Em caso de fraude...

- **Contacte imediatamente a instituição que lhe presta serviços bancários ou de pagamento**, se desconfiar de uma situação fraudulenta ou detetar movimentos que não autorizou.

  > Utilize os contactos indicados pela sua instituição ou consulte a lista de contactos dos emissores dos cartões de pagamento disponível no Portal do Cliente Bancário.

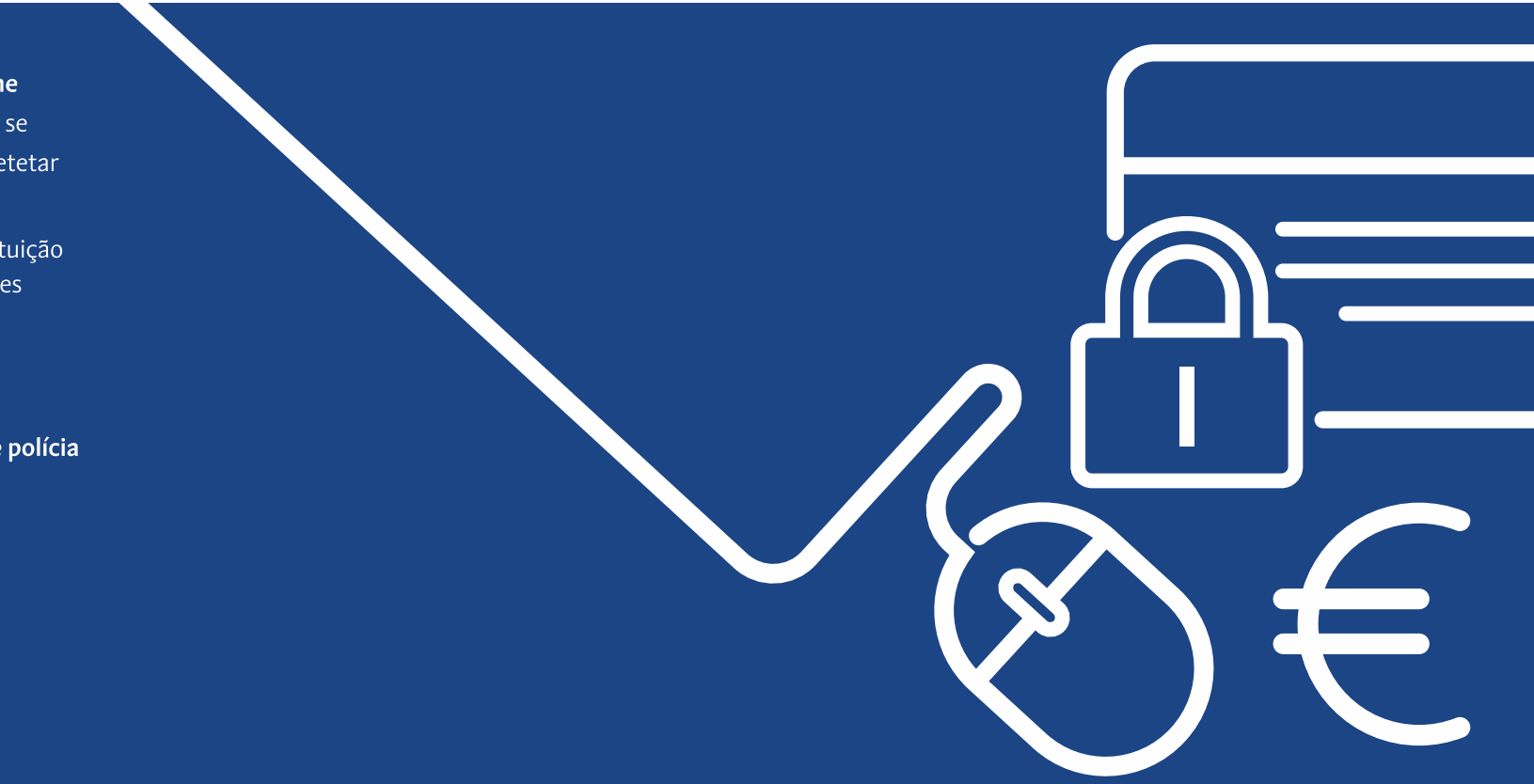
- **Participe a situação fraudulenta ao órgão de polícia criminal mais próximo (PSP, GNR ou PJ)** ou ao Ministério Público.

http://clientebancario.bportugal.pt
Direitos dos clientes • Prevenção de fraude

BANCO DE PORTUGAL
EUROSISTEMA

Segurança *online*

Prevenção de fraude



Fraude *online*

Quando realiza operações bancárias e pagamentos através da *internet* esteja atento a situações fradulentas, como:

- ***Phishing*** – ocorre quando uma entidade desconhecida (*hacker*) se faz passar por uma instituição ou empresa e, através de mensagens de correio eletrónico (*email*), de chamadas telefónicas ou de mensagens de telemóvel (*SMS*), tenta persuadir um cliente bancário a divulgar informações pessoais, tais como palavras-passe e números de contas bancárias.

- ***Pharming*** – ocorre quando um vírus informático instalado num computador, *smartphone* ou *tablet* redireciona a hiperligação (*link*) inscrita pelo cliente para uma página de *internet* falsa, nalguns casos idêntica à página oficial da instituição, permitindo a obtenção de informação confidencial do cliente. Este vírus pode ser inadvertidamente instalado pelo cliente através do *download* de um ficheiro aparentemente "inofensivo".

- ***Spyware*** – consiste num programa malicioso que se instala no computador, *smartphone* ou *tablet* do cliente sem que este se aperceba. Uma vez instalado, deteta se o cliente está a aceder a uma página de *internet* protegida e regista os dados inseridos pelo utilizador.

Prevenir a fraude *online*

Para realizar operações bancárias e pagamentos, com segurança, através da *internet*, utilizando um computador, um *smartphone* ou um *tablet*, deve ter em conta alguns cuidados:

Proteja os seus dados pessoais e a informação confidencial

- **Não utilize palavras-passe demasiado óbvias** (por exemplo, 123456) ou associadas a informação pessoal fácil de obter (como a data de nascimento).
- **Não divulgue palavras-passe a terceiros**, uma vez que são pessoais e intransmissíveis.
- **Não inscreva dados confidenciais** e outras informações **em sítios de *internet* cuja autenticidade não esteja assegurada**.

Proteja as ligações de *internet*

- **Proteja o equipamento que usa para aceder à *internet***, computador, *tablet*, *smartphone*, com programa antivírus e *anti-spyware* e utilize uma *firewall*. Mantenha os programas atualizados.
- **Evite utilizar equipamentos públicos** (computadores ou *tablets* partilhados) para realizar operações bancárias ou pagamentos.
- **Não abra e elimine** imediatamente **mensagens de correio eletrónico** (*email*) **de carácter duvidoso**.
- **Evite clicar** em hiperligações (*links*) ou fazer *downloads* de **fontes desconhecidas**.
- **Digite sempre o endereço eletrónico pretendido**, não acedendo à página através de hiperligações (*links*) em mensagens de correio eletrónico (*email*), de endereços gravados nos "Favoritos" ou no "Histórico" ou dos resultados de pesquisas em motores de busca.
- Verifique que o **endereço do sítio a que pretende aceder se inicia com https://** e que aparece um cadeado no final do endereço ou na barra inferior da janela.

Proteja-se de atividade não autorizada

- **Certifique-se que a instituição está autorizada** a prestar serviços bancários ou a realizar pagamentos através da *internet*.
- **Consulte a lista de instituições autorizadas** a prestar serviços bancários ou de pagamento em Portugal no Portal do Cliente Bancário.

Nas compras através da *internet*:

- **Procure primeiro informações sobre o vendedor**.
- **Prefira utilizar instrumentos de pagamento com caraterísticas de segurança acrescidas** (cartões com um limite de crédito, com uma reduzida data de validade e com procedimentos de autenticação adicionais) **ou crie um cartão virtua**l (em caixa automático ou no *homebanking*).
- **Guarde os registos das operações efetuadas** através da *internet*.
- **Consulte periodicamente a sua conta** e verifique os movimentos realizados.

No Portal do Cliente Bancário pode obter mais informações, nomeadamente, sobre:

- Prevenção da fraude
- Lista de instituições autorizadas a prestar serviços bancários e de pagamento
- Lista de contactos dos emissores de cartões de pagamento

Informe-se sobre os cuidados a ter na utilização de serviços bancários e nos pagamentos através da *internet*.