Skimming es el robo de información de tarjetas bancarias al momento de alguna transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para un posterior uso fraudulento. Se trata del copiado de la banda magnética.

Por lo general, el skimming se lleva a cabo en restaurantes, bares, gasolineras o cajeros automáticos, donde un cómplice criminar tiene en su posesión la tarjeta de la víctima para realizar algún cobro, sin que el dueño se percate, realiza una copia de la banda magnética con el simple hecho de pasar la tarjeta por un aparato.

En el caso del skimming en cajeros automáticos, el delincuente coloca un dispositivo y en ocasiones, acompañado de una microcámara para grabar el código PIN del usuario.

Se coloca un dispositivo en el cajero parecido al original, ya sea un teclado o un lector de tarjetas, en ocasiones ambos, mediante una carcasa completa sobre el cajero.

Cuando esto ocurre, el estafador siempre se encuentra a una distancia pequeña del cajero, para poder ir por sus aparatos y a información recopilada en cuanto una o pocas personas hayan utilizado el cajero.
Ante esto, han aparecido sistemas anti-skimming, que cifran o codifican la información que se encuentra en la banda magnética para evitar el fraude de clonación de tarjeta.

También, algunos fabricantes de cajeros han creado sistemas anti skimming, que permiten en algunos casos bloquear el ingreso de las tarjetas cuando detectan un dispositivo en la entrada del lector de tarjetas.

Algunos consejos para evitar esto son, en el caso de pago en comercios, nunca perder de vista la tarjeta, pedir al mesero que lleve la terminal a la mesa, o vigilar a quien realice el cobro, siempre teniendo a la vista la terminal y la tarjeta.

En el caso de los cajeros, verificar que el teclado y lector de tarjetas no se encuentre sobrepuesto, que no existan bordes separados o cualquier cosa fuera de lo normal.