, and/or property addresses. Victims are instructed to pay invoices for fees related to their permits and directed to make payments via wire transfer, peer-to-peer payment, or cryptocurrency.

Common indicators of the scheme are:

- The emails contain detailed, accurate information about planning and zoning requests, including property addresses, case numbers, and the true names of city and county officials.
- The emails use professional language, formatting, and imagery consistent with legitimate government communications for planning and zoning applications, including review processes, planning commission procedures, regulatory compliance, and relevant ordinances.
- The email addresses contain usernames similar to city or county planning and zoning departments but originate from non-governmental domains, such as "@usa.com"
- Email delivery may be timed to coincide with ongoing communications with city and county officials regarding the permitting process.
- Attached PDF invoices contain itemized statements of purported fees and direct applicants to request payment instructions via email, rather than telephone, to ensure a reliable audit trail for all correspondence related to the application. This is designed to deter the victim from calling the city or county office to verify the fees.
- The emails emphasize urgency, threatening delays or other obstacles in the permitting process if the applicant does not immediately render payment.

Tips To Protect Yourself

- Do not assume emails are legitimate based on the use of city or county letterhead, seals, names of officials, or proper spelling and grammar.
- Verify the email address, including the domain name, matches the email address of the official with whom you are corresponding and does not contain extraneous characters or misspellings.
- Check the city or county official website for notices about ongoing impersonation schemes.
- Call the city or county government, using the phone number listed on the official website, to verify outstanding fees.

Report It

If you or someone you know has fallen victim to this impersonation scam, file a complaint with the IC3 at www.ic3.gov. Be sure to include any available information including:

- The email address, date of email, phone number, if provided;
- The date of your project's scheduled hearing, if applicable; and,
- The amount listed in the fraudulent invoice, the method requested to pay fees, and bank account information, if provided.