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

A todos los usuarios de sistemas informáticos

P/C: Vilma S. Martínez
Rectora Interina

## Campaña de concientización: seguridad en el correo electrónico

El correo electrónico ha sido la herramienta de comunicación principal en la universidad durante más de dos décadas. Diariamente se reciben y envían una cantidad considerable de correos electrónicos con información oficial de índole académica y/o gerencial, lo cual representa una oportunidad de ataque para los delincuentes cibernéticos (hackers). Los hackers atacan el correo electrónico porque es un punto de entrada fácil a otros dispositivos y cuentas; y se basa, en gran parte, en el engaño, error humano y la ingeniería social. Solo se necesitaría una pulsación equivocada para provocar una crisis de seguridad. Las consecuencias de una brecha o ataque por medio del correo electrónico podrían provocar al recinto pérdida de datos, interrupción en procesos y daños a la reputación, ya que podrían salir correos electrónicos con contenido no apropiado.

Para salvaguardar la seguridad del correo electrónico, contamos con métodos de autenticación y herramientas para protegernos contra amenazas, tales como, los ataques de *malware*, *ransomware*, correo no deseado y phishing. Sin embargo, es nuestra responsabilidad estar atentos, ya que el ritmo y grado de sofisticación de estos esquemas de ataque podrían atravesar el perímetro de seguridad.

**Precauciones a tomar:**

1. Si recibe un correo electrónico solicitando hacer *click* en un enlace que le solicita información, la primera sospecha debe ser la dirección de email de quien lo envía: ¿Es una dirección válida? ¿La conoce? ¿Espera un email de esa dirección? Es importante tener **mucha precaución**, ya que en ocasiones salen con direcciones que parecen ser conocidas o del recinto, al tener @intersg.edu.

2. En muchas ocasiones, serán lo que aparenta ser direcciones de grandes empresas como Amazon, Ebay, Paypal, Facebook, entre otras; (en las que quizás usted está afiliada(o)) y están solicitando que provea información suya, sobre todo su *user* y *password* de ese servicio o empresa.

3. Es muy probable que la dirección de la empresa tenga alguna letra o número incorrecto, lo cual la convierte en una dirección sospechosa. Ejemplo sales@amaz0n.com o support@facebook.com.rus Una revisión importante que debe hacer es poner el puntero del mouse sobre el enlace (NO click) o url y observar la dirección. Probablemente verá una dirección similar a una empresa conocida, pero contiene alguna letra, carácter o abreviatura que no es familiar. Ejemplo: http://microsoft.com.kor/php

4. Nunca abra un *attachment* de un correo que usted no espera, ni conoce su origen.

5. Nunca abra un *attachment* de un correo que tenga las extensiones .zip, .vbs, .exe, .bat (aunque conozca la dirección y tenga antivirus).

6. Si necesita enviar un documento confidencial por email, primero debe encriptarlo y notificar al destinatario la clave para desactivarlo. De no poder hacer dicho proceso, se recomienda lo envíe vía Fax.

7. Esté pendiente de los asuntos o *subjects*, tales como, ***Dear customer, Hi there, Hello dear***. Un *subject* como: ***Urgent request, Action required, Respond inmediatelly*** los cuales implican urgencia e incitan a que usted, inconscientemente, acceda a lo que solicita el email.

8. Este atento cuando reciba un email (aunque sea de una dirección conocida) con una solicitud sensitiva, sobre todo si se trata de dinero, información confidencial o decisiones sensitivas. Ejemplo: una asistente administrativa recibe un email del CEO de una empresa (quien está fuera de la oficina) solicitando transferir gran cantidad de fondos con urgencia para procesar una transacción. Como la solicitud es tan inusual e implica una cantidad sustancial de dinero, la persona llama al CEO para validar y se encuentra con la sorpresa que la cuenta de email del CEO fue atacada (hackeada).

9. Use una contraseña compleja y que no contenga nombres de sus familiares o mascotas. Se recomienda que la cambie cada cuatro meses. Se mantendrá siempre la doble autenticación *(Multifactor Authentication)* de los usuarios.

10. La idea central: **use el sentido común y no confíe**. ¿En realidad está esperando ese email? ¿Está esperando ese *attachment*? ¿Solicitó algún servicio a esa empresa?

**¿Qué hacer?**
Si recibe un email sospechoso:

1. Darle forward a: tecnicos@intersg.edu, en el asunto o subject escribirá *email sospechoso para revisión.*

2. Marcarlo con el botón derecho y en el menú seleccionar Block y Block Sender. Eso borrará el mensaje y pondrá la dirección de procedencia en una lista negra, que en el futuro redireccionará los mensajes a la carpeta ***Junk Email***

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

Rogelio Toro Zapata
Director
Centro de Informática y Telecomunicaciones