CRÓNICA VISÃO ELECTRÓNICA
Nº 459 / 2017-11-02
http://www.gestaodefraude.eu
Edgar Pimenta

>> Nem sempre o que parece é!

O ato de defraudar tem normalmente como objetivo final a obtenção de um benefício. Muitas vezes (diria mesmo a esmagadora maioria) o objetivo é monetário. A máxima *follow the money* (seguir o dinheiro) é frequentemente utilizada nas investigações de fraude pois é esse rastro que permite muitas vezes chegar ao ponto final da cadeia. E é também utilizada pelos defraudadores para procurar o elo mais fraco da sequência e aí atacar.

Um sítio óbvio onde o dinheiro reside é nos ATM, comummente designados de Multibanco. Durante anos, o dinheiro era guardado em cofres bancários onde existiam um conjunto elevado de controlos físicos para limitar o acesso ao dinheiro. Nos ATMs o acesso é aparentemente mais fácil: porque são equipamentos que estão em locais públicos, criam essa perceção. Contudo, são vários os controlos que tiveram de ser criados para os proteger. Desde o óbvio reforço do cofre onde o dinheiro reside, passado por vários sensores físicos que detetem alterações, até à inutilização das notas com tinta em caso limite.

Parecem equipamentos acessíveis mas não é bem assim.

Mas se por um lado foram implementadas medidas físicas para evitar o roubo, a verdade é que se veio criar novos vetores de ataque.

Cada ATM tem um computador para o controlar. E só isto diz muito. Sendo o computador o coração e o cérebro dos ATMs, é ele que controla todas as ações. Poderá então ser mais fácil fazer o ATM dar-nos o dinheiro do que levá-lo para casa?

Obviamente, esse computador do ATM está protegido de acesso físico. Não terá o mesmo nível de proteção do dinheiro, mas ainda assim com acesso não muito fácil. No entanto, foram já identificadas situações nas quais tal comunicação foi conseguida, tendo resultado em perdas financeiras (vulgo roubo).

Sendo o controlo efetuado por um computador, este também está sujeito a vulnerabilidades. Alguém que consiga aceder remotamente e controla-lo pode ordenar que sejam disponibilizadas as notas a um cúmplice que se encontre no exterior.

CRÓNICA VISÃO ELECTRÓNICA
Nº 459 / 2017-11-02
http://www.gestaodefraude.eu
Edgar Pimenta

Mas sem dúvida que o vetor mais comum e provavelmente o elo mais fraco somos nós, os utilizadores. Temos os cuidados mais básicos quando vamos levantar dinheiro?

É verdade que existem ameaças nas quais podemos ser ludibriados sem ter completa perceção disso. É o caso do *skimming*: a colocação de leitores de cartões sobreposto ao local onde introduzimos o cartão, permitindo fazer a leitura da banda do nosso cartão. Normalmente, quem coloca esses equipamentos falsos coloca igualmente uma câmara oculta ou um teclado falso para conseguir obter o PIN associado ao cartão.

Logo, a utilização de ATMs que pareçam ter sido adulterados deve ser sempre evitada. Uma proteção adicional muito simples é taparmos o teclado para que nem câmaras ocultas nem curiosos próximo de nós sejam capazes de obter o nosso código PIN.

Este pequeno gesto, seja quando levantamos dinheiro, seja quando fazemos pagamentos, é muita vezes ignorado.

Mas existem outras boas práticas que devem ser seguidas:

- Não escrever o PIN num post-it e guardá-lo junto dos cartões;
- Não usar o mesmo PIN em vários cartões;
- Não usar partes da data de nascimento (sobretudo quando se guarda o cartão de cidadão junto dos cartões bancários);
- Usar um PIN aleatório.

Pequenos gestos que nos podem poupar muitos dissabores.