

The Virgin Islands Consortium

Property and Procurement Warns Vendors of Suspicious Procurement Emails Using Unauthorized @vi-gov.us Domain

DPP is warning vendors, government agencies and partners about suspicious emails impersonating Procurement Division personnel and using the unauthorized @vi-gov.us domain, urging recipients not to send money, disclose banking data or open unexpected links

Government / **Published On August 20, 2026 06:11 AM /**

Ernice Gilbert **August 20, 2026**



The official GVI BUY homepage, the Government of the Virgin Islands' procurement system. DPP is warning vendors about suspicious emails impersonating Procurement Division personnel.

The V.I. Department of Property and Procurement is warning vendors, government agencies and partners about suspicious emails impersonating members of its Procurement Division, including messages sent from addresses using the @vi-gov.us domain, which DPP says is not an official Government of the Virgin Islands email domain.

According to DPP, the communications may include the names, titles or other identifying information of Procurement Division personnel, potentially making them appear legitimate. The department is urging recipients to exercise caution with any message from an @vi-gov.us address that claims to represent DPP Procurement Division personnel.

DPP Says Staff Will Not Request Money Through Unsolicited Emails

DPP stressed that Procurement Division personnel will never use this type of unsolicited email communication to ask vendors, government agencies or individuals to send funds, purchase gift cards, transfer money, provide banking information or make payments.

The department also cautioned that the unauthorized use of an employee's name, title, email signature or other identifying information does not mean the communication originated from that employee or from the Government of the Virgin Islands.

What Recipients Should Do

DPP advised anyone who receives a suspicious communication to take the following precautions:

1. Do not respond to the message.
2. Do not send funds or make payments.
3. Do not click unfamiliar links or open unexpected attachments.
4. Do not provide banking information, passwords, login credentials or other sensitive information.
5. Review the sender's full email address carefully, rather than relying only on the displayed name.
6. Preserve the suspicious email and, when possible, take a screenshot showing the sender's full email address and the contents of the message.
7. Independently verify questionable communications through established government communication channels before taking any action.
8. Be aware that unauthorized use of a DPP employee's name, title, email signature or other identifying information does not establish that the communication came from that employee or the Government of the Virgin Islands.

DPP said it is aware of the suspicious communications and is encouraging vendors, government agencies and partners to remain vigilant as part of efforts to protect against potential fraudulent activity.

GVIBUY Access

DPP also directed users seeking to access GVIBUY to the official login page: [Log on to GVIBUY](#)

