+ 5 dicas para ficar seguro *online*

☞ #ficaadica

BANCO DE PORTUGAL
EUROSISTEMA

+ 5 dicas para ficar seguro *online* #ficaadica | 2023 • **Banco de Portugal** Rua do Comércio, 148 | 1100-150 Lisboa • www.bportugal.pt • **Edição** Departamento de Supervisão Comportamental • **Design** Departamento de Comunicação e Museu | Unidade de Design • **Tiragem** 10 000 exemplares • **ISBN (impresso)** 978-989-678-851-3 • **ISBN (*online*)** 978-989-678-852-0 • **Depósito Legal n.º** 511047/23

A evolução tecnológica, a inovação financeira permanente e a multiplicação de serviços e produtos financeiros de acesso digital fácil e rápido tornam a nossa relação com o setor financeiro numa relação cada vez mais virtual em que os canais digitais começam a ser a forma privilegiada de acesso aos produtos bancários. Sendo esta realidade positiva e próxima do perfil das novas gerações não está isenta de riscos para os quais devemos estar cada vez mais atentos. É muito importante o conhecimento das caraterísticas dos novos produtos, dos riscos dos novos canais de acesso e dos procedimentos de segurança a adotar.
A informação, conhecimento e utilização esclarecida do digital permitem que possamos usufruir das vantagens e conforto da inovação, com a segurança necessária e de uma forma mais protegida.
Do nosso lado fica o compromisso de promovermos a disponibilização da informação de forma transparente e acessível e de fomentar a formação financeira digital. As dicas que deixamos aqui são um passo neste nosso compromisso, e pistas para uma utilização segura dos canais digitais. **Fica a dica.**

Francisca Guedes de Oliveira
Administradora do Banco de Portugal

Fraude financeira digital Também caía nesta?

#ficaadica

Recebe um *e-mail* ou uma mensagem do seu banco ou de outro prestador de serviços de pagamento ou de uma entidade com a qual contratou um serviço. Dizem que a sua conta pode estar comprometida ou bloqueada e pedem que faça *login* para recuperar o acesso. Clica no *link* e insere as suas credenciais ou transmite-as por telefone, sem pensar duas vezes?

É provável que esteja perante uma forma comum de *phishing*, isto é, um ataque destinado a captar os seus dados pessoais. E há outras técnicas fraudulentas, aparentemente inofensivas e igualmente eficazes, que são usadas por pessoas que, em qualquer parte do mundo, se podem apropriar dos seus dados. Muitas vezes os piratas informáticos utilizam informação que obtêm nas redes sociais e utilizam a manipulação psicológica para ganhar a confiança da vítima e, assim, obter informações confidenciais.

Conheça os riscos

O pirata informático contacta-o por *e-mail*, por telefone ou faz uma publicação nas redes sociais, fazendo-se passar, por exemplo, por um banco ou outro prestador de serviços de pagamento, uma entidade pública ou um prestador de serviços. Por vezes, os piratas informáticos usam o *spoofing*, copiando os números de telefone ou *e-mails* e a aparência das entidades oficiais, para serem mais convincentes. Nestes contactos, aparentemente realizados por um motivo legítimo, tentam convencê-lo a disponibilizar os seus dados pessoais (diretamente ou fornecendo-lhe um *link* para uma página falsa, ainda que aparentemente legítima). Este tipo de ataque chama-se ***phishing*** (também conhecido como *vishing* ou *smishing*, se o contacto for feito por chamada ou SMS, respetivamente).

Ao fazer *download* de um ficheiro aparentemente inofensivo, pode estar a instalar no seu equipamento um vírus informático. Quando acede a um endereço correto, esse vírus redireciona-o para uma página falsa, através da qual são indevidamente recolhidos os seus dados pessoais. Este tipo de ataque chama-se ***pharming***.

Outras pessoas podem apropriar-se dos seus dados através da instalação de programas maliciosos que recolhem as suas informações. Este tipo de ataque chama-se ***spyware***.

Uma outra forma de terceiros se apropriarem dos seus dados é observando diretamente informação que está a escrever no seu telemóvel, *tablet* ou computador em locais com grande aglomeração de pessoas, como transportes públicos ou centros comerciais. Este tipo de ataque chama-se ***shoulder surfing***.

O que pode fazer para proteger os seus dados

#1 Avalie cuidadosamente os pedidos de informação que lhe dirigem.

- Nunca divulgue informação pessoal nem credenciais de acesso aos seus canais digitais ou códigos de autenticação de operações com terceiros. Um banco ou outro prestador de serviços de pagamento jamais lhe solicitaria esse tipo de informação por *e-mail*, SMS ou telefone.
- Não divulgue informação pessoal ou confidencial através de uma chamada telefónica que não tenha solicitado. Desconfie de mensagens que indicam que determinado serviço foi bloqueado e necessita de ser ativado ou que solicitam o pagamento de uma encomenda que não fez. Contactos com intenções fraudulentas são feitos normalmente num tom de urgência, para que divulgue rapidamente dados pessoais, sem ter tempo de pensar na melhor forma de agir.
- Se receber uma chamada, não assuma que esta é genuína apenas por o interlocutor estar na posse dos seus dados pessoais básicos. Esta informação poderá ser encontrada *online* (por exemplo, através das redes sociais).
- Não abra e elimine imediatamente *e-mails* duvidosos. Verifique o endereço do remetente (e não apenas o nome), o idioma, o tipo e o tom da linguagem utilizada e a apresentação gráfica da mensagem recebida. As mensagens fraudulentas adotam, muitas vezes, uma linguagem menos formal, com erros ortográficos ou de semântica e são escritas para transmitir ao leitor uma sensação de urgência.
- Não clique em hiperligações (*links*), não execute as ações pedidas (não execute programas sugeridos), nem abra anexos de fontes desconhecidas.
- Não inscreva dados confidenciais e outras informações pessoais em *sites* cuja autenticidade não esteja assegurada.

#2 Contacte a entidade em causa pelos contactos oficiais.

- Mesmo que julgue tratar-se de um contacto legítimo, não divulgue de imediato informação e contacte a entidade em causa pelos

contactos oficiais (e nunca usando os contactos fornecidos em *e-mails*, SMS ou nos telefonemas recebidos).

- Em caso de suspeita de fraude, reporte imediatamente a situação ao seu banco ou outro prestador de serviços de pagamento, através dos canais habituais, e às entidades policiais.

#3 Evite partilhar dados pessoais quando estes não forem essenciais para o serviço que lhe será prestado.

- Muitas plataformas e aplicações pedem acesso a informações pessoais, como a sua localização geográfica, contactos, microfone, câmara e álbum de fotografias, sem que tal seja relevante para a prestação dos serviços em causa. Essas informações podem ser depois partilhadas com outras entidades sem que o saiba.

#4 Verifique as configurações de privacidade e de segurança.

- Antes de começar a utilizar uma nova aplicação ou quando cria uma nova conta de utilizador na internet, verifique as configurações de privacidade e de segurança e defina-as para um nível de partilha de informações com o qual se sinta confortável.
- Cada dispositivo, aplicação ou navegador que usa tem recursos diferentes para limitar a forma como e com quem partilha informações: explore as opções e, se tiver dúvidas, informe-se.

#5 Não adie as atualizações e elimine sempre as contas e as aplicações que já não utiliza.

- As atualizações dos programas e das aplicações permitem corrigir problemas de segurança entretanto detetados. Uma aplicação no seu telemóvel que não usa e não atualiza pode constituir uma "porta" para eventuais ataques informáticos.

#6 Mantenha-se vigilante.

- Consulte periodicamente os movimentos da sua conta e contacte imediatamente o seu banco ou outro prestador de serviços de pagamento se detetar movimentos que não autorizou.


Serviços
bancários
digitais
siga estes
passos
#ficaadica

Quando acede à sua conta através da internet (*homebanking*) ou de uma aplicação móvel (*app*), deve ter em conta os riscos associados.

Saiba como se pode proteger e esteja atento aos procedimentos de segurança indicados pelo seu banco ou outro prestador de serviços de pagamento.

Em caso de dúvida, não execute a operação sem esclarecer previamente a situação com o seu banco ou outro prestador de serviços de pagamento.

Quando utiliza a internet

#1 Proteja o seu computador, *tablet* ou telemóvel.

- Defina palavras-passe e crie sequências de bloqueio de ecrã para que o seu equipamento não seja utilizado por terceiros.
- Não permita que *sites* ou aplicações com informação confidencial se iniciem automaticamente, sem ser necessário fazer o *login*.
- Mantenha atualizados o sistema operativo e os programas de antivírus e anti-*spyware* em todos os seus equipamentos.
- Mantenha o seu *browser* sempre atualizado.
- Não clique em *links* nem faça *downloads* de fontes desconhecidas.
- Não utilize redes *wi-fi* públicas ou desconhecidas.
- Não abandone o seu equipamento.

#2 Proteja os seus dados.

- Não divulgue as suas palavras-passe a terceiros.
- Escolha palavras-passe que não sejam demasiado óbvias (por exemplo, nunca use 123456, ABCDEF, QWERTY), nem que estejam associadas a informação pessoal fácil de obter (como datas de aniversário, nome dos filhos ou do cônjuge, números de telemóvel).
- Não use para acesso ao *homebaking* ou à *app* do seu banco ou outro prestador de serviços de pagamento a mesma palavra-passe que utiliza para desbloquear o equipamento ou para ligações a redes sociais, por exemplo.
- Não escreva palavras-passe e outra informação confidencial em papel, nem envie ou guarde essa informação em mensagens de *e-mail* ou no telemóvel.
- Utilize um gestor de *passwords offline*, como o Keepass.

Quando acede ao *homebanking* ou à *app*

#3 Aceda de forma segura à sua conta bancária através da internet (*homebanking*).

- Digite sempre o endereço eletrónico do seu *homebanking*, em vez de usar uma hiperligação (*link*), endereços gravados nos "Favoritos" ou no "Histórico" ou resultados de pesquisa de motores de busca.
- Verifique se o endereço que digitou é o endereço oficial da entidade.
- Confirme que o endereço do *site* começa por "https://" e que aparece um cadeado no final do endereço ou na barra inferior da janela. Se tal não acontecer, a página não é segura.
- Pode testar se o *site* é seguro usando o "truque da senha errada". Na primeira tentativa de acesso ao *site*, em vez do seu *login* habitual, coloque uma *password* errada. Se for aceite, isso significa que a entidade em causa não está a verificar o seu *login* (ou seja, pode estar a querer apenas recolher a *password* que escreve para utilizá-la de forma indevida).
- Garanta que insere a senha de acesso ao *homebanking* e outros elementos de autenticação em locais reservados e que não está a ser observado.
- Depois de utilizar o serviço de *homebanking*, termine a sessão e saia da página do banco ou de outro prestador de serviços de pagamento, clicando nos ícones existentes para o efeito. Confirme que é necessário fazer *login* para aceder novamente.

#4 Utilize de forma segura a aplicação móvel (*app*) do seu banco.

- Instale apenas aplicações obtidas em lojas de aplicações oficiais. Nem todas as aplicações são seguras e podem conter *software* malicioso.
- Analise, com cuidado, as avaliações (*reviews*) das aplicações antes de as descarregar. Existem aplicações com nomes e imagens muito semelhantes às *apps* dos bancos ou de outros prestadores de serviços de pagamento, propositadamente criadas para induzir em erro o utilizador.
- Verifique no *site* do seu banco ou de outro prestador de serviços de pagamento informação sobre a *app*

a descarregar e siga as instruções de configuração indicadas.

- Confirme quais os elementos de autenticação que lhe são solicitados cada vez que acede à *app* do seu banco ou de outro prestador de serviços de pagamento e desconfie se lhe for pedida informação adicional.
- Garanta que insere a senha de acesso à *app* do seu banco ou de outro prestador de serviços de pagamento e outros elementos de autenticação em locais reservados e que não está a ser observado. Se o seu dispositivo o permitir, privilegie elementos de autenticação biométricos (por exemplo, impressão digital ou reconhecimento facial), que são elementos que não podem ser apropriados por terceiros.
- Depois de utilizar a *app* do seu banco ou de outro prestador de serviços de pagamento, certifique-se de que a sessão foi terminada corretamente e que é necessário repetir o *login* para voltar a entrar.
- Em caso de dúvida, contacte imediatamente o seu banco ou outro prestador de serviços de pagamento, através dos canais habituais; ele saberá ajudá-lo.

#5 Utilize de forma segura as aplicações de pagamento (*app* de pagamento) operadas por terceiros (por exemplo, o MB WAY, Apple Pay, Google Pay, Garmin Pay, Fitbit Pay, Swatch Pay).

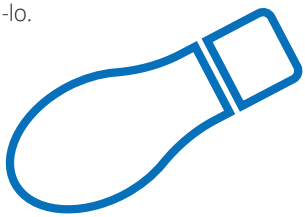
Saiba quais as *apps* de pagamento operadas por terceiros que o seu banco ou outro prestador de serviços de pagamento disponibiliza. Pode utilizar estas *apps* em simultâneo com a *app* do seu banco ou de outro prestador de serviços de pagamento.

Conheça as caraterísticas da *app* de pagamento que pretende utilizar, incluindo as operações que permite realizar e eventuais comissões que lhe possam ser cobradas.

- Instale apenas aplicações obtidas em lojas de aplicações oficiais.
- Na adesão à *app*, adicione apenas o seu número de telemóvel, se aplicável. Nunca associe um número de telemóvel de um terceiro à sua *app* de pagamento, pois, ao fazê-lo, poderá estar a permitir que um infrator aceda à sua informação e/ou aos seus fundos.
- Garanta que insere a senha de acesso à *app* de pagamento em locais reservados e que não está a ser observado.
- Quando realiza transações com a *app* de pagamento, certifique-se de que está a utilizar a funcionalidade

correta e leia, cuidadosamente, as notificações que recebe na aplicação antes de as aceitar. Caso a sua *app* de pagamento permita transferências, tenha especial atenção se receber uma notificação a "pedir dinheiro"; ao aceitar, estará a autorizar uma transferência de dinheiro da sua conta para outra pessoa;

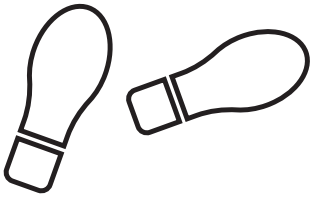
- Nunca partilhe com terceiros as informações de acesso à *app* de pagamento ou os códigos de autenticação das operações realizadas.
- Se receber uma notificação de uma operação que não realizou, contacte imediatamente o seu banco ou outro prestador de serviços de pagamento, através dos canais habituais, ele saberá ajudá-lo.



Depois de aceder ao *homebanking* ou à *app*

#6 Mantenha-se vigilante.

- Consulte periodicamente os movimentos da sua conta.
- Verifique a data e a hora do último acesso ao *homebanking* ou à *app*.
- Ative alertas de transferências e de débitos ou outros mecanismos de segurança que o seu banco ou outro prestador de serviços de pagamento disponibilize.
- Se receber algum *e-mail* ou SMS suspeito, supostamente do seu banco, informe-se da sua autenticidade pelos contactos oficiais do banco ou de outro prestador de serviços de pagamento (e nunca por contactos fornecidos no *e-mail* ou no SMS suspeito).
- Guarde na lista de contactos do seu telemóvel o contacto direto disponibilizado pelo seu banco ou outro prestador de serviços de pagamento. Assim, se detetar alguma irregularidade, conseguirá contactá-lo mais rapidamente.
- Recorde-se de que o seu banco ou outro prestador de serviços de pagamento nunca lhe solicitará os dados de acesso ao *homebanking* ou à *app* por telefone, *e-mail* ou SMS.



#7 Se desconfiar de fraude, aja adequadamente.

- Contacte imediatamente o seu banco ou outro prestador de serviços de pagamento caso detete movimentos que não autorizou ou que não reconhece. Para o efeito, utilize os contactos que o seu banco ou de outro prestador de serviços de pagamento lhe indicou ou o contacto constante da lista de emissores dos cartões de pagamento, publicada no *site* do Banco de Portugal.
- Peça imediatamente o cancelamento das credenciais de acesso ao *homebanking* ou à *app* do seu banco ou de outro prestador de serviços de pagamento e, se for o caso, do seu cartão de pagamento.
- Participe a situação ao órgão de polícia mais próximo (PSP, GNR ou PJ) ou ao Ministério Público.

#8 Se perder o cartão de pagamento ou algum elemento de segurança, comunique-o imediatamente ao seu banco.

- Comunique ao seu banco ou outro prestador de serviços de pagamento, logo que possível, o furto, o roubo ou a apropriação abusiva do cartão de pagamento, das credenciais de acesso ao *homebanking* ou da *app* ou de qualquer elemento de segurança utilizado para realizar operações financeiras através destes canais.
- Se forem realizadas operações de pagamento não autorizadas antes da comunicação ao banco ou outro prestador de serviços de pagamento, poderá ter de suportar um valor até um máximo de 50 euros.
- Em situações fraudulentas ou de negligência grave, poderá ter de suportar um valor superior a 50 euros.
- Caso tenha havido perda, roubo ou apropriação indevida das credenciais de acesso ao *homebanking* ou à *app* ou do cartão de pagamento e caso tenha alertado o seu banco ou outro prestador de serviços de pagamento desse facto, não poderá ser chamado a pagar os valores que forem movimentados sem autorização após esse alerta.

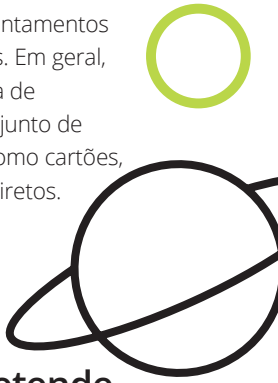

Abertura
de conta
à distância
#ficaadica

Sabia que atualmente já consegue abrir uma conta de depósito à ordem através de meios de comunicação à distância?

Informe-se se o banco junto do qual pretende abrir conta permite fazê-lo à distância e conheça as condições exigidas para o efeito.

Qualquer que seja o canal utilizado para abrir conta, presencial ou à distância, o banco tem de lhe disponibilizar informação clara e completa e esclarecer todas as suas dúvidas.

A conta de depósito à ordem permite-lhe movimentar os fundos depositados em qualquer altura. Pode fazer depósitos, levantamentos de dinheiro e pagamentos. Em geral, é possível associar à conta de depósito à ordem um conjunto de serviços de pagamento, como cartões, transferências e débitos diretos.



Antes de abrir conta

#1 Certifique-se de que o banco no qual pretende abrir conta está registado no Banco de Portugal.

- Garanta que o banco está registado no Banco de Portugal e que está autorizado a receber depósitos.

Nunca faça depósitos junto de entidades não autorizadas.

#2 Informe-se junto do banco no qual pretende abrir conta se é possível abrir conta através de canais digitais.

- Nem todos os bancos permitem a abertura de conta através de canais digitais. Em alguns casos, o processo pode ser iniciado através do *site* ou da *app* do banco, com o preenchimento de dados pessoais, mas poderá ter de se dirigir presencialmente à instituição para comprovar algum elemento de identificação.

#3 Verifique a segurança do *site* ou da *app* do Banco.

- Confirme que o endereço a que pretende aceder se inicia com "https://" e que aparece um cadeado no final do endereço ou na barra inferior da janela. Se tal não acontecer, a página não é segura.
- Instale apenas aplicações obtidas em lojas de aplicações oficiais.

- Adote os procedimentos de segurança habituais para proteger o seu computador, *tablet* ou telemóvel:
  - Mantenha atualizados os programas de antivírus e *anti-spyware*;
  - Não clique em *links* nem faça *downloads* de fontes desconhecidas;
  - Não utilize redes *wi-fi* públicas ou desconhecidas;
  - Não utilize equipamentos públicos para realizar pagamentos ou outras operações bancárias.

Não introduza os seus dados (nome, número de telemóvel, *e-mail*, número de cartão de cidadão, números de contas bancárias ou números de cartões de crédito) em *sites* que não conheça ou de cuja autenticidade desconfie.

#4 Analise a informação disponibilizada antes da abertura da conta.

Depois de ter acedido ao *site* ou *app* do banco e de ter preenchido os seus dados, o banco deve fornecer-lhe um conjunto de informação sobre a conta que pretende abrir:

- Ficha de informação normalizada (FIN) — documento com as caraterísticas da conta;
- Documento de informação sobre comissões — documento com informação sobre as comissões associadas aos serviços de pagamento mais representativos;
- Formulário de informação ao depositante (FID) — documento com informação sobre o sistema de garantia de depósitos;
- Condições gerais da conta.

Analise com cuidado toda a informação prestada e compare com alternativas, tendo em conta:

- Encargos associados à conta, por exemplo, as comissões de manutenção;
- Encargos associados à realização de operações de pagamento a partir dessa conta, por exemplo, encargos com cartões ou transferências.

No momento de abrir conta

#5 Verifique quais os procedimentos a adotar para abrir a conta através de canais digitais.

Na plataforma de apoio à abertura de conta, no *site* ou na *app* do banco, deverão ser indicados os passos a seguir para abrir conta à distância.

Em regra, terá de:

- Ler os documentos com as caraterísticas da conta;
- Preencher um conjunto de dados pessoais;
- Comprovar os seus elementos identificativos.

#6 Disponibilize ao banco os seus elementos identificativos e respetivos comprovativos.

Para abrir conta são solicitados, nomeadamente, os seguintes elementos identificativos:

- Nome completo, data de nascimento, tipo, número, data de validade e entidade emitente do documento de identificação;
- Número de identificação fiscal;
- Profissão e entidade patronal, quando existam;
- Endereço completo da residência permanente.

A comprovação dos elementos identificativos do cliente pode ser feita, nomeadamente, através do recurso à Chave Móvel Digital, da utilização eletrónica do cartão de cidadão ou do recurso à videoconferência.

Quando utiliza a videoconferência, tenha em atenção que:

- A videoconferência tem de ser gravada pelo banco e realizada em tempo real e sem pausas, com indicação da respetiva data e hora, e com som e imagem de qualidade;
- Durante a videoconferência, ser-lhe-á solicitado que mostre a frente e o verso do seu documento de identificação, para que o banco possa captar a imagem dos elementos de identificação, incluindo fotografia e assinatura;
- Durante a videoconferência, ser-lhe-á pedido que insira o "código único descartável" (OTP – *one-time password*) na plataforma de apoio à abertura de conta. O código é remetido pelo seu banco para o contacto que indicou (telemóvel ou *e-mail*).
- Poderão ainda ser-lhe solicitados outros documentos comprovativos, nomeadamente comprovativo de morada (por exemplo, uma fatura de água ou luz) e comprovativo da sua situação profissional (por exemplo, um recibo de vencimento).

#7 Guarde cópia do contrato de abertura de conta.

- Guarde a cópia do contrato de abertura de conta. O banco é obrigado a facultar-lhe esta cópia em suporte duradouro.

Após a abertura de conta

#8 Mantenha sempre atualizados os seus dados junto do banco.

- Deve comunicar ao banco quaisquer alterações verificadas nos elementos de identificação e nos dados de contacto que disponibilizou no momento de abertura de conta, como, por exemplo, a morada, o contacto telefónico ou o *e-mail*.

#9 Utilize a conta de forma responsável.

- Mantenha saldo na sua conta suficiente para os movimentos que realiza.
- A instituição pode permitir que utilize fundos além do saldo da conta, mas saiba que se trata de um crédito e que terá de reembolsar esse valor, acrescido de encargos.

#10 Saiba que tem direito a encerrar a conta sem custos.

- O encerramento da sua conta não tem encargos associados, mas pode ser-lhe exigido um prazo de pré-aviso, nunca superior a um mês. Isso significa que, depois de notificar o banco de que pretende encerrar a conta, ele tem, no máximo, um mês para o fazer.
- Poderá confirmar o encerramento da sua conta, através da consulta à Base de Dados de Contas Bancárias, disponível *online* através do *site* do Banco de Portugal, do Portal do Cliente Bancário, ou, presencialmente, nos respetivos postos de atendimento ao público.

Compras *online*

em segurança

#ficaadica

As compras *online* são uma forma cómoda e, por vezes, mais barata de adquirir bens e serviços. Mas há que ter alguns cuidados.

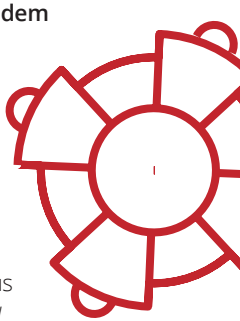
Procure informações sobre o vendedor e, caso avance com a compra, utilize sempre meios de pagamento com segurança acrescida.

Antes de fazer uma compra *online* ou através de *apps*

#1 Procure informações sobre o vendedor.

- Verifique se o vendedor é credível: pesquise na internet o nome da empresa ou procure referências junto de amigos ou conhecidos.
- Desconfie se não encontrar uma morada ou contactos telefónicos, ou os termos e condições da venda.
- Pesquise e leia sobre as experiências que outros clientes tiveram com determinado produto ou loja *online*, por exemplo, em fóruns de discussão.

Seja cauteloso perante ofertas irrecusáveis ou pechinchas, pois, frequentemente, correspondem a situações de fraude.



#2 Verifique a segurança do *site* ou da *app*.

- Confirme que o endereço a que pretende aceder se inicia com "https://" e que aparece um cadeado no final do endereço ou na barra inferior da janela. Se tal não acontecer, a página não é segura.
- Instale apenas aplicações obtidas em lojas de aplicações oficiais.
- Adote os procedimentos de segurança habituais para proteger o seu computador, *tablet* ou telemóvel:
  - Mantenha atualizados os programas de antivírus e anti-*spyware* e a *firewall* ativa;
  - Não clique em *links* nem faça *downloads* de fontes desconhecidas;
  - Não utilize redes *wi-fi* públicas ou desconhecidas;
  - Não utilize equipamentos públicos para realizar pagamentos *online*.

Não introduza os seus dados (nome, número de telemóvel, *e-mail*, cartão de cidadão, números de contas bancárias ou números de cartões de crédito) em *sites* que não conheça ou de cuja autenticidade desconfie.

#3 Leia os termos e condições.

- Verifique os métodos de pagamento disponibilizados.
- Informe-se sobre eventuais custos adicionais — por exemplo, custos de envio ou direitos alfandegários, se a loja estiver sediada fora da União Europeia.
- Verifique as condições e os custos em caso de devolução e de troca. Na União Europeia, tem 14 dias para devolver qualquer produto comprado na internet.

Quando faz a compra

#4 Certifique-se de que apenas disponibiliza os dados necessários para concluir a compra.

- Desconfie de solicitações de dados (por exemplo, palavras-passe, dados de documentos de identificação pessoal ou dados do cartão de pagamento) que lhe pareçam excessivas ou estranhas, ainda que provenientes de uma entidade aparentemente confiável. Em caso de dúvida, peça esclarecimentos ao seu banco ou outro prestador de serviços de pagamento, através dos contactos oficiais.

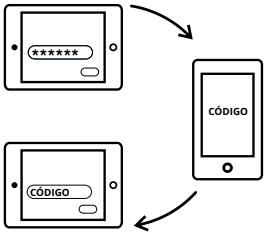
#5 Opte por uma forma de pagamento com segurança acrescida.

- **Referência multibanco.** O comerciante, caso disponibilize esta forma de pagamento, envia um SMS ou um *e-mail* com os dados para que efetue o pagamento, dentro de determinado prazo, num caixa automático ou através do *homebanking*.
- **Cartões com um saldo/*plafond* limitado e com prazo de validade reduzido,** como são os cartões

pré-pagos. Estes cartões limitam a possibilidade de reutilização indevida do cartão e o valor das perdas possíveis.

- **Cartões virtuais de utilização única ou com montante e prazo de validade limitados.** Um cartão virtual é um cartão gerado e utilizado em contexto eletrónico. No momento da compra, os dados do cartão real não são divulgados, tornando a operação mais segura. Esta funcionalidade pode ser disponibilizada pelo seu banco ou outro prestador de serviços de pagamento e por determinadas *apps* de pagamento.
- **Instrumentos de pagamento com segurança acrescida.** Prefira utilizar cartões com procedimentos de segurança acrescida como é o caso da versão mais recente do serviço *3D Secure*. Em regra, este serviço estará já ativo nos cartões de crédito ou de débito que permitem efetuar compras *online*. Caso não esteja, solicite a adesão/ativação junto do seu banco ou de outro prestador de serviços de pagamento. Neste caso, quando efetuar uma compra, ser-lhe-á, por norma, pedido que realize autenticação forte do cliente, isto é, que introduza dois elementos de autenticação válidos, em complemento aos dados do cartão *3D Secure*. Em Portugal, a solução mais comum para autenticação forte de operações *online* com cartão é a validação da operação na *app* do seu banco ou outro prestador de serviços de pagamento.

Autenticação forte



A autenticação forte é efetuada com, pelo menos, dois fatores de autenticação diferentes (p. ex., uma palavra-passe mais um código recebido no telemóvel)

Depois de fazer a compra

#6 Guarde os registos.

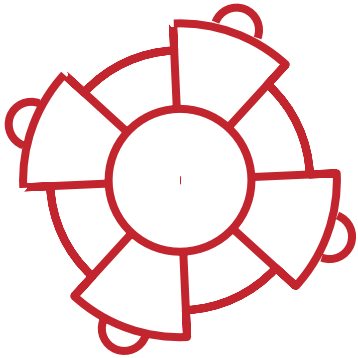
- Guarde os registos da compra efetuada, incluindo a informação sobre o comerciante e o respetivo endereço eletrónico. Sempre que possível, faça o *print screen* dos dados da operação.

#7 Verifique regularmente a sua conta.

- Consulte periodicamente os movimentos da conta e verifique se os movimentos realizados correspondem às compras que efetuou.

#8 Comunique as suspeitas de fraude.

- Caso suspeite de utilização abusiva ou não autorizada do seu cartão de pagamento ou se desconfiar que os seus elementos de identificação ou validação (como credenciais de acesso ao *homebanking*) foram utilizados indevidamente, comunique imediatamente essa situação ao seu banco ou outro prestador de serviços de pagamento, através dos contactos disponibilizados por este ou através dos contactos divulgados no *site* do Banco de Portugal e no Portal do Cliente Bancário.
- Comunique a situação ao órgão de polícia mais próximo (PSP, GNR ou PJ) ou ao Ministério Público.
- Se necessário, peça ao seu banco ou outro prestador de serviços de pagamento que cancele o cartão ou as credenciais de acesso ao *homebanking*.




Crédito
aos consumidores
online
Não vá
em cantigas
#ficaadica

Sabia que já é possível contratar produtos de crédito aos consumidores através de canais digitais, *online* ou *mobile*?

Confirme junto do banco se o produto de crédito que pretende contratar está disponível através de canais digitais e conheça as condições exigidas para o efeito.

Independentemente do canal de contratação utilizado, as instituições têm de lhe disponibilizar informação clara e completa nas várias fases do contrato e meios para que possa esclarecer todas as suas dúvidas.

Verifique se os seus rendimentos são suficientes para assegurar o pagamento da dívida que pretende contrair e de outras que já detenha. Tenha em atenção que as prestações do crédito são uma despesa mensal fixa do orçamento familiar, com impacto até à amortização total do empréstimo, pelo que deve ter em conta os rendimentos e as despesas que antecipa vir a ter no futuro.

Antes de contrair um crédito aos consumidores através de canais digitais

#1 Certifique-se de que a instituição está autorizada a conceder crédito.

- Confirme que a instituição está registada no Banco de Portugal e que está autorizada a conceder crédito. Nunca contrate um crédito com uma entidade não autorizada.

#2 Verifique a segurança do *site* ou da *app* da instituição.

- Confirme que o endereço a que pretende aceder se inicia com "https://" e que aparece um cadeado no final do endereço ou na barra inferior da janela. Se tal não acontecer, a página não é segura.
- Instale apenas aplicações obtidas em lojas de aplicações oficiais.
- Adote os procedimentos de segurança habituais para proteger o seu computador, *tablet* ou telemóvel:

- Mantenha atualizados os programas de antivírus e anti-*spyware*;
- Não clique em *links* nem faça *downloads* de fontes desconhecidas;
- Não utilize redes *wi-fi* públicas ou desconhecidas;
- Não utilize equipamentos públicos para realizar pagamentos ou outras operações bancárias.

Não introduza os seus dados (nome, número de telemóvel, *e-mail*, número de cartão de cidadão, números de contas bancárias ou números de cartões de crédito) em *sites* que não conheça ou de cuja autenticidade desconfie.

#3 Compare diferentes propostas antes de contratar o crédito.

- Preste informações verdadeiras e completas à instituição e diga claramente qual a finalidade do crédito que pretende contrair. Os diversos tipos de crédito aos consumidores têm diferentes finalidades, prazos e custos associados.
- Antes de tomar uma decisão sobre o crédito a contratar, compare diferentes propostas.
- As instituições devem apresentar-lhe com destaque, no ecrã ou na página principal da plataforma de comercialização, informação sobre as caraterísticas fundamentais do crédito, as comissões e eventuais despesas. Esta informação é apresentada em carateres de maior dimensão, caixas informativas, simulações, súmulas ou outros meios similares.
- Descarregue e leia atentamente a **ficha de informação normalizada**, documento que apresenta as principais caraterísticas do crédito.
- Analise com cuidado toda a informação prestada e:
  - Pondere todos os custos do crédito, verificando a TAEG — a taxa anual de encargos efetiva global — e o MTIC — o montante total imputado ao consumidor — das propostas de crédito;
  - Verifique se as propostas de crédito preveem a aquisição de outros produtos. A taxa de juro pode ser mais reduzida, caso aceite adquirir os produtos propostos; no entanto, esses produtos têm habitualmente custos;

– Tenha atenção ao prazo do empréstimo. Créditos com prazos mais longos têm, em geral, prestações mais baixas, mas terá de pagar juros por mais tempo.

#4 Esclareça todas as suas dúvidas antes de contratar o crédito.

- Informe-se sobre os procedimentos aplicáveis. As instituições são obrigadas a apresentar, no ecrã ou na página principal da plataforma de comercialização, as etapas do processo e os elementos necessários à contratação, de modo que seja evidente, desde o primeiro momento:
  - Quais são as várias fases do processo de contratação;
  - Se é necessário utilizar outros canais, dispositivos ou meios de comunicação no decurso do processo de contratação;
  - Quais são os documentos necessários para a contratação do crédito.
- As instituições devem prestar-lhe assistência a respeito do crédito, das fases do processo e da documentação necessária, disponibilizando, por exemplo, uma linha de atendimento ou de conversação ao vivo, um *chatbot*, respostas a perguntas frequentes, uma infografia ou um vídeo explicativo.

No momento da celebração de um contrato de crédito aos consumidores através de canais digitais

#5 Leia com atenção todos os documentos.

- Verifique as opções associadas ao crédito, como as vendas associadas facultativas de outros produtos (por exemplo, seguros ou cartões de crédito) ou o financiamento de encargos, e selecione-as apenas

forem vantajosas para si. Tenha em atenção que estas vendas não devem estar pré-selecionadas e são sempre facultativas, ou seja, não é obrigado a escolher nenhuma delas para aceder ao crédito. Tenha em atenção o eventual impacto no custo total do produto financeiro, verificando o efeito sobre a TAEG e o MTIC.

- Para que o processo de contratação avance, terá de percorrer todas as páginas dos documentos de informação obrigatórios, como a ficha de informação normalizada e a minuta do contrato, e confirmar a respetiva leitura no final dos documentos.

#6 Confirme a sua vontade de contratar o crédito.

- A instituição deve informá-lo previamente sobre os métodos disponíveis para confirmar a sua vontade de contratar o crédito, que podem incluir a assinatura eletrónica qualificada, a Chave Móvel Digital ou a autenticação forte do cliente.

Durante a vigência do contrato

#7 Pode exercer os seus direitos de livre revogação e de reembolso antecipado.

- Na plataforma de comercialização, no *site* ou na *app*, a instituição mutuante disponibiliza-lhe um espaço dedicado para comunicar o seu interesse em exercer o direito de livre revogação. Isto significa que tem 14 dias de calendário, contados a partir da data da assinatura do contrato, para desistir do contrato sem necessidade de justificar a decisão perante a instituição. Exercido o direito de revogação, tem de pagar à instituição, num prazo de 30 dias, o capital e os juros vencidos desde a data de utilização do crédito até à data do reembolso do capital.
- Para amortizar todo ou parte do crédito antes do prazo previsto no contrato, deve notificar a instituição pelos meios indicados para o efeito. Para exercer este direito de reembolso antecipado, poderá ter de pagar uma comissão.

#8 Analise a informação que a instituição lhe transmite durante o contrato.

- Esteja atento às comunicações que a instituição lhe envia, através de correio eletrónico, SMS ou notificações (*push notifications*), alertando-o para a disponibilização, na área privada da plataforma de comercialização, do *site* ou da *app* da instituição, de informação relevante (nomeadamente, a alteração de condições contratuais referentes a comissões e despesas eventualmente aplicáveis).
- Confira o extrato detalhado que a instituição lhe deve disponibilizar periodicamente com informação sobre a evolução do empréstimo.
- Informe-se quais são os meios ao seu dispor para apresentar uma reclamação ou recorrer a meios de resolução alternativa de litígios.

#9 Pague atempadamente as prestações acordadas e mantenha os seus dados atualizados junto da instituição.

- Pague pontualmente as prestações do empréstimo.
- Caso tenha ou antecipe vir a ter dificuldades em pagar as suas prestações, notifique a instituição, para que esta possa promover medidas que evitem o incumprimento (Plano de ação para o risco de incumprimento).
- Comunique sempre à instituição alterações de morada, de contactos ou outros dados relevantes.

A campanha #ficaadica é uma campanha de educação financeira digital do Banco de Portugal para promover a utilização segura de produtos e serviços bancários nos canais digitais.

Esta publicação reúne as dicas dirigidas à população em geral, que estão também disponíveis no **Portal do Cliente Bancário** — **https://clientebancario.bportugal.pt** —, na área de "Formação financeira", juntamente com outros materiais de apoio, no **Instagram** do Banco de Portugal — **@bancodeportugaloficial** — e no canal **YouTube** do Banco de Portugal — https://**www.youtube.com/@BancodePortugalOficial.**