**UNIVERSIDAD INTERAMERICANA DE PUERTO RICO**
**RECINTO DE SAN GERMÁN**
**Centro de Informática y Telecomunicaciones**

A los usuarios de sistemas informáticos

P/C: José Luis Colón González, Ph.D.
Rector

Rogelio Toro Zapata
Director

## Campaña de Concientización: Seguridad en el Correo Electrónico

El correo electrónico ha sido la principal herramienta de comunicación en la universidad durante más de dos décadas. Diariamente se reciben y envían numerosos correos electrónicos con información oficial de índole académica y administrativa, lo que representa una oportunidad de ataque para los delincuentes cibernéticos (hackers).

Los ciberdelincuentes atacan el correo electrónico porque constituye un punto de entrada relativamente sencillo a otros dispositivos y cuentas, y porque muchos de sus ataques se basan en el engaño, el error humano y la ingeniería social. Una sola acción equivocada podría provocar un incidente de seguridad. Las consecuencias de una brecha o ataque mediante el correo electrónico podrían incluir pérdida de datos, interrupción de procesos y daños a la reputación institucional, particularmente si se envían mensajes con contenido inapropiado o se compromete información confidencial.

Para salvaguardar la seguridad del correo electrónico, contamos con métodos de autenticación y herramientas de protección contra amenazas, tales como malware, ransomware, correo no deseado (spam) y phishing. Sin embargo, es responsabilidad de todos permanecer alerta, ya que estos ataques evolucionan constantemente y pueden llegar a superar las medidas de seguridad establecidas.

**Precauciones a tomar:**

1. Si recibe un correo electrónico que le solicita hacer clic en un enlace para proporcionar información personal o institucional, lo primero que debe verificar es la dirección de correo del remitente. Pregúntese: ¿Es una dirección válida? ¿La conoce? ¿Espera recibir un correo de esa dirección?
   Es importante actuar con cautela, ya que algunos mensajes utilizan direcciones que aparentan ser legítimas o incluso institucionales, incluyendo dominios similares a @intersg.edu.

2. En muchas ocasiones, los mensajes aparentan provenir de grandes empresas como Amazon, eBay, PayPal o Facebook, entre otras, y solicitan información personal, especialmente nombres de usuario y contraseñas.

3. Es común que la dirección del remitente contenga una letra, número o carácter diferente al legítimo, lo que la convierte en una dirección sospechosa.
   Ejemplos: sales@amaz0n.com support@facebook.com.rus ,http://microsoft.com.kor/phP
   Antes de hacer clic en cualquier enlace, coloque el cursor del mouse sobre la dirección o URL (sin hacer clic) y observe cuidadosamente el destino. Es posible que parezca una dirección legítima, pero que incluya caracteres, abreviaturas o dominios desconocidos.

4. Nunca abra un archivo adjunto (*attachment*) proveniente de un correo electrónico que no espera recibir o cuyo origen desconoce.

5. Nunca abra archivos adjuntos con extensiones como .zip, .vbs, .exe o .bat, aunque conozca al remitente y disponga de un programa antivirus.

6. Si necesita enviar un documento confidencial por correo electrónico, procure protegerlo mediante cifrado (encriptarlo) o contraseña y comunique la clave al destinatario utilizando un medio alterno. Si no es posible proteger adecuadamente el documento, evalúe utilizar otros métodos seguros autorizados por la institución.

7. Preste atención al asunto (*subject*) del mensaje. Frases como: *Dear Customer, Hi There, Hello Dear, Urgent Request, Action Required, Respond Immediately* buscan crear una sensación de urgencia para inducirle a actuar sin analizar cuidadosamente el mensaje.

8. Mantenga una actitud crítica ante cualquier correo electrónico que solicite información confidencial, transferencias de dinero o decisiones importantes, incluso cuando provenga de una dirección conocida.
   Por ejemplo, una asistente administrativa podría recibir un mensaje aparentemente enviado por el director ejecutivo de una empresa solicitando una transferencia urgente de fondos. Antes de realizar cualquier acción, debe validar la solicitud mediante una llamada telefónica u otro medio confiable, ya que la cuenta de correo del remitente podría haber sido comprometida.

9. Utilice contraseñas robustas que no incluyan nombres de familiares, mascotas o información personal fácilmente identificable. Además, mantenga habilitada la autenticación multifactor (Multi-Factor Authentication – MFA), la cual continúa siendo un requisito de seguridad para los usuarios.

10. La recomendación principal es utilizar el sentido común y mantener una actitud de sana desconfianza. Pregúntese: ¿Realmente esperaba este correo electrónico? ¿Esperaba este archivo adjunto? ¿Solicité algún servicio a esta empresa? ¿Tiene sentido esta solicitud?

11. No comparta contraseñas con ninguna persona.

12. No apruebe solicitudes inesperadas de autenticación multifactor (MFA).

13. Mantenga el sistema operativo y las aplicaciones actualizadas.

14. Reporte inmediatamente cualquier incidente o sospecha de compromiso de cuenta

**¿Qué hacer si recibe un correo sospechoso?**

1. Reenvíelo a tecnicos@intersg.edu

2. En el asunto (subject) escriba: Correo sospechoso para revisión.

3. Bloquee al remitente. Haga clic con el botón derecho sobre el mensaje y seleccione la opción Block o Block Sender. Esto eliminará el mensaje y agregará la dirección del remitente a una lista de bloqueo, de manera que futuros mensajes sean dirigidos automáticamente a la carpeta **Junk Email** (Correo no deseado).

Cualquier dato adicional, no dude en comunicarse con: tecnicos@intersg.edu, 787-264-1912, exts. 7103, 7674, 7675