CRÓNICA VISÃO ELECTRÓNICA
Nº 448 / 2017-08-17
http://www.gestaodefraude.eu
Elisabete Maciel

>> Ingenuidade ou Insensatez?

Durante os últimos anos, os alertas na imprensa, nas instituições financeiras, ou mesmo nos nossos computadores pessoais, tem sido mais que muitos. Então, por que será que as fraudes informáticas se sucedem constantemente? Será que continuamos a cometer os mesmos erros ou será uma questão de atitude, assumindo que os alvos são sempre os outros? Será que estamos a esquecer as boas práticas no acesso à internet quando efetuamos operações bancárias e/ou pagamentos online?

No passado mês de junho, no âmbito da operação internacional "E-Commerce 2017", coordenada pela Europol e na qual participaram 26 países, Portugal incluído, foram detidos 76 indivíduos defraudadores profissionais e membros de redes criminosas que actuam na Internet.

Os suspeitos foram responsáveis por mais de 20 000 transações fraudulentas com cartões de crédito e cuja informação estava comprometida num valor superior a 5 milhões de euros. Dois dos detidos foram apanhados em Portugal em flagrante delito pela Unidade Nacional de Combate ao Cibercrime e à Criminalidade.

Hoje em dia, grande parte das transações via internet utiliza o cartão de crédito. Uma das fraudes com elevada prevalência associada a este tipo de transação é a do cartão não presente (CNP). É assim designada pois, para ser concretizada, não há como identificar o seu proprietário. Basta, sim, saber o número do cartão, a data de validade e o código de segurança. Qualquer defraudador na presença destes dados, os quais podem ser obtidos via phishing(1), por exemplo, poderá realizar uma ou mais transações antes da fraude ser detectada.

Verifica-se que este tipo de fraude tem vindo a crescer significativamente em países com elevados valores de transações por habitante (essencialmente nos EUA, na França, na Alemanha ou Reino Unido). Embora tenham sido implementadas medidas para a sua prevenção, nomeadamente o envio de um código por SMS para ser possível completar a transação, constata-se ainda assim um aumento significativo deste tipo de fraude. Tal justifica-se com

o crescimento exponencial das vendas pela internet e, mais do que isso, relaciona-se com o facto de as ferramentas de prevenção não estarem a ser integralmente adotadas por todas as partes envolvidas no processo. É de notar que uma transação deste tipo envolve vários intervenientes: o comprador/consumidor, o vendedor e a instituição financeira.

Não querendo menosprezar as responsabilidades das outras entidades envolvidas, quando o consumidor não conhece os mecanismos de prevenção de fraudes, põe em causa todo o processo. Ou seja, ignora o modo de como o seu comportamento coloca-o imediatamente em risco de ser defraudado.

Quais são então algumas das boas práticas a observar?

Antes de se ligar à Internet:

- Evite o uso de equipamentos públicos;
- Garanta que o equipamento está devidamente protegido (anti-virus, anti-spyware e firewall);
- Faça atualizações periódicas de todos os programas que protegem o computador.

Ao aceder à Internet:

- Não utilize palavras passe evidentes (data de nascimento, nome de parentes,…)
- Não abra e elimine de imediato mensagens de correio eletrónico de caráter duvidoso;
- Não clique em links e não faça downloads de fontes desconhecidas;
- Não digite dados confidenciais em sites cuja autenticidade não esteja garantida.

Ao efetuar uma compra:

- Nunca forneça os dados do seu cartão;
- Nunca envie o número PIN ou qualquer outro dado do cartão por correio eletrónico ou por chat;
- Evite fazer compras online em sites que não acomodam uma autenticação completa;

CRÓNICA VISÃO ELECTRÓNICA
Nº 448 / 2017-08-17
http://www.gestaodefraude.eu
Elisabete Maciel

- Verifique se a transferência está devidamente protegida (existência do símbolo cadeado na barra do endereço);
- Guarde todos os registos das operações realizadas.
- Não se esqueça de consultar com frequência a sua conta de forma a verificar os movimentos efetuados.

Ao observar estas regras na efetivação de operações através de internet, está a prevenir situações de fraude e a proteger-se contra o cibercrime.

NOTAS

1 Situação que se verifica quando alguém (hacker) se faz passar por uma empresa/instituição credível e, através de mensagem de correio eletrónico, tenta convencer um cliente bancário a divulgar informações pessoais, tais como passwords, números de contas bancárias, etc.