CRÓNICA VISÃO ELECTRÓNICA
Nº 299 / 2014-10-09
http://www.gestaodefraude.eu
Edgar Pimenta

>> Quão diligentes somos a proteger o nosso dinheiro "eletrónico"?

O dinheiro, o nosso dinheiro, é cada vez menos "tangível", no sentido de que cada vez mais é tratado de forma digital. Embora o dinheiro esteja no mesmo sítio, os bancos, o acesso a esse mesmo dinheiro é feito de várias e diversas formas, sendo que o tradicional, através de um qualquer balcão físico, tenderá a ser dos mais reduzidos.

Vamos então ver como aceder à nossa informação bancária e quais os riscos que cada um desses acessos pode ter.

Multibanco

Provavelmente um dos acessos por meios eletrónicos mais comuns. Em termos de segurança, baseia-se numa autenticação por 2 fatores, considerando-se por isso mais segura: algo que eu sei – o PIN – e algo que eu tenho – o cartão. Uma vez efetuada esta autenticação, são permitidas diversas operações , sendo que em alguns casos as mesmas estão limitadas no seu valor (ex: levantamentos diários e transferências).

O cartão é fundamental para a realização de qualquer operação. Caso este seja roubado ou perdido, é também necessário o PIN. São esses dois fatores que lhe concedem uma segurança reforçada.

E quais os riscos de segurança que podemos ter?

O cartão pode ser roubado de várias formas, algumas mais tecnológicas, outras menos e outras sem qualquer tecnologia associada.

Uma das formas consiste, em vez do roubo físico do cartão, na cópia da informação que consta da banda magnética. Trata-se de uma clonagem do cartão. Esta pode ser feita, por exemplo, num multibanco que tenha sido "adulterado". Nestas situações, é ainda possível que tenha sido instalado um qualquer sistema (ex: mini camara de vídeo) que permita a obtenção do PIN.

A clonagem pode também ser feita por alguém mal-intencionado

CRÓNICA VISÃO ELECTRÓNICA
Nº 299 / 2014-10-09
http://www.gestaodefraude.eu
Edgar Pimenta

a quem possamos dar o cartão quando estamos a fazer um pagamento. O cartão é passado num pequeno aparelho que faz a leitura da sua banda magnética. E como normalmente não somos discretos na marcação do PIN, pode ser relativamente fácil a um terceiro obter esse mesmo PIN.

Assim, que cuidados podemos ter?

Em primeiro lugar, devemos manter sempre contacto visual com o nosso cartão quando usado em pagamentos. Devemos ainda dificultar a obtenção do PIN, tapando a digitação do mesmo – em multibanco e terminais de pagamento – e não escolhendo PINs demasiado óbvios. Já agora, se usamos um PIN no smartphone, este deve ser diferente do PIN do Multibanco.

Adicionalmente, devemos evitar usar multibancos em zonas mais abandonadas ou com menor frequência de passagem. Podemos ainda estar alerta para alterações efetuadas nos equipamentos.

Homebanking

Os sistemas de homebanking, seja através de computador pessoal ou através de um dispositivo móvel (e.g. smartphone, tablet) apresentam riscos diferentes. Estes sistemas permitem um acesso a mais informação do que num Multibanco, sendo por isso mais apetecíveis numa perspetiva maliciosa.

O phishing é uma das formas principais de obter as credenciais de acesso a sistemas de homebankig. Baseia-se em ludibriar o utilizador para que ele forneça as suas credenciais de acesso e, por vezes, de outros métodos de autenticação adicionais (e.g cartão matriz ou códigos adicionais). Assim, desconfie sempre quando lhe for enviado um e-mail que peça urgência na validação de credenciais de acesso, mesmo que esse e-mail pareça vindo do seu banco. Em caso de dúvida, ligue para o banco e informe-se.

O malware é outra das ameaças à informação e transações acessíveis por homebanking. Existe malware específico para adulterar transações bancárias e/ou roubar credenciais de acesso. Assim, o investimento num sistema de antivírus recente e que seja periodicamente atualizado é algo completamente justificável.

No caso específico dos smartphones e tablets, e dado o caráter

CRÓNICA VISÃO ELECTRÓNICA
Nº 299 / 2014-10-09
http://www.gestaodefraude.eu
Edgar Pimenta

portátil dos mesmos, devem ser adicionados outros cuidados. Passam por colocar um bloqueio no acesso ao telemóvel e, eventualmente, um outro à aplicação de homebanking. Deve ainda ter-se cuidado com a instalação de programas/aplicações. Nem sempre estamos completamente cientes da informação a que essas aplicações acedem. E a segurança destes equipamentos ainda deixa algo a desejar....

e-mail

Com o advento do digital, começamos a prescindir cada vez mais do papel. E o e-mail passou a ser considerado um canal preferencial para trocar informações com os bancos, seja pela receção dos extratos bancários, seja para todo o género de pedidos, ordens e esclarecimentos. E será que temos os cuidados adequados na gestão do nosso e-mail utilizado neste âmbito?

Alguns dos cuidados passam por ter uma password robusta e única, por alterar essa mesma password periodicamente, por não aceder em computadores/equipamentos desconhecidos e por utilizar todas as medidas de segurança que os fornecedores do serviço providenciam (por exemplo: o gmail permite que o acesso ao e-mail seja baseado numa password e num código único gerado a cada 30 segundos por uma aplicação no nosso telemóvel).

NFC - Near Field Communication

O futuro dos pagamentos passa por aqui. Em que consiste?

Muitos dos smartphones mais recentes, nos quais se incluí o novo iPhone6, suportam já esta tecnologia. Basicamente, basta aproximar o telemóvel dum terminal de pagamento específico (com NFC) para que o pagamento seja efetuado.

Embora a tecnologia exista, a sua aplicação prática ainda está algo embrionária. Mas sendo um sistema que pretende sobretudo ser fácil para o utilizador, no precário equilíbrio entre segurança e a facilidade/usabilidade, é fácil perceber qual terá a primazia.