

(Para leer la versión en español visita nuestra página web:
www.utrgv.edu/is/files/documents/email-phishing-havidan-es.pdf o haz clic [aquí](#).)

The University of Texas
Rio Grande Valley
.....
Information Security Office

Dear UTRGV Community,

There have been reports involving the following phishing email targeting UTRGV employees. The screenshot below is a sample of the email and includes some common identifying characteristics of phishing/scam emails.

IMAGE STARTS

The screenshot shows an email header and body with several red boxes highlighting suspicious elements:

- From:** Havidan Rodriguez <provost@utrgv.edu> <sheedy_catherine@wheatoncollege.edu > (A box labeled "Non-affiliated UTRGV email address" points to the second email address.)
- Subject:** Important Notice!!!
- To:** [Redacted] (A box labeled "Email is not addressed to anyone" points to the recipient field.)
- Attachment:** Important Notice From President Guy Bailey. phd.pdf (189 KB) (A box labeled "FAKE and UNSAFE document" points to the attachment name.)
- Salutation:** Dear Staffs and Faculty, (A box labeled "Staffs" points to the word "Staffs").
- Body Text:** This is an important notice to all utrgv[The University of Texas RioGrande Valley] staffs and Faculty. You are advised to review the attached document to prepare you towards the latest development in UTRGV. (A large box highlights the entire body text, which contains several grammatical errors.)
- Signature:** Sincerely, Havidán Rodríguez, PhD, Provost and Executive Vice President for Academic Affairs, 1201 West University Drive, Edinburg, Texas 78539, provost@utrgv.edu, 956-665-2111, 956-665-2114 fax, The University of Texas Rio Grande Valley. (A box labeled "Misspellings and Grammar errors" points to the signature block.)

IMAGE ENDS

The email attachment is fake and includes a link to a phishing website that requests your username and password. Please **do not open the attachment or provide your**

username or password to the phishing website. Please follow these cautionary tips and advice on how you can get help in case you received this or any other phishing email.

I received this email, what can I do?

- The email has been reported by multiple employees and we want to thank you for your diligence. We no longer need this phishing email forwarded, please simply delete the email. If you receive a new phishing or scam email, those can be forwarded to itdns@utrgv.edu
 - You can also visit the IT website for more instructions about how to report a phishing message: www.utrgv.edu/it/how-to/report-phishing-messages
- If you clicked on any of the links and provided your password, it is imperative that you change it immediately.
 - Visit the IT website www.utrgv.edu/it/how-to/account-management-change-password for instructions on changing your password or contact the IT Service Desk at 665-2020 or 882-2020.

Stay safe and secure, watch out for the following:

- Unsolicited emails, text, or social media posts or fake websites that may prompt you to click on a link or to share valuable personal and financial information.
- Fake IRS agents: The IRS will never email or call you demanding immediate payment without having first mailed a bill. Nor will they ask for a credit or debit card number via email or phone.
- Soliciting W-2 information from payroll.
- "Federal Student Tax" are scams targeting students and parents and demanding payments.

Where can I find more information about phishing?

If you like to know how phishing works, how to identify phishing scams, and more. Please visit the ISO website: www.utrgv.edu/is

If you have any questions, concerns, or comments please reach us at:

Phone: (956)665-7823

Email: is@utrgv.edu

Sincerely,

The Information Security Office

For the Spanish version of this email visit our website:

www.utrgv.edu/is/files/documents/email-phishing-havidan-es.pdf



Brownsville • Edinburg • Harlingen • McAllen
Rio Grande City • South Padre Island • utrgv.edu

