PHISHING

El **PHISHING** es uno de los métodos de ingeniería social (ganar confianza para obtener información sensible) más utilizados por ciberdelincuentes para estafar y obtener información confidencial como contraseñas o información bancaria.

Este tipo de ataques se ha convertido en una de las principales amenazas que acechan a las instituciones y empresas.

LOS RIESGOS derivados de estas técnicas son el robo de identidad y datos confidenciales, pérdida de productividad y consumo de recursos de las redes corporativas. Los métodos utilizados para la realización del **PHISHING** incluyen SMS **(SMISHING)**, telefonía IP **(VISHING)**, Redes sociales, entre otros.

Para evitar estos riesgos es recomendable adoptar buenas prácticas, principalmente en el **USO DEL CORREO ELECTRÓNICO**.

- **No brinde información confidencial a terceros.**
- **Verifique la procedencia de la información recibida por correo electrónico, preste atención a la redacción de los mensajes y sospeche si existen expresiones sin sentido y errores ortográficos o gramaticales. Póngase en contacto con el remitente por otra vía en caso de que lo considere necesario, por ejemplo: entidades financieras, instituciones estatales, entre otros.**
- **Instale un antivirus para proteger su equipo de códigos maliciosos.**
- **Infórmese periódicamente sobre las últimas noticias de seguridad en el ci.ucr.ac.cr/ciberseguridad.**
- **Desconfíe si le ofrecen regalías por correo electrónico y comuníquelo inmediatamente al correo ci5000@ucr.ac.cr del Centro de Informática.**

UCR

PHISHING

El **PHISHING** es uno de los métodos de ingeniería social (ganar confianza para obtener información sensible) más utilizados por ciberdelincuentes para estafar y obtener información confidencial como contraseñas o información bancaria.

Este tipo de ataques se ha convertido en una de las principales amenazas que acechan a las instituciones y empresas.

LOS RIESGOS derivados de estas técnicas son el robo de identidad y datos confidenciales, pérdida de productividad y consumo de recursos de las redes corporativas. Los métodos utilizados para la realización del **PHISHING** incluyen SMS **(SMISHING)**, telefonía IP **(VISHING)**, Redes sociales, entre otros.

Para evitar estos riesgos es recomendable adoptar buenas prácticas, principalmente en el **USO DEL CORREO ELECTRÓNICO**.

- **No brinde información confidencial a terceros.**
- **Verifique la procedencia de la información recibida por correo electrónico, preste atención a la redacción de los mensajes y sospeche si existen expresiones sin sentido y errores ortográficos o gramaticales. Póngase en contacto con el remitente por otra vía en caso de que lo considere necesario, por ejemplo: entidades financieras, instituciones estatales, entre otros.**
- **Instale un antivirus para proteger su equipo de códigos maliciosos.**
- **Infórmese periódicamente sobre las últimas noticias de seguridad en el ci.ucr.ac.cr/ciberseguridad.**
- **Desconfíe si le ofrecen regalías por correo electrónico y comuníquelo inmediatamente al correo ci5000@ucr.ac.cr del Centro de Informática.**

UCR

No proporcione información personal como cuenta bancaria, número de tarjeta de crédito y pin, clave de cajeros automáticos, número de cédula o número de teléfono, a menos que esté realmente pagando por productos o servicios a través de medios electrónicos confiables para el consumidor, tales como: tarjetas, plataformas de pago, transferencias bancarias entre otros.

Si ha sido víctima de un intento de "phishing" informe a la entidad suplantada y a las instituciones correspondientes.

EN LUGAR DE UTILIZAR LOS ENLACES incluidos en los correos electrónicos, escriba la dirección directamente en el navegador.

Antes de hacer clic en los vínculos incluidos en el mail, coloque el cursor sobre el vínculo y asegúrese de que la dirección url que aparece sea la misma que figura en el texto del vínculo.

Antes de introducir información confidencial en una página web **VERIFIQUE QUE SEA SEGURA:** debe empezar con https:// y tener un candado cerrado en el navegador.

No abra enlaces sospechosos que reciba a través de mensajes de texto , podrían redirigirlo a un sitio fraudulento.

EL SMISHING es un nuevo tipo de delito o actividad criminal a base de técnicas de ingeniería social con mensajes de texto **DIRIGIDOS A LOS USUARIOS DE TELEFONÍA MÓVIL**. El sistema emisor de estos mensajes intentará suplantar la identidad de alguna persona conocida de entre nuestros contactos, o incluso a una empresa de confianza. Las víctimas de smishing reciben mensajes SMS similares a este:

"Estamos confirmando que se ha dado de alta para un servicio de citas. Se le cobrará 2 dólares al día a menos que cancele su petición: www.??.com".

EL VISHING o el uso delictivo del teléfono se realiza a través de una llamada telefónica que simula proceder de una entidad bancaria solicitándole verificar una serie de datos. Evite brindar sus datos personales a través de llamadas telefónicas sospechosas.

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
CI
Centro de **Informática**

No proporcione información personal como cuenta bancaria, número de tarjeta de crédito y pin, clave de cajeros automáticos, número de cédula o número de teléfono, a menos que esté realmente pagando por productos o servicios a través de medios electrónicos confiables para el consumidor, tales como: tarjetas, plataformas de pago, transferencias bancarias entre otros.

Si ha sido víctima de un intento de "phishing" informe a la entidad suplantada y a las instituciones correspondientes.

EN LUGAR DE UTILIZAR LOS ENLACES incluidos en los correos electrónicos, escriba la dirección directamente en el navegador.

Antes de hacer clic en los vínculos incluidos en el mail, coloque el cursor sobre el vínculo y asegúrese de que la dirección url que aparece sea la misma que figura en el texto del vínculo.

Antes de introducir información confidencial en una página web **VERIFIQUE QUE SEA SEGURA:** debe empezar con https:// y tener un candado cerrado en el navegador.

No abra enlaces sospechosos que reciba a través de mensajes de texto , podrían redirigirlo a un sitio fraudulento.

EL SMISHING es un nuevo tipo de delito o actividad criminal a base de técnicas de ingeniería social con mensajes de texto **DIRIGIDOS A LOS USUARIOS DE TELEFONÍA MÓVIL**. El sistema emisor de estos mensajes intentará suplantar la identidad de alguna persona conocida de entre nuestros contactos, o incluso a una empresa de confianza. Las víctimas de smishing reciben mensajes SMS similares a este:

"Estamos confirmando que se ha dado de alta para un servicio de citas. Se le cobrará 2 dólares al día a menos que cancele su petición: www.??.com".

EL VISHING o el uso delictivo del teléfono se realiza a través de una llamada telefónica que simula proceder de una entidad bancaria solicitándole verificar una serie de datos. Evite brindar sus datos personales a través de llamadas telefónicas sospechosas.

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
CI
Centro de **Informática**