HORRY COUNTY GOVERNMENT

Fake Fee Requests Impersonating County Staff

Incident Brief: Planning and Zoning Fee Impersonation Scheme

Information Security Office | October 2026 | TLP:CLEAR

In October 2026, Horry County received its first confirmed report of a fraud scheme the FBI warned about nationally in March 2026. Criminals are impersonating city and county planning staff to collect fake fees from people with active land-use applications. This brief explains how the scheme works, how to recognize it, and what to do. It contains no case, applicant, or personal details and may be shared freely.

AT A GLANCE	
What happened	Criminals posed as a Horry County planner and emailed a fake fee invoice to someone with an active rezoning application, asking for payment by wire transfer.
Outcome	The applicant's representative recognized the scam, did not pay, and reported it. No county systems or accounts were compromised, and no money was lost.
Who is at risk	Residents, developers, agents, and businesses with active county applications or permits. The emails go to their own inboxes, outside county systems.
The one rule	**Before paying any emailed fee request, call the department using the phone number listed on the county website.**

What happened

An agent representing a current rezoning applicant received an email that appeared to come from a named county planner. It cited the real case number, property, and zoning request, and attached an official-looking invoice with the county logo requesting an “approval fee” of several thousand dollars by wire transfer. The agent noticed the sender's address was not a county address, did not respond, and reported it. Similar fake-invoice fraud has recently cost at least one other local government in the region real money, and these schemes are growing more convincing.

How the scheme works

Every step relies on information that is public by law. Nothing here required access to county systems.

1 Research

Criminals pull case numbers, property details, and staff names from public planning and zoning records.

2 Disguise

They create a free email account made to look like a county department, such as one with “horrycountysc.gov” placed before an unrelated domain.

3 Contact

They email the applicant or agent directly, posing as a real staff member, with a professional invoice using the county logo.

4 Pressure

The invoice says a fee is due before approval can proceed and warns of delays to approval or agenda placement.

5 Isolate

The target is told to keep all communication in email “for auditability.” The real purpose is to keep them from calling the county.

6 Collect

When the target replies asking how to pay, the criminal sends wire instructions for an account they control.

Because these emails go straight to the applicant's personal or business inbox, they never pass through county email systems. The county cannot block them on the recipient's behalf.

Warning signs

These messages look authentic. Focus on how they ask for money, not how they look.

- The sender's address does not end in **@horrycountysc.gov**, even if the name or address text includes the county's name.
- Payment is requested by wire transfer, peer-to-peer app, gift card, or cryptocurrency.
- Payment instructions are available only by replying to the email.
- You are told to keep all communication in email and not to call.
- The invoice is “due upon receipt” or warns that approval or agenda placement will be delayed.
- The fee was never mentioned during your normal dealings with the department.

IMPORTANT: Horry County does not request application or permit fees by wire transfer through email. Official county email comes only from addresses ending in @horrycountysc.gov.

County response

Planning and Zoning reported the email to the Horry County Information Security Office the same day the applicant's representative reported it. The Information Security Office confirmed the email was fraudulent and that no county account or system was involved, and blocked the sender's email domain at the county email gateway.

The incident was documented under the county's incident response process and shared with state cybersecurity partners so other South Carolina jurisdictions can warn their applicants.

Lessons learned

A skeptical person is the control that works. Technology did not stop this attempt, and in this scheme it cannot, because the fraud happens entirely outside county systems. The recipient who checked the sender address prevented the loss.

Public records are the raw material. Case details and staff names are public by law and need to stay that way. The answer is to tell the public clearly how the county does and does not ask for money.

The exposure extends beyond Planning and Zoning. Any department that collects fees tied to public filings, such as building permits and business licensing, faces the same risk and should use the same standard payment-verification language.

What you can do

If you are	What to do
Residents, applicants, and agents	Treat any emailed fee request as unverified until you confirm it by phone. Call the department using the number listed on the county website, never a number from the email.
County departments that collect fees	State in applicant correspondence and on your web pages how fees are legitimately paid, and that the county will never request a wire transfer by email. Forward any customer report of a suspicious payment request to the Information Security Office right away.
Businesses and organizations	Confirm any new or changed payment instructions by calling a known contact before sending money, never by replying to the request.

Verify and report

If you receive a suspicious request, do not reply, click links, or open attachments. Contact the department directly using the phone number listed on the county website. County staff should report suspicious messages to the Information Security Office or the IT/GIS Help Desk.

Already paid?

Contact your bank immediately to try to stop or recall the transfer, then file a report with the FBI at ic3.gov. Speed matters: the sooner the bank is notified, the better the chance of recovering funds.

SOURCE

FBI Internet Crime Complaint Center, PSA I-030926-PSA: Criminals Impersonating City and County Officials in Phishing Emails for Planning and Zoning Permits, March 9, 2026.