QUE ES EL PHISHING

El Phishing es uno de los métodos más utilizados por delincuentes cibernéticos para **estafar y obtener información confidencial de forma fraudulenta**. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que **suplanta la identidad de una persona u organización de confianza.**

Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un **mensaje pensado para asustarle** que exige que **vaya a un sitio web o tendrá que afrontar alguna consecuencia.**

Tipos de ataques de phishing

Todos tiene en común el uso de un **pretexto fraudulento para adquirir datos valiosos**.

- Envían correos electrónicos masivos al mayor número posible de personas. Ese es el caso de los que recibimos **sobre el correo, que suplantan a la Uva.** Suelen ser mensajes como estos: **"el correo está lleno", "ha excedido la cuota de correo", "la cuenta de correo está bloqueada", "la cuenta de correo se inactivará"** y nos piden que pulsemos en un enlace para **reactivar la cuenta de correo, validarla o aumentar la cuota amenazándonos con bloquearnos la cuenta de correo**.

  Ese mismo correo lo podemos recibir, por ejemplo, de un Banco, intentando que les facilitemos los números de cuentas corrientes, número de tarjeta, pin de tarjeta.

- Phishing que **ataca a una persona u organización específica.** Hacen búsqueda en Internet de nombres, cargos, direcciones de correo electrónico y similares. Con esto, el autor del phishing **crea un correo electrónico creíble.**

- Phishing de clonación: Hacen una **copia de correos electrónicos legítimos enviados anteriormente que contienen un enlace o un archivo adjunto**. Sustituyen los enlaces o archivos adjuntos por otros con contenido malicioso disfrazado para hacerse pasar por el auténtico. Al hacer clic en el enlace o abrir el adjunto, los delincuentes pueden tomar el control de Pc. Luego el autor del phishing puede falsificar la identidad de la víctima.

  Este caso también lo hemos tenido en la Uva hace poco, recibíamos correos de personas de la Uva, Servicios Centrales, Rectorado, Vicerrectorado……que habían clonado correos legítimos.

- Phishing telefónico: Llaman afirmando representar a su banco, la policía o incluso la Agencia Tributaria. A continuación, le asustan con algún tipo de problema e insisten en que lo solucione inmediatamente facilitando su información de cuenta o pagando una multa.

  Esta misma estafa puede hacerse vía SMS o Wasap, algunas veces con un enlace malicioso incorporado en el que hacer clic.

- En algunos casos suplantan alguna Organización y **nos piden dinero** (los phishing que se hacen pasar por Correos para que paguemos para validar un paquete)

CONSEJOS Y RECOMENDACIONES

No siempre es sencillo, pero algunos **consejos, disciplina y sentido común** nos ayudarán.

- Nota **algo raro** o inusual en el correo recibido.

- El mensaje está **mal redactado**, mal traducido o, directamente, tiene palabras en otros idiomas sin venir a cuento, si no hay concordancia gramatical de género y número, etc.

1. El correo electrónico hace una **oferta** que parece demasiado buena para ser verdad.

2. Desconfíe de mensajes de correo en los que con cualquier excusa se le **pida introducir datos personales suyos** o acceder a una página web donde se les pidan.

3. Desconfíe de **correos electrónicos no solicitados** que incluyan adjuntos, ya que éstos pueden contener código malicioso.

4. En la medida de lo posible **nunca acceda a enlaces que aparezcan en mensajes de correo** porque puede ser que no lleven donde parece. **Si pasamos el cursor del ratón por encima del enlace**, sin hacer clic en él, en la parte inferior izquierda de la ventana de la aplicación que estemos manejando (tanto navegador web como cliente de correo electrónico) **aparecerá la URL real**.

   En el caso de móviles y tablets se puede dejar el dedo pulsado en el enlace y darle a la opción de "copiar", pegándolo luego en cualquier aplicación de texto (por ejemplo, aplicación de Notas, Word, etc.) pero no en el navegador, por supuesto.

   Si quiere acceder a una **página de una organización** (ya sea UVa, entidad bancaria, otra organización), **hágalo directamente desde su página web**.

5. El mensaje es de alguien conocido, pero no lo esperábamos, es posible que esté **falseado el remitente**, en algunos casos, si ponemos el cursor sobre el remitente nos puede mostrar el remitente real.

LA UVA LE RECUERDA

1. **La UVa NUNCA LE PEDIRA POR CORREO SUS DATOS DE USUARIO NI QUE ACCEDA A PAGINAS WEB PARA INTRODUCIRLOS POR SUPUESTOS "PROBLEMAS"**.

2. Nadie nos va a enviar un **mensaje institucional desde una cuenta de otro país.**

3. Si tiene **dudas sobre un mensaje**, contacte con el personal informático del centro informatica.economicas@uva.es o con el CAU de la UVA soporte@uva.es tel: 983-184000

4. Si nos llega un **mensaje de una, aparentemente, cuenta UVa** y algo nos hace sospechar (tipo de mensaje, tipo de enlace, mala redacción, imagen corporativa mal utilizada, etc.) siempre podemos buscar en el directorio UVa y comprobar los datos de esa persona y llamarla para preguntar.

   Hace unos meses llegaron unos correos con un fichero adjunto y el texto "te envío el documento que me pediste", de una dirección conocida. Este virus empezó a reenviar masivamente correos infectados por toda la Uva.

5. **Si hemos "picado**" y hemos dado contraseñas lo que hay que hacer es cambiarlas rápidamente.

   La contraseña de la Uva se cambia en Mi Portal UVa (miportal.uva.es) y nada más entrar, en "Mis Datos", en la tercera fila viene "Clave -> Cambiar clave": ponemos la clave actual una vez y la nueva dos veces, siguiendo las instrucciones sobre cómo debe ser esa contraseña.

   La contraseña de correos antiguos hay que enviar un correo a soporte@uva.es

6. También sería muy conveniente **pasar el antivirus.**