

# **CONSEJOS PARA PREVENIR ATAQUES DE PHISHING**

## **1. APRENDE A IDENTIFICAR CLARAMENTE LOS CORREOS ELECTRÓNICOS SOSPECHOSOS DE SER PHISHING**

Existen algunos aspectos que inequívocamente, identifican este tipo de ataques a través de correo electrónico:

- Utilizan nombres y adoptan la imagen de empresas reales
- Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa
- Incluyen webs que visualmente son iguales a las de empresas reales
- Como gancho utilizan regalos o la pérdida de la propia cuenta existente

## **2. VERIFICA LA FUENTE DE INFORMACIÓN DE TUS CORREOS ENTRANTES**

Tu banco nunca te pedirá que le envíes tus claves o datos personales por correo. Nunca respondas a este tipo de preguntas y si tienes una mínima duda, llama directamente a tu banco para aclararlo.

## **3. NUNCA ENTRES EN LA WEB DE TU BANCO PULSANDO EN LINKS INCLUIDOS EN CORREOS ELECTRÓNICOS**

No hagas clic en los hipervínculos o enlaces que te adjunten en el correo, ya que de forma oculta te podrían dirigir a una web fraudulenta.

Teclea directamente la dirección web en tu navegador o utiliza marcadores/favoritos si quieres ir más rápido.

## **4. REFUERZA LA SEGURIDAD DE TU COMPUTADORA**

El sentido común y la prudencia es tan indispensable como mantener tu equipo protegido con un buen antivirus que bloquee este tipo de ataques. Además, siempre debes tener actualizado tu sistema operativo y navegadores web.

## **5. INTRODUCE TUS DATOS CONFIDENCIALES ÚNICAMENTE EN WEBS SEGURAS**

Las webs seguras han de empezar por 'https://' y debe aparecer en tu navegador el icono de un pequeño candado cerrado.

## **6. REVISA PERIÓDICAMENTE TUS CUENTAS**

Nunca está de más revisar tus cuentas bancarias de forma periódica, para estar al tanto de cualquier irregularidad en tus transacciones online.

## **7. NO SÓLO DE BANCA ONLINE VIVE EL PHISHING**

La mayor parte de ataques de phishing van contra entidades bancarias, pero en realidad pueden utilizar cualquier otra web popular del momento como gancho para robar datos personales: eBay, Facebook, Pay Pal, etc.

### **8. EL PHISHING SABE IDIOMAS**

El phishing no conoce fronteras y pueden llegarte ataques en cualquier idioma. Por norma general están mal escritos o traducidos, así que este puede ser otro indicador de que algo no va bien.

Si nunca entras a la web en inglés de tu banco, ¿Por qué ahora debe llegarte un comunicado suyo en este idioma?

### **9. ANTE LA MÍNIMA DUDA SE PRUDENTE Y NO TE ARRIESGUES**

La mejor forma de acertar siempre es rechazar de forma sistemática cualquier correo electrónico o comunicado que incida en que facilites datos confidenciales.

Elimina este tipo de correos y llama a tu entidad bancaria para aclarar cualquier duda.