Fraude em pagamentos com cartão

Medidas de Prevenção

05- Unidade de Moeda Falsa e de Cibercriminalidade

Haia, 11-04-2012

Este alerta da Europol destina-se a reforçar a prevenção e a sensibilizar para a utilização correta de todos os tipos de cartões de pagamento, tanto *online* como presencialmente.

Para divulgação pública
Nível de classificação: pública
Versão 2012041103

FRAUDE EM PAGAMENTOS COM CARTÃO – MEDIDAS DE PREVENÇÃO

Dado que todos os anos há muitas vítimas de fraude em pagamentos com cartões, a Europol reconhece a necessidade de informar o público sobre as medidas básicas de prevenção contra fraudes quando usar cartões para pagamento, quer sejam de débito, de crédito, pré-pagos – do tipo "MBNet" - ou outros.
Este folheto informativo visa evitar que os titulares de cartões de pagamento sejam vítimas de fraudes, especialmente durante os períodos de férias, quando é mais provável que as pessoas os usem em locais que nem sempre lhes são familiares, estando por isso mais vulneráveis a fraudes.
As seguintes recomendações diminuem o risco de se tornar uma vítima de fraude em pagamentos com cartão.

RECOMENDAÇÕES GERAIS

- Proteja os seus cartões e os respectivos dados.
- Quando fizer um pagamento com um cartão, nunca o perca de vista.
- Peça ao comerciante para confirmar o valor debitado no seu cartão.
- Não abandone e destrua cuidadosamente os recibos das transações efetuadas com o seu cartão. Rasgue todos os recibos e documentos que contenham informações relacionadas com os seus assuntos financeiros.
- Confira cuidadosamente os seus recibos com os seus extratos. Se verificar alguma transação que não lhe seja familiar contacte imediatamente o seu banco.
- Nunca escreva o seu PIN e nunca o revele a terceiros, mesmo que lhe digam que se trata do seu banco, empresa emissora do cartão ou polícia.
- Não guarde o seu livro de cheques juntamente com os cartões.
- Assine os novos cartões logo que os receba.
- Corte em vários pedaços pela banda magnética e/ou chip os cartões caducados/não utilizados/bloqueados logo que receba os novos cartões. Desfaça-se dos pedaços em locais diferentes (i.e. em recipientes diferentes ou uns pedaços em casa e outros no local de trabalho).
- Não deixe os seus cartões em malas, pastas ou bolsos de casacos sem vigilância em locais públicos e mantenha sempre os seus pertences consigo.
- Quando fizer transações *online*, assegure-se de que está a usar um software antivírus e um sistema operativo atualizados.
- Alternativas que evitam a exposição do seu cartão serão o uso de sistemas tipo Pay-Pal, iDeal, cartões pré-pagos – do tipo "MBNet" - ou o serviço *online banking* no pagamento de bens ou serviços.

Caixas Multibanco (ATM)

- Mantenha-se atento a pessoas que estejam à sua volta. Se alguém o estiver a observar, a comportar-se de forma suspeita ou a incomodá-lo, dirija-se a outro ATM. Não se distraia com desconhecidos durante a transação.
- Se detetar alguma coisa de anormal no ATM, peças soltas (teclado, ecrã, e ranhura de entrada do cartão) ou se houver vestígios de manipulação, não utilize essa máquina e informe imediatamente o banco ou a polícia.
- Mantenha-se muito próximo da caixa multibanco. Encubra sempre o teclado com a mão livre e com o corpo para evitar que alguém o veja a inserir o PIN.
- Se o ATM não devolver o seu cartão, participe imediatamente o extravio ao seu banco.

Terminais de Pagamento (TPA)

O skimming ("*clonagem*" do cartão) pode ocorrer em estabelecimentos comerciais, em especial em bares, restaurantes, máquinas de pagamento de estacionamento e postos de combustível com pagamento automático na bomba.

- Nunca perca de vista (e, se possível, nunca largue) o seu cartão durante as transações de pagamento.
- Insista para que o cartão fique sempre dentro do seu campo de visão.

Viagens (Hotéis, bares, restaurantes)

Se estiver alojado num hotel, é prática comum que lhe peçam o seu cartão de crédito para garantir o pagamento do quarto (e serviços). Deverá ser suficiente a indicação do número do cartão e o seu nome. No entanto, são, frequentemente, solicitados mais dados como procedimento padrão:

- Não permita que o comerciante fotocopie o verso do cartão (é suficiente fotocopiar a frente do mesmo). Isto evita as fraudes com o código de 3 dígitos no verso. Se, de qualquer forma, isso acontecer e não puder ser anulado, é de considerar a hipótese de bloquear o cartão imediatamente.
- Se o comerciante passar o cartão na máquina para o validar, pergunte-lhe o que é que acontece aos dados, quais os dados que são armazenados, como, onde e por quanto tempo. Se forem armazenados localmente num ficheiro de texto, isso deverá ser considerado um risco e poderá encarar a hipótese de bloquear o cartão. Se os dados forem armazenados encriptados ou num servidor remoto (i.e. sede), há um menor risco de os dados serem roubados/utilizados ilicitamente.
- Não digite o PIN do seu cartão senão no acto final de pagamento (sempre ocultando-o face a terceiros).
- Assegure-se que o cartão lhe é devolvido; não o entregue em "depósito". Embora existam cada vez mais bares e cafés a fazer isso, não é seguro [como alternativa poderá entregar um outro cartão (de débito) ou um cartão fictício].
- Não entregue o documento de identidade (i.e. passaporte, carta de condução) em "depósito". Pode entregar fotocópias destes documentos, mas apenas em alternativa aos dados do cartão de crédito, ou uma coisa ou outra. Disponibilizar os dois em conjunto aumenta o risco de fraude ou mesmo de usurpação de identidade. Em último recurso, peça que sejam destruídas as fotocópias ou que lhe sejam entregues após a sua saída.

- Se bem que raramente, alguns hotéis conservam os dados pessoais (incluindo dados do cartão de crédito) nas suas chaves/cartão eletrónicos. Uma vez que nunca consegue ter a certeza absoluta do que está armazenado nestes cartões, certifique-se que está sempre na posse do cartão durante a estadia e, ou guarda o cartão depois da sua estadia e o destrói (como acima descrito) ou assegura-se que os dados eletrónicos são devidamente apagados/eliminados/substituídos. Nunca deite fora cartões-chave usados em caixotes do lixo públicos.
- Quando entra num bar, café, restaurante ou clube, é cada vez mais frequente pedirem-lhe o seu cartão em "depósito" ao abrir a conta ou quando encomenda uma refeição. Isto obviamente não é seguro e como alternativa poderá entregar um outro cartão (de débito) ou um cartão fictício.

Em princípio, na maioria dos casos, estará protegido do uso indevido do seu cartão de pagamento (e do respetivo saldo). No entanto, o uso indevido ainda pode causar-lhe uma série de transtornos, quando bloqueado e a substituir. ***Mais vale prevenir do que remediar!***

Que fazer se, por infortúnio, for vítima de fraude com cartão de pagamento (ou furto de identidade)?

- Contactar imediatamente o banco ou empresa emissor para cancelar o(s) cartão(s) afetado(s) e bloquear imediatamente a(s) conta(s) associada(s).
- Se possível, tentar retirar/transferir todo o dinheiro da conta afetada.
- Se possível, tentar evitar que montantes mais avultados (por ex. salários) sejam depositados na(s) conta(s) afetadas).
- Participar às autoridades locais.
- Consultar regularmente as suas contas e comunicar ao banco transferências suspeitas. Em princípio, o prejuízo será reembolsado mas, por vezes, isso só acontece depois da averiguação interna estar concluída. Caso tenha de suportar custos (risco próprio) ou prejuízos, poderemos aconselhá-lo sobre a melhor forma de evitar que os mesmos lhe sejam cobrados.
- Consultar regularmente os seus relatórios de crédito para garantir que ninguém abriu novas contas bancárias em seu nome.