Universidad de Puerto Rico
Recinto de Rio Piedras

23 de julio de 2026

CIRCULAR NUM. 1 2026-2027
A TODA LA COMUNIDAD UNIVERSITARIA

Sr. Roberto García
Director Asociado

AVISO DE SEGURIDAD INFORMÁTICA - CAMPAÑA ACTIVA DE PHISHING DIRIGIDA A LA COMUNIDAD UNIVERSITARIA

En los pasados días, la Universidad de Puerto Rico ha observado un aumento inusual de mensajes asociados a una campaña de phishing, utilizando cuentas institucionales comprometidas, dirigidos a estudiantes, personal docente y empleados no docentes.

Como parte del monitoreo de seguridad realizado se han observado los siguientes patrones y características comunes:

- Mensajes que hacen referencia a cancelación de cuentas**,** ofrecimientos de empleo u otros escenarios diseñados para inducir urgencia.
- Inclusión de URLs externas cuyo propósito es recopilar información confidencial de los usuarios.
- Mensajes con ‘Subject’: “Alerta de Acceso Autenticado”; “Entrada confirmada: nueva solicitud”

Es importante reiterar que la Universidad de Puerto Rico no cancela cuentas institucionales ni solicita información de acceso**,** tales como contraseñas, respuestas a preguntas de seguridad o códigos de autenticación, ni por correo electrónico, ni por llamadas telefónicas, ni por mensajes de texto**.**

Las comunicaciones recibidas, así como los incidentes reportados, han sido referidos al personal encargado de seguridad de la Oficina de Sistemas de Información de la Administración Central para su análisis, investigación y manejo conforme a los protocolos institucionales.

División de Tecnologías Académicas y Administrativas
6 Ave. Universidad STE 601, San Juan, Puerto Rico, 00925-2526
Tel. (787) 764-0000 ext. 83800
Fax. 787-764-2755

CIRCULAR NUM. 1 2026-2027
A TODA LA COMUNIDAD UNIVERSITARIA
23 de julio de 2026

Como medidas cautelares, se ejecutaron las siguientes acciones de seguridad:

- Eliminación de los mensajes identificados de los buzones de correo.
- Implementación de políticas de filtrado basadas en los patrones observados en el "subject" y las URLs.
- Restablecimiento de contraseñas (password reset) en las cuentas afectadas.

Exhortamos enfáticamente a toda la comunidad universitaria a:

- Nunca compartir sus contraseñas**,** respuestas a preguntas de seguridad ni códigos de autenticación.
- No completar formularios ni acceder a enlaces contenidos en correos sospechosos.
- Reportar cualquier mensaje similar directamente desde la aplicación de correo electrónico institucional (Outlook) utilizando la opción de "junk" o "phishing"**.**
- Proteger su seguridad digital y no atender este tipo de correos**.**

Si usted completó algún formulario asociado a uno de estos correos fraudulentos, le recomendamos acceder de inmediato al portal institucional Portal UPR y utilizar el mecanismo de "Olvidé mi contraseña" para realizar el cambio correspondiente. Este proceso permitirá que la nueva contraseña se propague a todas las plataformas institucionales.

Este aviso se emite conforme a la Política Institucional sobre el Uso y Acceso a los Recursos de la Tecnología de la Información, aprobada mediante la Certificación Núm. 85 (2022-2023) de la Junta de Gobierno de la Universidad de Puerto Rico, la cual establece la responsabilidad de todos los usuarios de:

- Proteger la seguridad, integridad y confidencialidad de los recursos tecnológicos institucionales.
- Utilizar los sistemas de información de forma ética, responsable y segura.
- Reportar posibles incidentes o violaciones de seguridad a las entidades correspondientes.

Para información adicional y recursos educativos sobre cómo evitar ser víctima de fraude electrónico, le recomendamos visitar el Portal de Seguridad de la Tecnologia de Informacion de la Universidad de Puerto Rico.

Para asistencia técnica, puede efectuar una orden de servicio en: Mesa de Ayuda de la DTAA