5 DICAS
PARA FICARES MAIS SEGURO *ONLINE*
#ficaadica

BANCO DE PORTUGAL
EUROSISTEMA

5 dicas para ficares mais seguro *online* #ficaadica | 2018 • **Banco de Portugal** Av. Almirante Reis, 71 | 1100-012 Lisboa • www.bportugal.pt • **Edição** Departamento de Supervisão Comportamental • **Design** Departamento de Comunicação e Museu | Unidade de Design • **Tiragem** 30 000 exemplares • **ISBN (impresso)** 978-989-678-605-2 • **ISBN (*online*)** 978-989-678-606-9 • **Depósito Legal n.º** 448395/18

A forma como consumimos produtos e serviços financeiros mudou muito nos últimos anos. Hoje utilizamos estes produtos e serviços, em qualquer altura e em qualquer lugar, através do computador, do *smartphone* ou do *tablet*, de forma rápida e cómoda. Mas há riscos associados que devemos ter em conta, não só quando fazemos pagamentos ou quando utilizamos o *homebanking*, mas também quando partilhamos informações pessoais nas redes sociais, por *e-mail* ou por telefone, quando clicamos num *link* aparentemente inofensivo, quando fazemos um *download* ou descarregamos uma *app*. Convido alunos e professores a conhecerem algumas regras de segurança relacionadas com a utilização dos produtos e dos serviços financeiros. A educação financeira digital é fundamental na formação de consumidores esclarecidos, capazes de beneficiar do que de melhor a inovação tem para oferecer. **Fica a dica.**

Carlos da Silva Costa
Governador do Banco de Portugal

NÃO FAÇAS
DA INTERNET
UM JOGO
DE ALTO RISCO
#ficaadica

Quando navegas na internet tens noção dos riscos?

Cada vez mais ouvimos falar de *hackers* e piratas informáticos que acedem a dados pessoais de outras pessoas através de falhas de segurança nos computadores, telemóveis e *tablets* e nas contas de internet.

Phishing? *Spyware*? O que é isso?

Há pessoas que tentam passar-se por outras para obter os teus dados.

Um simples *download* pode instalar vírus que fazem abrir páginas onde te são pedidos dados pessoais.

Há aplicações e programas, aparentemente inofensivos, que espiam o que fazes.

Há ataques que direcionam todas as chamadas e SMS que recebes para outro telemóvel.

Phishing

Ocorre quando um *hacker* se faz passar por uma instituição ou empresa e, através de *e-mails*, de redes sociais, de chamadas ou SMS, tenta que divulgues informações pessoais.
Acontece quando recebes *e-mails* duvidosos com *links* que remetem para páginas falsas, que imitam por exemplo o *site* do banco e solicitam que preenchas um conjunto de dados.

Pharming

Ocorre quando um vírus informático instalado no computador, *tablet* ou telemóvel (*smartphone*) redireciona um *link* que escrevas para uma página falsa na *internet* (a chamada "página espelho"). Nalguns casos esta página é idêntica ao site do banco e permite a terceiros obter toda a informação pessoal que introduzes.

Este vírus pode ser instalado ao fazeres *download* de um ficheiro aparentemente inofensivo.

Spyware

Ocorre quando um programa malicioso é instalado no computador, *tablet* ou telemóvel (*smartphone*), sem que te apercebas, com o objetivo de espiar o teu equipamento e os teus dados.

Este programa pode ser instalado ao fazeres *download* de um ficheiro aparentemente inofensivo.

Uma vez instalado, o programa deteta se estás a aceder a *sites* protegidos, como as páginas de *homebanking*, e regista os dados inseridos, que depois podem ser usados indevidamente por outras pessoas.

SIM Card Swap

Ocorre, por exemplo, quando alguém recolhe informação sobre ti, diretamente ou nas redes sociais, e consegue fazer-se passar por ti numa loja de telecomunicações e solicitar uma segunda via do teu cartão de telemóvel.

Isto permite que todas as chamadas e SMS recebidas, incluindo *one-time passwords* (palavras-chave "descartáveis", válidas apenas para um acesso ao *homebanking* ou para uma transação, que são enviadas por SMS), sejam direcionadas para o cartão de telemóvel que está na posse daquela pessoa.

O que podes fazer para te proteger?

Protege o teu computador, *tablet* ou telemóvel

- Define *passwords* e cria sequências de bloqueio de ecrã para que o teu equipamento não seja utilizado por terceiros;
- Não permitas que *sites* ou aplicações com informação confidencial se iniciem automaticamente, sem ser necessário fazer o *login*;
- Mantém atualizados o sistema operativo e os programas de antivírus e anti-*spyware* em todos os teus equipamentos. Mantém a *firewall* ativa;
- Evita utilizar equipamentos públicos (computadores partilhados, por exemplo), principalmente quando pretendes realizar operações bancárias ou pagamentos.

Protege as ligações de internet

- Não te ligues a redes *wi-fi* públicas ou desconhecidas;
- Não abras *e-mails* de caráter duvidoso. O *e-mail* tem erros? É escrito noutra língua? Não é normal que te contactem com aquele género de *e-mail*? Desconfia

e informa-te diretamente com a pessoa ou pelos canais oficiais da entidade que, alegadamente, te está a contactar (por exemplo, o banco, a loja *online*, a entidade de serviços de entrega...);

- Não cliques em *links* desconhecidos nem faças *downloads* de fontes desconhecidas;
- Não abras anexos de *e-mails* enviados por remetentes que não conheces;
- Digita sempre o endereço eletrónico ao qual pretendes aceder, em vez de usares um *link* ou de acederes ao histórico da *internet*;
- Verifica se o endereço a que pretendes aceder se inicia com https:// e que aparece um cadeado no final do endereço ou na barra inferior da janela. Isto significa que a ligação é segura;
- Podes testar se o *site* é seguro usando o "truque da senha errada". Em vez do teu *login* habitual, coloca uma *password* errada. Se for aceite, isso significa que a entidade em causa não está a verificar o teu *login* (ou seja, pode estar a querer apenas recolher a *password* que escreves para utilizá-la de forma indevida);
- Instala apenas aplicações com caráter fidedigno, obtidas em lojas de aplicações oficiais. Nem todas as aplicações são seguras e podem conter *software* malicioso.

Protege os teus dados

- Não divulgues as tuas *passwords* a terceiros;
- Não escrevas *passwords* ou outra informação confidencial em papel, nem guardes essa informação em *e-mails* ou no telemóvel;
- Cria *passwords* que não sejam fáceis de adivinhar e utiliza diferentes *passwords* para diferentes contas;
- Não introduzas os teus dados (nome, número de telemóvel, *e-mail*, cartão de cidadão, números de conta bancária) em *sites* que não conheças ou de cuja autenticidade desconfies. Em caso de dúvida, fecha a janela e tira dúvidas com os teus pais e com as entidades que habitualmente contactas (por exemplo, o banco ou a loja *online*).

O TELEMÓVEL REVELA DEMASIADO SOBRE TI

#ficaadica

Usas o telemóvel (*smartphone*) para acederes às redes sociais ou ao *e-mail*? E ao *homebanking*? Fazes pagamentos com o telemóvel?

O telemóvel pode alojar uma grande quantidade de informação confidencial sobre ti e sobre as operações que fazes.

Usas o telemóvel para tudo e mais alguma coisa?

Navegas em qualquer lugar?

Pintas-te por uma boa *app*?

O que podes fazer para te proteger?

Dificulta o acesso ao teu telemóvel

- Constrói *passwords* seguras, que não sejam demasiado óbvias (por exemplo, nunca uses palavras-passe como "123456" ou a tua data de nascimento);
- Define uma sequência de bloqueio de ecrã do telemóvel e troca-a com regularidade.

Protege as ligações de internet

- Não permitas que *sites* ou aplicações se iniciem automaticamente, sem ser necessário fazer *login*;
- Atualiza regularmente os programas que protegem o teu telemóvel, como programas de antivírus;
- Não ligues o telemóvel a redes *wi-fi* públicas ou desconhecidas;
- Não cliques em *links* nem faças *downloads* de fontes desconhecidas.

Utiliza *apps* seguras e em segurança

- Instala apenas *apps* fidedignas, através de lojas de aplicações oficiais;
- Se a oferta parecer demasiado boa, desconfia. Se sabes que uma *app* ou serviço normalmente é pago e encontras uma versão gratuita, tem em atenção que essa versão pode conter vírus;
- Verifica as permissões de acesso aos dados exigidos pelas *apps*. Pede-te acesso à câmara do telemóvel em qualquer momento? E ao microfone? Não descarregues aplicações que exijam permissões aparentemente excessivas.

PENSA ANTES
DE "POSTAR"
#ficaadica

As redes sociais são a tua segunda casa?

As redes sociais permitem que fales e partilhes informação com amigos de todo o mundo, que conheças iniciativas do teu interesse, vídeos que te divertem, projetos de solidariedade.

Mas, como tudo, também têm os seus riscos.

Fazes *posts* a torto e a direito?

Dizes tudo sobre ti?

O que podes fazer para te proteger?

Gere as definições de privacidade

- Deves modificar as definições de privacidade do teu perfil nas redes sociais para que apenas "amigos" ou "seguidores" possam ver o que partilhas;
- Podes bloquear pessoas ou um grupo de pessoas específicas, impedindo-as de ver o teu perfil.

Pensa antes de partilhar

- Não divulgues informações pessoais ou confidenciais. Por exemplo, não divulgues as tuas *passwords* nem fotografias dos teus cartões bancários;
- Pondera se é necessário partilhares informação como a tua data de aniversário, o teu número de telefone, o nome da tua escola. Se não é necessário, não divulgues;
- O que partilhas nas redes sociais pode ser visto e partilhado por outros e pode ser mal interpretado ou utilizado de forma fraudulenta;
- Mesmo que apagues informação, esta pode ter sido vista, gravada ou partilhada antes de ter sido eliminada;
- Não partilhes imagens ou vídeos sem autorização das pessoas envolvidas.

Informa-te sobre as políticas de gestão de dados

- Criar um perfil numa rede social é, em geral, gratuito. No entanto, muitas vezes as empresas que gerem as plataformas sociais recolhem os teus dados e armazenam tudo o que gostas, comentas ou partilhas, para que possam, por exemplo, dirigir-te publicidade específica;
- Consulta a forma como os teus dados são utilizados na Política de Dados da rede social.

NÃO COMPRES (*ONLINE*) GATO POR LEBRE

#ficaadica

Fazes as tuas compras *online* em segurança?

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

Fazes compras *online* de olhos fechados?

Fazes compras de forma segura?

Vais logo direto ao que interessa?

Dás tudo o que te pedem?

Fazes a compra e já está?

O que podes fazer para te proteger?

Antes de fazeres uma compra *online* ou através de *apps*, informa-te

Procura informações sobre o vendedor

- Pesquisa na internet pelo nome da empresa;
- Desconfia se não encontrares uma morada ou um contacto de telefone para o qual possas ligar e os termos e condições da venda;
- Lê sobre as experiências que outros clientes tiveram com determinado produto ou loja *online*, por exemplo em fóruns de discussão.

Verifica a segurança do site ou da *app*

- Verifica se o endereço a que pretendes aceder se inicia com https:// e se aparece um cadeado no final do endereço ou na barra inferior da janela. Isto significa que a ligação é segura;
- Instala apenas aplicações com caráter fidedigno, obtidas em lojas de aplicações oficiais.

Adota os procedimentos de segurança habituais para proteger o teu computador, *tablet* ou telemóvel

- Mantém atualizados os programas de antivírus e anti-*spyware* e a *firewall* ativa;
- Não utilizes redes *wi-fi* públicas ou desconhecidas;
- Não utilizes equipamentos públicos para realizar pagamentos.

Lê os termos e condições

- Verifica os métodos de pagamento;
- Informa-te sobre eventuais custos adicionais – custos de envio ou direitos alfandegários, se a loja estiver sediada fora da União Europeia (UE);
- Verifica as condições e os custos em caso de devolução e de troca. Por norma, na UE tens 14 dias para devolver qualquer produto comprado na *internet*.

Quando fazes a compra, opta por uma forma de pagamento segura

Certifica-te de que apenas disponibilizas os dados necessários para concluir a compra

Opta, preferencialmente, por uma das seguintes formas de pagamento:

- Referência multibanco. Neste caso, a loja envia-te uma mensagem ou *e-mail* com os dados para efetuares o pagamento, dentro de determinado prazo, num caixa automático ou através do *homebanking*;
- Cartões virtuais. A aplicação MB WAY, por exemplo, permite-te gerar cartões virtuais MB NET. Assim, quando efetuas o pagamento inseres os dados do cartão virtual e não os dados do cartão real;
- Instrumentos de pagamento com segurança acrescida, como cartões com um limite de crédito baixo, com prazo de validade reduzido ou com procedimentos de autenticação adicionais. Com o *3-D Secure*, por exemplo, podes fazer compras *online* seguras com os dados reais do teu cartão, porque beneficias de métodos acrescidos de segurança no ato de pagamento. O *site* onde efetuas a compra tem de ter este sistema, apresentando as denominações *Verified by Visa*, *SecureCode* ou *SafeKey*. Quando estiveres a fazer o pagamento num vendedor *3-D Secure*, além dos dados do teu cartão, deves introduzir as credenciais de autenticação, que pode ser, por exemplo, um código enviado por SMS para o teu telemóvel.

Depois de fazeres a compra

- Guarda os registos da compra efetuada, incluindo a informação sobre o vendedor;
- Consulta periodicamente a tua conta bancária e verifica se os movimentos realizados correspondem às compras que efetuaste.

NÃO CEDAS
À FRAUDE
#ficaadica

E se fores vítima de fraude *online*?

Quando realizas operações bancárias e pagamentos através da *internet*, está atento a possíveis situações de fraude.

Em caso de dúvida, fecha a janela e tira dúvidas com os teus pais e com o teu banco.

Desconfias de uma situação fraudulenta?

Não sabes do teu cartão bancário?

Tiraram-te dinheiro da conta sem autorização?

O que podes fazer para te proteger?

Se desconfiares de fraude, age rapidamente

- Contacta imediatamente o teu banco através dos contactos que este te indicou ou através do contacto constante na lista de emissores dos cartões de pagamento, disponível no *site* do Banco de Portugal e no Portal do Cliente Bancário;
- Pede imediatamente o cancelamento das credenciais de acesso ao *homebanking* ou, se for o caso, do cartão;
- Participa a situação fraudulenta ao órgão de polícia criminal mais próximo (PSP, GNR ou PJ) ou ao Ministério Público.

Se perderes o cartão bancário, participa o desaparecimento

- Contacta imediatamente a entidade que emitiu o cartão se o tiveres perdido, se ele tiver sido roubado, furtado ou apropriado indevidamente por alguém, ou se suspeitares que o cartão foi clonado ou falsificado;
- Podes consultar os contactos das entidades emitentes de cartões no *site* do Banco de Portugal e no Portal do Cliente Bancário.

Conhece os teus direitos e deveres

- Se forem realizadas operações de pagamento que não autorizaste, podes ter de suportar até um máximo de 50 euros;
- Se mentires ou se não tiveres cumprido as regras de segurança, podes ter de suportar um valor superior a 50 euros;
- Caso tenha havido perda, roubo ou apropriação indevida das credenciais de acesso ao *homebanking* ou do cartão e caso tenhas alertado o teu banco desse facto, não poderás ser chamado a pagar os valores que forem movimentados sem autorização após esse alerta.

O Banco de Portugal reúne nesta publicação os materiais da campanha de educação financeira digital **#ficaadica**, promovida para sensibilizar os jovens em idade escolar para os cuidados a observar nos canais digitais, no acesso a produtos e serviços bancários.

Esta publicação é dirigida a escolas secundárias de todo o país e está também disponível no **Portal do Cliente Bancário – https://clientebancario.bportugal.pt** –, na área de "Formação financeira", juntamente com outros materiais de apoio e no **Instagram** do Banco de Portugal – **@bancodeportugaloficial**.