Como fazer compras de forma segura pela Internet

Guia de orientação para consumidores

O texto agora publicado corresponde a uma tradução da responsabilidade da ANACOM de um excerto do relatório "*How to shop safety online"*, publicado pela ENISA[1] no seu *site*. Não se garante que este texto reproduza exactamente a versão original, pelo que apenas o relatório da ENISA é considerado autêntico.

Orientações para os consumidores

No que respeita à segurança na Internet, mais vale prevenir que remediar. Os consumidores devem manter-se sempre vigilantes. Tal não é tão difícil como pode parecer. Seguidamente apresentam-se algumas dicas que os consumidores devem ter presentes antes de efectuarem compras *online*.

Proteja a sua privacidade

Os autores das fraudes de identidade apenas necessitam de algumas informações suas para terem acesso às suas contas ou para abrirem linhas de crédito no seu nome. Em alguns casos, poderão não fazer uso directo das informações que obtêm, mas, em vez disso, venderem estas informações no mercado negro, o que torna muito mais difícil investigar quem captura estes elementos, quando e onde o faz.

É por isso essencial que adopte os seguintes procedimentos para proteger a sua privacidade:

- Verifique a política de privacidade da loja na Internet onde pretende efectuar as suas compras a fim de perceber como é que a empresa trata a informação que recolhe acerca de si. Se não lhe agrada aquilo que vê, adquira noutra loja.
- Nunca partilhe palavras-chave/códigos (*passwords*) e altere-as pelo menos de 6 em 6 meses.
- Ao escolher uma palavra-chave, adopte uma composição de letras (maiúsculas e minúsculas), símbolos e números combinados que não possam ser facilmente descobertos. Quanto mais longa e complexa a *password*, mais difícil é de descobrir.
- Utilize autenticação o mais segura que puder. Um pirata da Internet tem capacidade para investigar o *login* e *password*, mas é pouco provável que possua as suas credenciais (*token*, cartão ou telefone móvel), que geram códigos robustos para alcançar uma autenticação segura. Por outras palavras, não registe os seus dados apenas com uma *password* estabelecida por si, recorra adicionalmente e, sempre que disponível, a funcionalidades de autenticação tais como *tokens, smartcards* ou, em alguns casos, serviços que usam o telemóvel para enviar por SMS um *pin* de utilização única.

[1] http://www.enisa.europa.eu/act/ar/deliverables/2010/how-to-shop-safely-online?searchterm=how+to+shop

- Verifique sempre as condições de privacidade nas redes sociais e aplicativos de comunicações. Opte sempre pela máxima privacidade para a generalidade dos conteúdos que publica na Internet. Pode sempre adoptar permissões de privacidade para determinado grupo de artigos.
- Seja cuidadoso com as pessoas com quem faz amizade na Internet. Qualquer pessoa se pode registar sob uma falsa identidade na maioria dos *sites* de redes sociais na Internet.
- Seja cauteloso antes de publicar qualquer informação que possa ser usada por empresas e organizações para verificar a sua identidade, especialmente data de nascimento, localização e identificação do parentesco.
- Quando lhe for solicitado o preenchimento de formulários, analise cuidadosamente se a organização necessita realmente dos dados que está a solicitar.
- Quando se regista num *site* na Internet, lembre-se que não é, habitualmente, necessário preencher todos os campos. Os dados de carácter obrigatório são normalmente o primeiro nome e apelido, endereço de correio electrónico e morada para entrega da encomenda. Os elementos de carácter facultativo podem ser utilizados para campanhas de *marketing* e para traçar o perfil de consumo.
- Quando lhe é solicitada resposta a questões de autenticação, especialmente em serviços de baixo valor para si, não há obrigação de fornecer respostas exactas.
- Ocasionalmente, use o seu motor de busca preferido para verificar qual a informação que está publicada acerca de si na Internet. Se encontrar informação que não pretenda ver divulgada, poderá tentar contactar os responsáveis pelos *sites* para solicitar alteração de dados incorrectos ou remoção de dados pessoais.
- Se puder, encripte os dados que armazena em discos duros, especialmente em computadores portáteis e, no caso de informações confidenciais, suportes de dados amovíveis, como CD e *pen-drives*.
- Certifique-se que destrói os elementos confidenciais qualquer que seja o suporte. O papel pode ser triturado, tal como a maioria dos meios ópticos (mas verifique a sua destruidora). Os discos rígidos são muitas vezes revendidos e têm sido encontrados ainda com dados confidenciais (obviamente que estando esses discos encriptados, é muito improvável que os dados possam ser lidos).

Evite acumular informação em *sites* na Internet

Muitos vendedores perguntar-lhe-ão se deseja guardar a sua informação pessoal de forma a que seja automaticamente acessível mais tarde, caso tenha outras transacções a fazer. O vendedor poderá possibilitar o armazenamento do seu nome, moradas de entrega e de facturação, formas de pagamento e detalhes financeiros tais como, números de cartões de crédito ou outras informações bancárias. Permitir este armazenamento de dados, pode acarretar uma série de riscos:

- Aumenta o número de locais onde estão guardados estes dados pessoais e, assim, aumenta a probabilidade destes dados serem comprometidos.

- Deposita confiança no vendedor *online* para protecção dos elementos que forneceu. Mesmo com uma segurança sofisticada, existe risco dos sistemas serem comprometidos e serem roubadas as informações.

Pondere cuidadosamente a conveniência de permitir que os seus dados pessoais sejam armazenados num *site* de vendas na Internet, que fica fora do seu controlo, comparativamente a guardar estas informações de forma alternativa. Se está a fazer uma compra única, é aconselhável que permita o armazenamento dos seus dados pessoais no *site* do vendedor.

Proteja o seu computador

Alguns criminosos na Internet usam *software* espião (*Spyware*) ou programas de investigação de senhas (*keylogger programs*) para roubar informação pessoal no seu computador. Estes programas gravam todas as teclas digitadas, permitindo aos ladrões de identidade alcançarem os nomes de registo e as senhas de entrada de acesso a contas bancárias ou *sites* de compras *online*. Outros investigam ("*sniff*") redes sem fios não seguras, sem que os seus donos se apercebam, para conseguirem acesso a pastas partilhadas no seu computador.

Alguns passos simples poderão ajudar a protegê-lo quando fizer compras pela Internet. Não requerem grande esforço e podem resultar em ganhos significativos de segurança do seu computador pessoal. Para envidar esforços, assegure-se de que:

- Instala uma *firewall* assim como um antivírus e anti-*spyware*. Actualize regularmente (se possível diariamente) protecções para vírus e para "spyware" e faça uma análise semanal ao computador para verificação de vulnerabilidades.
- Evite transferir anexos do correio electrónico para o seu computador ou digitar ligações a *sites* (*links*), a menos que as mensagens sejam de proveniência conhecida e confiável.
- Nunca forneça informação confidencial através de mensagem de correio electrónico. Tenha presente que comerciantes legítimos, bancos ou correctoras nunca lhe solicitarão nomes de utilizador, senhas de entrada, *pin* ou qualquer outra informação confidencial através de correio electrónico. Apenas pessoas mal intencionadas adoptam essas atitudes.
- Se tiver um computador portátil, crie uma palavra passe para acesso a este.
- Utilize uma rede Wi-Fi sem fios segura. Crie uma palavra passe para acesso à rede sem fios de sua casa e evite efectuar compras *online*, operações em banca *online* ou efectuar operações de investimento, através de *sites* na Internet com acesso de rede pública sem fios.
- Desligue-se da Internet quando não necessitar de estar *online*.
- Adopte sempre uma versão actual do sistema operativo. Os sistemas operativos mais modernos providenciam uma espécie de sistema automático de actualização, que deverá assegurar que está a correr correctamente e a maior parte dos vendedores envia mensagens ou notificações para actualizações de *software* (*patches*) que podem ser descarregados em *sites* por eles aconselhados.

- Utilize um *browser* (aplicação para aceder à Internet) actual. Têm sido efectuados melhoramentos significativos nas gerações mais recentes de *browser* na Internet, assim, deve assegurar que está a utilizar a versão mais recente desse produto e que mantém as actualizações disponíveis no mercado.
- Esteja atento às notificações de segurança do seu *browser*. Alguns *browser* actuais, incluindo os dois líderes de mercado (*Microsoft Internet Explorer* e *Mozilla Firefox*), garantem alertas quando existem *sites* de reputação não confiável. Estes ajudam a reconhecer tentativas de fraude. Se o seu *browser* não lhe proporciona esta funcionalidade, adopte um produto disponibilizado por um outro vendedor.
- Execute um produto antivírus confiável e mantenha-o actualizado. Muitos computadores vêm com tempo limitado de assinaturas gratuitas de um dos principais produtos comerciais. Deverá certificar-se de que compra a versão actualizada ou, em alternativa, instalar outro produto quando a versão gratuita expirar. Há também uma série de produtos eficazes de livre acesso para utilizadores individuais. Instale somente uma versão de um dado produto, pois a coexistência de várias versões pode ser conflituante, tornar o processador mais lento e funcionar de forma ineficaz podendo permitir a entrada de códigos maliciosos.
- Certifique-se que o acesso ao seu computador necessita de introdução de uma *password*. Este procedimento não só protege o conteúdo do computador no caso de furto, como também constitui uma segurança adicional contra *hackers* maliciosos que tentem aceder ao computador.
- Configure o *screensaver* de modo a requerer a entrada de uma senha para desbloqueamento. Este procedimento previne o acesso indesejável ao seu computador enquanto se ausenta.

Faça compras de forma segura na Internet

Ainda que tenha o seu computador munido do *browser* mais seguro, *firewall*, antivírus e anti-*spyware*, é importante que mesmo assim se mantenha vigilante enquanto estiver *online*. Seguidamente apresentam-se algumas práticas que deverá adoptar para promover a sua segurança:

- Desconfie de *sites* que apresentem uma construção simples e que não forneçam nenhuma informação de segurança que possa ser verificável. Se não tiver a certeza de que se trata de um *site* ilegítimo, envie uma mensagem ou telefone para a empresa, antes de fornecer qualquer informação.
- Procure por um ícone de cadeado em qualquer *site* de compras. Para ser fiável, o ícone de cadeado deve aparecer no interface de *browser* e não como conteúdo da própria página.
- Evite *sites* que têm óbvios e abundantes erros de edição.
- Instale as versões mais recentes de todo o *software* que pretende ter no seu computador.
- Seja cuidadoso com o que faz a partir de um computador desprotegido ou desconhecido.
- Esteja atento aos termos e condições do sistema de pagamento que utiliza.

- Tenha atenção às despesas de porte e de embalagem dos produtos que adquire *online*.
- Ao comparar preços de produtos e serviços oriundos de países não pertencentes ao Espaço Económico Europeu, lembre-se que poderá ter que pagar IVA e direitos de importação.
- Faça compras a comerciantes fiáveis e mercados bem administrados (como por exemplo Amazon e eBay), que dispõem de procedimentos estabelecidos para apresentação de reclamações.
- Evite efectuar compras na Internet a partir de computadores de acesso público. Estes são usados por todo o tipo de pessoas, incluindo aqueles que, ao contrário de si, não estão preocupados nem conscientes da necessidade de segurança. Estes computadores são muitas vezes usados, intencionalmente ou não, para visitar *sites* que contém *software* malicioso, que irá coligir toda a informação digitada no teclado, incluindo senhas de entrada e informação financeira, tal como números de cartões de crédito e outras informações bancárias. A menos que absolutamente necessário, evite utilizar computadores de acesso público para verificar ou digitar informação confidencial.
- Tenha presente os seguintes provérbios: "Se lhe parece demasiado bom para ser verdade, desconfie" ou "não compre gato por lebre".

Para mais informações recorra à entidade de apoio ao consumidor no seu país.

Pagamentos seguros

Apresenta-se de seguida um conjunto de passos que deverá dar de modo a garantir a segurança dos pagamentos *online*:

- Sempre que possível utilize um meio de pagamento com reduzido montante de limite máximo de débito.
- Verifique a sua conta bancária e as declarações que surgem após o pagamento com cartão de crédito e, de forma regular, caso suspeite de alguma transacção realizada.
- Sempre que possível, use um método de pagamento temporário.
- Tenha preferência por cartões de débito ou crédito de instituições bancárias que garantam serviço de prevenção de fraudes (para tal verifique o *site* do banco para obter informação sobre este serviço).

Conheça os seus direitos

Se alguma coisa correr mal com uma compra *online*, é essencial que conheça quais os seus direitos em termos de correcção de erros ou reembolso. Tenha presente que efectuar compras *online* não lhe retira os direitos fundamentais como consumidor e, frequentemente, dá-lhe direitos adicionais. É importante que esteja consciente dos direitos que a lei lhe garante, nos termos do contrato de compra e das condições do meio de pagamento que utiliza.

Porém, precisa de ter presente que, em muito casos, a jurisdição do contrato que realizou está no domínio legal do mercado de origem.

As compras pela Internet não reduzem os seus direitos de consumidor e podem até dar-lhe direitos adicionais.

- Os bens deverão corresponder exactamente ao descritivo no *site* da Internet. Isto significa que os artigos terão que respeitar a(s) funcionalidade(s) e qualidade descritas no *site* e quaisquer opções que tenha requerido devem ser as oferecidas. Pode ocorrer que o vendedor, em virtude de quebra de *stocks* ou outros motivos, lhe envie um produto diferente. Neste caso não tem obrigação de o aceitar, a menos que tenha dado o seu acordo prévio a essa variante.
- Os produtos que adquire deverão ser-lhe entregues em perfeito estado, isto é, intactos. Tratando-se de bens depreciáveis, têm que estar dentro da data de validade. Se um artigo lhe chegar partido ou com defeito, tem o direito de, num período de 6 meses, solicitar a resolução da questão.
- Deverá receber a sua encomenda num prazo máximo de 30 dias, findo o qual terá direito a reembolso. Quem realiza o contrato com a empresa que faz a entrega é o vendedor, pelo que é a este que cabe a responsabilidade de a garantir.
- Segundo a Directiva Europeia da Venda à Distância, o consumidor tem o direito de desistir do contrato num prazo de 7 dias úteis e devolver o bem. Pode ser-lhe exigido o pagamento das despesas de porte, mas, ao abrigo de um recente acórdão, as despesas iniciais de porte e embalagem devem ser igualmente reembolsadas. Bens e serviços com data de validade ou que, de alguma forma, sejam personalizados, estão sujeitos a aplicação de regras diferentes.
- Pode ter direitos legais ou contratuais de reembolso por parte do prestador do meio de pagamento. A Directiva Europeia do Pagamento de Serviços deve estar transposta e detalhadas as regras para a legislação nacional.
- Os termos e condições definidas no *site* do fornecedor dar-lhe-ão protecção adicional.
- Com respeito ao pagamento de bens adquiridos, tenha presente que, segundo a legislação Europeia, uma vez efectuado o pagamento, deverá o vendedor fornecer-lhe um recibo correspondente à sua transacção.

Alguns governos europeus proporcionam protecções específicas para aqueles que fazem compras *online*. A lei britânica de protecção de dados, por exemplo, garante que as informações que uma empresa recebe por parte do cliente, quando este realiza uma compra através da Internet, devem ser tratadas da mesma forma que as que são processadas numa loja tradicional. Os comerciantes não estão autorizados a partilhar a informação a terceiros sem o consentimento do cliente.

Se suspeitar de roubo da sua identidade, contacte o seu banco, solicite que investiguem a sua conta e o alertem em caso de actividade anormal. Reporte a ocorrência às principais agências de crédito e às autoridades policiais locais. Deverá também alertar a entidade emissora de passaportes, caso suspeite que alguém está a tentar usar o seu passaporte em seu nome. Para este reporte reúna toda a documentação, e registe comunicações e conversas que lhe pareçam suspeitas, se possível, com o registo de nomes, números e datas.

De acordo com a legislação Europeia para as vendas/compras à distância, numa situação de pagamento em duplicado, tem o direito de cancelar o contrato no prazo de 7 dias a partir da

data de emissão do recibo. No que respeita à entrega do bem adquirido, a empresa deverá garantir a entrega no prazo máximo de 30 dias. A legislação permite que, em caso de litígio, seja possível intentar acção nos tribunais nacionais ou optar por uma alternativa de resolução de litígios.

Regras fundamentais para comprar na Internet de forma segura

Quando efectua compras na Internet, deve ter em conta as seguintes regras:

Categoria	Recomendação	Descritivo
Conheça o seu fornecedor	Verifique os termos e condições	Preste especial atenção à política de cancelamento e reembolso, detalhes sobre entrega e informação de garantias. Os portes de envio, custo final e jurisdição aplicável devem ser verificados cuidadosamente. Faça uma cópia de todas estas condições.
	Verifique o país de origem e morada	Existem lojas *online* que se assemelham ao seu fornecedor local, mas que estão situadas em países estrangeiros. No caso de comerciante internacional, preste especial atenção a direitos aduaneiros, impostos e questões legais. Como comprador é responsável pelo apuramento destes procedimentos de venda.
	Esteja atento a lojas fraudulentas	Assegure-se que está a visitar a loja online que realmente pretende. Existem lojas fraudulentas com endereços de Internet idênticos aos dos legítimos. Estes endereços falsos podem surgir no formato de endereço curto ou difundido em mensagens de correio electrónico.
Proteja os seus dados pessoais	Adopte senhas únicas	Não utilize a mesma senha para diferentes lojas. Adopte senhas robustas.
	Verifique a política de privacidade	Que dados pessoais são armazenados, por quanto tempo e para que finalidade? Quando é que esses dados serão apagados? De que

Categoria	Recomendação	Descritivo
		forma são protegidos?
	Forneça apenas a informação pessoal obrigatória que lhe é solicitada	No que respeita ao registo da sua compra num *site*, não disponibilize dados pessoais que não sejam absolutamente necessários para o trâmite da transacção.
	Verifique se existe encriptação (SSL) na transferência de dados pessoais	*Secure Socket Layer* (SSL) encripta a comunicação entre o *browser* e a loja *online.*
	Processo de pagamento	Escolha o seu método de pagamento de forma prudente. Consulte a secção adequada nos bancos e serviços de pagamento para conhecer com maior detalhe os riscos inerentes.
Conheça os seus direitos	Direitos legais que protegem o consumidor na Internet	Deve conhecer os regulamentos e procedimentos aplicáveis às vendas à distância. Estes podem divergir entre países.
Saiba o que está a comprar	Verifique os detalhes do produto	Confirme o preço do produto, o custo total, a versão e a autenticação. Erros dactilográficos na designação das marcas deverão alertá-lo. Esteja atento aos produtos fraudulentos/piratas.
	Verifique a entrega do produto	A quantidade, o aspecto e o acabamento estão de acordo com o seu pedido? Se tiver dúvidas contacte imediatamente o fornecedor por escrito.
Esteja atento	Verifique os movimentos bancários após pagamento com cartão de crédito	Verifique se a transferência foi realizada pelo valor acordado e se não existem despesas não autorizadas.

"*Get Safe Online*" é um exemplo de uma campanha de sensibilização para as questões de segurança. Esta iniciativa de sensibilização para a reserva de férias em segurança no Reino Unido, foi lançada em conjunto com a ABTA – a maior associação de viagens do Reino Unido. Na base desta campanha esteve um estudo que concluiu que 1 em cada 3 internautas corre riscos de fraude quando efectua a reserva de férias *online*. Praticamente dois terços dos internautas do Reino Unido desconhecem os esquemas fraudulentos mais comuns, tais como

fraudes no aluguer de casas, mensagens não solicitadas (*spam*) ou chamadas telefónicas de pessoas ou empresas desconhecidas. Cerca de 30% dos utilizadores da Internet reservam as suas férias sem confirmação de autenticidade das agências de viagens. Antes de marcar as suas férias, consulte: Get Safe Online.

Linhas de orientação para os comerciantes na Internet

Vender bens ou serviços na Internet trás benefícios tanto para comerciantes retalhistas como para industriais, tais como poupança de custos, uma base mais alargada de potenciais clientes e um processo mais eficiente de vendas. Porém, é essencial que, quando se cria uma loja na Internet, a empresa esteja consciencializada das responsabilidades e obrigações para com os clientes. Seguidamente expõem-se um número de passos que deve ter em conta no momento de criar uma loja na Internet.

Equipa

- A partir do momento em que se envolve nas Tecnologias da Informação e Comunicação deve adequar o seu modelo de gestão. Isto significa que a sua equipa deverá incluir especialistas de segurança informática na equipa de gestão do negócio, internos ou subcontratados a empresas especializadas na prestação destes serviços.
- Deverá promover formação ao pessoal não especialista quanto ao seu papel e responsabilidade no âmbito do *site* de comércio electrónico e assegurar-se de que conhecem os direitos dos consumidores e que lidam com estes de forma apropriada. Os colaboradores deverão ter formação que lhes permita detectar, reportar e lidar com eventuais situações de fraude.

Garanta a segurança dos seus sistemas

- Assegure-se de que os sistemas instalados e a plataforma base do seu negócio *online* são seguros. Isto significa que, por forma a evitar que a sua página na Internet seja atacada por pessoas mal-intencionadas, deve instalar sistemas como *firewall, audit trails e log files* e assegurar-se de que são monitorados de forma a detectar eventual intrusão. Execute todos os testes de auditoria. Os *audit trails* não só permitem ter uma caracterização das visitas à sua página, como também podem apoiar na investigação de um incidente de segurança. Os *log files* podem servir de alerta de potenciais ataques e podem ser usados para combater ataques ao sistema em curso.
- Utilize certificados SSL para garantir a segurança das comunicações entre a página e o cliente. Assegure-se de que os certificados são comprados a vendedores de reconhecida confiança.
- Teste regularmente a eventual existência de vulnerabilidades de segurança que possam ser exploradas por criminosos.
- Se contratar serviços externos para a criação da sua loja *online*, garanta que as cláusulas contratuais incluem responsabilidades ao nível da segurança.

Conteúdo da página

- Garanta que o conteúdo do seu *site* está correcto e que os preços e outras informações estão actualizados. A proliferação de erros na página prejudicará a confiança do cliente

que a visita. Também deve assegurar que todos os preços incluem taxas/impostos, despesas de portes de envio e custos alfandegários.

- Ofereça informação sobre política de privacidade e indique com clareza quais os procedimentos adoptados em relação à recolha e tratamento de dados pessoais que são fornecidos pelos clientes.
- Assegure que tem processos e procedimentos preparados, assim como uma equipa com formação, para identificar e lidar com potenciais actividades fraudulentas.

Questões regulamentares e de conformidade

Certifique-se de que você e a sua equipa conhecem os regulamentos e questões de conformidade no âmbito da actividade que desenvolve e da loja *online*. Em particular, o seguinte enquadramento regulamentar:

- Directiva 97/7/EC – Protecção do consumidor nos contratos celebrados à distância;
- Directiva 1999/44/EC do Parlamento Europeu e do Conselho de 25 Maio 1999 – Determinados aspectos da venda de bens ao consumidor e garantias associadas;
- Directiva 2000/31/EC do Parlamento Europeu e do Conselho de 8 Junho 2000 – Determinados aspectos legais dos serviços da sociedade de informação, em particular do comércio electrónico, no Mercado Interno (Directiva do Comércio Electrónico);
- Directiva 2002/58/EC do Parlamento Europeu e do Conselho de 12 Julho 2002 – Processamento de Dados Pessoais e Protecção da Privacidade no Sector das comunicações Electrónicas (Directiva da Privacidade e Comunicações Electrónicas);
- Directiva 95/46/EC do Parlamento Europeu e do Conselho de 24 de Outubro 1995 – Protecção dos indivíduos no que respeita ao processamento de dados pessoais e liberdade de movimento destes dados.

Deve acautelar o conhecimento dos regulamentos específicos de jurisdição local no âmbito de bancos, transferências bancárias, operações de lavagem de dinheiro e comércio electrónico.

PCI DSS[2] - PCI *Data Security Standard*

Os comerciantes *online* devem certificar-se de que não são os elos mais fracos na segurança dos dados dos titulares dos cartões. Devem ter capacidade para assumir os pagamentos *online* de forma segura e, assim, assegurar a confiança dos seus clientes.

Assim, será desejável a conformidade com os requisitos PCI DSS. A maior parte dos comerciantes estão no nível 3 ou 4, precisando de efectuar quatro acções para validação da conformidade:

[2] https://www.pcisecuritystandards.org/
O PCI DSS é um padrão de segurança multifacetado, que inclui os requisitos para a gestão de segurança, políticas, procedimentos, arquitectura de redes, desenho de *software* e outros componentes importantes medidos de protecção. Este padrão global é destinado a ajudar as organizações a proteger de forma proactiva os dados da conta do cliente

- Formar os colaboradores em matéria de segurança de cartões de crédito e melhores práticas genéricas de segurança.
- Promover e implementar fortes políticas de segurança e procedimentos.
- Verificar trimestralmente os endereços Internet Protocol (IP) externos subjacentes a sistemas de pagamento utilizando o ASV – *Approved Scanning Vendor* devidamente aprovado pelo PCI SSC[3].
- Preencher um questionário de auto-avaliação (SAQ – *self-assessment questionnaire*) e registá-lo no seu banco adquirente.

Este é um processo contínuo e o questionário de auto-avaliação deve ser preenchido todos os anos. Os colaboradores que desenvolvam actividade neste âmbito, que tenham contacto físico ou contacto com a infra-estrutura tecnológica de suporte de dados de cartões de crédito, devem receber formação logo após a sua contratação e, pelo menos, uma vez por ano. O comerciante deverá escolher um dos diversos ASV - *Approved Scanning Vendor* que existem no mercado, sendo da sua responsabilidade a efectivação trimestral destes *scans*. Os formulários dos questionários de auto-avaliação podem ser descarregados gratuitamente do *site* da PCI SSC. No entanto, deverá ser tido em conta que existem alguns vendedores a oferecerem soluções completas e integradas aos comerciantes para verificação de conformidade a partir de ferramentas na Internet. Recomenda-se que o comerciante garanta uma solução abrangente e com os quatro elementos mencionados – formação do colaborador, políticas e procedimentos, *scanning* e questionários de auto-avaliação – em detrimento de apenas um subconjunto dos requisitos exigíveis.

Os comerciantes *online* também têm de estar continuamente familiarizados com os diversos tipos de fraudes na Internet. Têm de relatar tentativas ou suspeitas de fraude aos seus fornecedores de serviços de pagamento ou bancos, assim que tomam conhecimento de possíveis incidentes.

É por isso que o PCI DSS tornou obrigatória a formação dos funcionários, como parte do requisito 12.6 das normas. Sensibilizar para possíveis questões de segurança e de fraude em compras *online* é essencial no seu combate. Contudo, quer os comerciantes, quer os consumidores, precisam de estar conscientes de que a responsabilidade de garantir o combate do problema recai sobre os comerciantes.

Os comerciantes são ainda aconselhados a rever os procedimentos de combate à fraude *online,* utilizando soluções tecnológicas para complementar a formação dos colaboradores e a segurança tradicional. Se o comerciante tem uma solução bem desenvolvida de comércio *online*, é recomendável que invista em soluções de combate ao crime financeiro, por forma a reduzir as perdas por fraude, melhorando a eficiência das investigações e a gestão de casos, aumentando a exactidão na detecção de fraude, reduzindo despesas de capital e custos de suporte e reduzindo o risco de sanções e penalizações aplicadas por parte dos reguladores.

[3] https://www.pcisecuritystandards.org/approved_companies_providers/become_asv.php