

Estimada comunidad UTRGV,

Ha habido informes que implican el siguiente ataque de phishing por correo electrónico dirigido a los empleados de UTRGV. La siguiente captura de pantalla es una muestra del correo electrónico e incluye características comunes de estos tipos de ataques.

COMIENZA LA IMAGEN

The screenshot shows an email interface with several red boxes highlighting suspicious elements:

- Correo electrónico no afiliado con UTRGV**: Points to the sender's email address, [sheedy\\_catherine@wheatoncollege.edu](mailto:sheedy_catherine@wheatoncollege.edu).
- Correo electrónico no incluye recipiente**: Points to the 'To:' field, which is empty.
- Documento FALSO y PELIGROSO**: Points to the attachment 'Important Notice From President Guy Bailey. phd.pdf (189 KB)'.
- Errores gramaticales**: Points to the 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.'.

The email content includes:

**From:** Havidan Rodriguez <[provost@utrgv.edu](mailto:provost@utrgv.edu)> <[sheedy\\_catherine@wheatoncollege.edu](mailto:sheedy_catherine@wheatoncollege.edu)>  
**Subject:** Important Notice!!!  
**To:** [Redacted]  
**Attachments:** Important Notice From President Guy Bailey. phd.pdf (189 KB)  
**Text:** Dear Staffs and Faculty,  
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.  
Sincerely  
--  
**Havidán Rodríguez, PhD**  
Provost and Executive Vice President for Academic Affairs  
1201 West University Drive  
Edinburg, Texas 78539  
[provost@utrgv.edu](mailto:provost@utrgv.edu)  
956-665-2111  
956-665-2114 fax  
The University of Texas  
Rio Grande Valley

LA IMAGEN TERMINA

El archivo adjunto a este correo electrónico es falso e incluye un enlace a un sitio web de phishing que solicita su nombre de usuario y contraseña. **No abra el archivo adjunto o proporcione su nombre de usuario o contraseña al sitio web** de

phishing. Siga estos consejos de precaución y consejos sobre cómo puede obtener ayuda en caso de que recibió este o cualquier otro ataque de phishing.

*He recibido este correo electrónico, ¿Qué puedo hacer?*

- El correo electrónico ha sido reportado por varios empleados y queremos agradecerle por su diligencia. Ya no necesitamos este correo electrónico de phishing reenviado, simplemente borre el correo electrónico. Si recibe un nuevo ataque de phishing, envíelo a [itdns@utrgv.edu](mailto:itdns@utrgv.edu)
  - También puede visitar el sitio web de TI para obtener más instrucciones sobre cómo informar un mensaje de suplantación de identidad: [www.utrgv.edu/it/how-to/report-phishing-messages](http://www.utrgv.edu/it/how-to/report-phishing-messages)
- Si ha hecho clic en cualquiera de los enlaces de correo electrónico y ha proporcionado su contraseña, es necesario que la cambie inmediatamente.
  - Visite el sitio web de TI [www.utrgv.edu/it/how-to/account-management-change-password](http://www.utrgv.edu/it/how-to/account-management-change-password) para obtener instrucciones sobre cómo cambiar su contraseña o póngase en contacto con el Centro de Servicio de IT al 665-2020 o al 882-2020.

*Manténgase seguro y a salvo, tenga cuidado con lo siguiente:*

- Correos electrónicos no solicitados, mensajes de texto o de redes sociales o sitios web falsos que pueden indicarle que haga clic en un enlace o comparta valiosa información personal y financiera.
- Agentes falsos del IRS: El IRS nunca enviará por correo electrónico o le llamará exigiendo un pago inmediato sin haber enviado por primera vez una factura. Tampoco pedirán un número de tarjeta de crédito o débito vía correo electrónico o teléfono.
- Correos electrónicos solicitando información W-2.
- Estafas de "Impuesto Federales de Estudiantes" dirigidas a estudiantes y padres exigiendo pagos.

*¿Dónde puedo encontrar más información sobre phishing?*

Si te gustaría saber cómo funciona el phishing, cómo identificar estas estafas y más. Visita el sitio web de la Oficina de la Seguridad Informática: [www.utrgv.edu/is](http://www.utrgv.edu/is)

Si tiene alguna pregunta, por favor contáctenos vía:

Teléfono: (956)665-7823

Correo electrónico: [is@utrgv.edu](mailto:is@utrgv.edu)

Sinceramente,

**The Information Security Office**



Brownsville • Edinburg • Harlingen • McAllen  
Rio Grande City • South Padre Island • [utrgv.edu](http://utrgv.edu)

