

FACUA alerta de una campaña de 'phishing' que suplanta a Carrefour Pass para robar información personal

FACUA-Consumidores en Acción alerta de una nueva campaña de *phishing* que se hace pasar por el servicio financiero Carrefour Pass para hacerse con los datos personales de los usuarios. Las víctimas, todas ellas en posesión de esta tarjeta de crédito, reciben un correo electrónico que simula la necesidad de actualización de los datos proporcionados a la empresa para que pueda seguir usando los servicios contratados con ellos.

La Oficina de Seguridad del Internauta, dependiente del Ministerio de Energía, Turismo y Agenda Digital, recoge este aviso en su sección de alertas de seguridad con fecha de este 29 de mayo. Bajo el asunto "*nueva actualización*" o "*Carrefour Servicios Financieros*", el mensaje fraudulento informa al usuario de que debe actualizar sus datos para seguir usando el servicio. Para ello le pide pulsar en un enlace y seguir las instrucciones en la página web a la que redirige.

Al introducir cualquier dato y seleccionar el botón "*Entrar*" en esta web se cargará una nueva página en la que se solicitarán los datos de la tarjeta de crédito del usuario. Una vez introducida la información, éste es redirigido para validar el pago de una compra que no ha realizado, para lo que se pide que facilite el nombre y apellidos, fecha de nacimiento y DNI.

Por último, pide a la víctima que elija una pregunta y una respuesta que servirán supuestamente "*para modificar su número de teléfono móvil en caso necesario*". Cuando el usuario ha finalizado todos estos pasos es redirigido a la web real de Carrefour.

Recomendaciones para evitar el engaño

Uno de los elementos que deben hacer sospechar a los usuarios que reciban este correo es la cantidad de errores gramaticales que contiene, así como la dirección remitente del texto, que no se corresponde con un dominio de Carrefour, algo que no encaja en este tipo de comunicaciones corporativas.

Si la víctima ha caído por completo en el engaño y ha facilitado todos sus datos, debe ponerse en contacto con Carrefour Pass para comunicarle lo sucedido. En caso de tener algún cargo en la tarjeta de crédito que no se ha realizado, el usuario debe contactar con su entidad bancaria.

Para evitar ser víctima de este tipo de fraudes tipo *phishing*, no deben abrirse los correos de usuarios desconocidos o que no se hayan solicitado. En el caso de abrirlos, nunca se deben contestar ni enviar cualquier tipo de información personal.

Además, se debe tener precaución ante cualquier tipo de enlace o descarga de ficheros adjuntos en correos, SMS o mensajes en redes sociales. Para estar más protegido, es importante tener un sistema operativo actualizado y antivirus.