

CARDING

Carding es la denominación actual que se ha dado al delito tecnológico en el cual se involucran fraudes con tarjetas de crédito.

Estos fraudes pueden darse o no a través de internet; telefónicamente usted puede ser víctima de ingeniería social (capacidad de una persona de convencer a otra a hacer algo indebido o reprochable a través de mecanismos verbales inconscientes o subyacentes) e ingenuamente dar su número de tarjeta de crédito para colaborar con, por ejemplo, la ONG "salvemos al oso panda" etc.

Si usted utiliza Internet nunca responda e-mails solicitando información de su tarjeta, las empresas emisoras de tarjetas de crédito hacen hincapié en que jamás le enviarán un email solicitándole el número de su tarjeta, fecha de expiración, etc. (esto se conoce como "Phishing" y encuadra a los delitos o fraudes relacionados con la captura de datos de tarjetas de crédito.

Estos emails normalmente son fraudulentos y simulan ser de las entidades crediticias. También es posible recibir estas comunicaciones telefónicamente. El argumento que suelen utilizar es que de no responder se perderían sus datos y, en algunos casos, que podrían ser canceladas sus cuentas.

Estos tipos de fraudes se producen a diario y por diferentes canales de comunicación. Existen en los diarios de grandes tiradas avisos falsos que ofrecen tentadoras ofertas similares "Gane plata sin moverse de su casa" los cuales poseen mecanismos posteriores que ponen en serio riesgo su seguridad financiera.

El fenómeno del Carding va de la mano con la ingeniería social, motivo por el cual es importante tomar en cuenta algunas recomendaciones:

Si recibe la TC en su domicilio constate que el sobre en que la recibe esté completamente cerrado y no presente indicios de haber sido abierto.

Firme su tarjeta al momento de recibirla.

Si usted debe destruir una TC expirada córtela en varios pedazos (destruyendo completamente la banda magnética) y tire los pedazos en diferentes cestos de basura.

Nunca lleve sus tarjetas de crédito en su cartera o maletín.

Nunca lleve todas sus tarjetas juntas, intente llevar sólo una o dos.

Guarde en su domicilio en un sitio seguro los números de sus tarjetas, fechas de vencimiento y números telefónico de denuncias por extravío, robo o hurto de las mismas.

No utilice claves triviales, intente crear claves difíciles de adivinar por terceros.

Al realizar compras con sus tarjetas de crédito nunca pierda de vista la misma.

Guarde los cupones y tickets de las compras.

Al recibir su resumen de cuenta controle inmediatamente las operaciones realizadas.

Nunca preste a otra persona su tarjeta (es ilegal prestarla y es ilegal que el comerciante venda a quien no es el titular de la tarjeta)

Nunca deje tickets o cupones abandonados en cualquier lugar (si verificó su resumen de cuenta y el mismo está bien, en todo caso, queme sus cupones y tickets)

Nunca escriba su número de tarjeta en algún papel que se pueda extraviar.

Nunca dé su número de tarjeta telefónicamente a menos que la empresa con quien hable sea de total confianza.

Evite proporcionar datos personales o confidenciales en centros comerciales, con el pretexto de hacerlo participar en sorteos o promociones de empresas o comercios de dudosa procedencia.

Si en algún comercio le solicitan una identificación al momento de hacer su compra, muéstrala, lo hacen como una medida para prevenir el mal uso de su TC.

Sea particularmente cuidadoso en lugares públicos.

QUE HACER EN CASO DE FRAUDE

Las Tarjetas de Crédito (TC) ofrecen protección contra el fraude desde el momento en que la TC es denunciada ante la entidad emisora. Esto no suele ocurrir con las Tarjetas de Débito (TB).

En caso de fraude o sospecha del mismo llame inmediatamente a la entidad emisora de su TC y bloquee su tarjeta.

Posteriormente debe informar por escrito a la entidad emisora de su TC comunicándole formalmente el robo de su tarjeta. Deberá constar el día de extravío, día que usted informó verbalmente de la pérdida y los datos de la tarjeta. También es prudente acompañar la misiva con la denuncia policial correspondiente.

Cuide la privacidad de sus claves secretas y evite compartirlas con terceros.

Nunca lleve escrito el número de clave de seguridad, debe memorizarlo.

Consulte en la entidad emisora de su tarjeta por los procedimientos en caso de robo o extravío de la misma (teléfonos, horarios de atención, procedimientos por denuncias, etc)

Si quiere limitar su riesgo informe por escrito inmediatamente.

CAJEROS AUTOMÁTICOS

Si se encuentra en un cajero automático, respete la distancia con quien se encuentra delante de usted operando en el mismo, es importante la privacidad de cada usuario.

No ingrese su clave personal cerca de terceros o extraños.

Cuente su dinero discretamente.

Una vez retirado el dinero y la tarjeta espere a que la pantalla del mismo se reinicie.

Lléve consigo los comprobantes que emite el cajero automático. Los mismos contienen información que puede ser usada en su perjuicio.

Si el cajero automático retiene su tarjeta dé aviso inmediatamente a la entidad emisora a efectos de bloquear la misma.

MEDIDAS DE SEGURIDAD ANTE EL FRAUDE DE SUPLANTACION DE IDENTIDAD

No preste su tarjeta.

Usted es el responsable de todos los cargos que se cobren si prestó la misma.

Legalmente sólo usted puede usar la tarjeta con su nombre.

Usted no estará protegido contra el uso desautorizado del plástico si los cargos los hace alguien a quien usted le prestó la tarjeta a sabiendas, incluso familiares y amigos.

No dé su número de tarjeta telefónicamente o por e-mail excepto que esté realmente seguro de quien es su interlocutor o de que pertenezca a una empresa en quien usted confíe.

Verifique siempre y cuidadosamente las operaciones en su resumen de cuenta.

Asegúrese de saber quién tiene acceso a sus tarjetas. Si se utilizan sin su consentimiento, es probable que tenga que pagar las compras de todas formas.

Luciano Salellas
Auditor en Seguridad Informática
<http://www.sr-hadden.com.ar>