Los piratas informáticos cada vez buscan nuevas formas de atacar a los usuarios. Lo que habitualmente buscan es obtener datos e información personal que posteriormente venden en el mercado negro. En esta ocasión, el objetivo del 'hacker' ha sido algo más concreto.

En 2007, según informa el portal *Audiencia Electrónica*, un desarrollador llamado Naoki Hiroshima registró la cuenta de Twitter '@N', muy buscada y codiciada por un gran número de usuarios. Aquí comenzaron sus problemas. Consejos para hacer un buen uso de Twitter.

Desde entonces, este informático ha recibido diversas ofertas de empresas y desarrolladoras (que ofrecían por la cuenta más de 50.000 dólares), hasta amenazas e intentos de cambios de contraseña que, finalmente, no llegaban a realizarse. Twitter y las grandes marcas, el inicio de una historia de amor en siete tuits.

Pero un mal día le llegó un correo desde el hosting GoDaddy, donde este tenía alojadas sus páginas web y su dominio de correo electrónico dueño del usuario '@N'. En el mail se le notificaba que sus datos habían sido modificados, por lo que no podía verificar que realmente él era el dueño de dichas páginas ni de dicho correo.

Después de eso, el desarrollador se dio cuenta de que el objetivo era su cuenta de Twitter, por lo que intentó cambiar el correo electrónico asociado. Demasiado tarde, el pirata ya tenía acceso a su cuenta de correo electrónico y a su cuenta de Facebook.

La amenaza

A continuación, según detalla el portal, el pirata informático contactó con Naoki y le amenazó con borrar todo el contenido alojado en su cuenta de GoDaddy si no le entregaba a cambio la

cuenta '@N'. Consejos para esquivar el espionaje en Internet.

Naoki Hiroshima no pudo hacer otra cosa que entregar su usuario al pirata para poder recuperar todos sus datos del hosting.

¿Cómo lo hizo?

El pirata informático ha confesado a la víctima su técnica. Al parecer, todo se debe a «ingeniería social», una técnica sencilla y efectiva.

El hacker ha explicado que se hizo pasar por un empleado cuando llamó al soporte de PayPal, y asegura que no fue difícil hacer que el agente le compartiera los últimos 4 dígitos de la tarjeta de crédito de la víctima, según *Qore*.

A continuación, contactó con GoDaddy que, con los datos de la tarjeta, pudo acceder rápidamente a todo el panel de administración de GoDaddy y, con ello, comenzar la extorsión a Naoki Hiroshima

PayPal se defiende

Tras conocerse la noticia en la que quedaban en evidencia las medidas preventivas de PayPal, la firma salió a defenderse. Aclararon que su personal está altamente entrenador para prevenir intentos de ingeniería social y que ya revisaron sus registros. Y, aunque admiten que hubo un intento fallido de obtención de datos, la compañía no divulgó información personal de Hiroshima.

El portal *Qore* también explica que la cuenta de la víctima no fue vulnerada, cosa que el mismo Hiroshima aclara, y que trabajarán con él para averiguar si pueden ayudar.

Twitter también tomó cartas en el asunto, pues la cuenta en cuestión ya no es accesible. De presentarse evidencias sólidas, existe la posibilidad de que Hiroshima recupere su nombre de usuario original.

Fuente: eleconomistaamerica