

## As fraudes mais recentes

---

### 1. Phishing a Dados de Cartões de Crédito (Dezembro de 2009)

Um esquema recentemente utilizado tem como objectivo capturar os dados de cartões de crédito. Para esse efeito recorre a PCs que estejam infectados com código malicioso e, após o utilizador introduzir os dados de login do seu serviço de internet banking (user e password), o acesso é redireccionado para um site fraudulento, em que é solicitado ao utilizador a introdução de dados referentes ao cartão de crédito.



### 2. Novo e-mail fraudulento (Dezembro de 2009)

Surgiu um novo e-mail de cariz fraudulento que visa infectar os computadores dos utilizadores que acedam aos links nele contidos, para posterior obtenção fraudulenta das credenciais de autenticação a serviços de Internet Banking.



O acesso aos links despoleta o download de código malicioso, passível de infectar o computador que está a ser utilizado.

Nos computadores infectados, ao aceder ao Caixadirecta on-line, ao Caixa e-Banking bem como a outros serviços bancários on-line, são apresentados ecrãs falsificados a solicitar os códigos de acesso e outras credenciais de autenticação do cliente.



**Autenticação**

Bem-vindo ao Internet Banking da CGD

|   | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| A |   |   |   |   |   |   |   |   |
| B |   |   |   |   |   |   |   |   |
| C |   |   |   |   |   |   |   |   |
| D |   |   |   |   |   |   |   |   |
| E |   |   |   |   |   |   |   |   |
| F |   |   |   |   |   |   |   |   |
| G |   |   |   |   |   |   |   |   |
| H |   |   |   |   |   |   |   |   |

Nº Cartão Matriz:  Nº Contribuinte:

Se ainda não é cliente, active o serviço Caixa directa on-line.

**Virus nos PCs simulam Caixadirecta on-line**

Caixa está mudando seus métodos de identificação dos seus utilizadores para maior segurança dos nossos clientes. Agradecemos quando solicitado o preenchimento do cartão matriz, responda correctamente para melhor atendê-lo.

Necessário recadastramento do cartão matriz.

Gravar

Utilitários

Get PDF/XP/READER

Verifique Seguro

CGD © 2009 Todos os direitos reservados | Linha de apoio 707 24 24 24 (24 horas por dia/todos os dias do ano)

Se recebeu algum e-mail deste teor, deverá apagá-lo de imediato, não acedendo ao link disponibilizado. Caso tenha acedido ao link contido no email, deverá contactar de imediato a linha de apoio 707 24 24 24 (24 horas por dia/todos os dias do ano) e dar conhecimento dessa situação.

### 3. Falsa "Notícia de Lisboa"

Mais um caso de phishing que utiliza uma notícia falsa, de forma a induzir o receptor do email a seleccionar o link.

**Falsa “Notícia de Lisboa” (Outubro de 2009)**

From: @hotmail.com  
To:  
Subject: Notícia direto de Lisboa  
Date: Tue, 27 Oct 2009 18:22:37 +0000

**Governo oferece apoio de Lisboa para resolver situação de Alexandra**

A menina russa retirada de uma família portuguesa desapareceu na Rússia, agora o caso está sendo investigado pela Interpol.

Confira os vídeos e notícias dela na Rússia

vídeos e notícias

**Fraude**

Link fraudulento, o acesso ao alegado vídeo e notícias é passível de infectar o computador do utilizador com **software malicioso**.

Se recebeu este email, deverá apagá-lo de imediato, não acedendo aos *link's* disponibilizados. Caso tenha utilizado os *link's* contidos no email, deverá contactar de imediato a linha de apoio 707 24 24 24.

#### 4. Phishing em nome da CLIX, Vodafone e PSP (Outubro 2009)

Os últimos ataques de phishing têm como modo de ataque preferencial a utilização abusiva do nome de entidades não-bancárias, nomeadamente a CLIX, Vodafone e a PSP (Polícia de Segurança Pública).

## Falso "Postal Clix" (Outubro de 2009)

From: postais@clix.pt  
Sent: segunda-feira, 26 de Outubro de 2009  
To:  
Subject: Você recebeu um Clix Postal!

Remetente falsificado, o email não foi enviado pelo Clix

Olá!

Alguém preparou-lhe uma surpresa a partir do canal de postais do Clix.

Consulte o seguinte endereço Web:

<http://www.postais.clix.pt/ver.html?id=4346973&id=22092>

Espero que goste!

Para visualizar a página referida, clique no endereço Web indicado. O postal enviado estará disponível para visualização durante os próximos 15 dias.

Imprima os seus postais utilizando as opções que o canal de postais do Clix lhe oferece e guarde, para sempre, a recordação de um momento muito especial.

Envie postais pelo Clix, gratuitamente e sempre que quiser, em <http://www.postais.clix.pt>.

Link fraudulento, a página acedida não é do Clix sendo passível de infectar o computador do utilizador com **software malicioso**.

O intuito dos emails é induzir o receptor a aceder ao link ou ao ficheiro em anexo, de forma a que seja **instalado no computador um vírus** que depois permitirá a **captura de dados confidenciais**, como por exemplo os códigos de acesso a sites de banca à distância.

## Falsa "Mensagem Vodafone" (Outubro de 2009)

From: mensagem@vodafone.pt  
To:  
Cc:  
Subject: Vodafone - Mensagem Multimídia

Remetente falsificado, o email não foi enviado pela Vodafone



Link fraudulento, a página acedida não é da Vodafone sendo passível de infectar o computador do utilizador com **software malicioso**.

Se recebeu estes *email's*, deverá apagá-los de imediato, não acedendo aos *link's* disponibilizados. Caso tenha utilizado os *link's* contidos nos *email's*, deverá contactar de imediato a linha de apoio 707 24 24 24.

**Falsa "Convocatória PSP" (Outubro de 2009)**

From: psp [investigacoes@psp.pt]  **Remetente falsificado, o email não foi enviado pela PSP**

To:

Cc:

Subject: Convocatória Judicial

**PROCEDIMENTO INVESTIGATÓRIO N.º 812.217/2009**

 **Fraude**

COMPARECIMENTO EM JUÍZORIA

Relativa ao procedimento investigador em epígrafe, em relação a passada noite de 17 de Setembro de 2009 decorrido em crime público, como poderá verificar abaixo.

ANEXO: CONVOCATÓRIA-PSP

 **Link fraudulento, a página acedida não é da PSP sendo passível de infectar o computador do utilizador com software malicioso.**

© Polícia de Segurança Pública © todos os direitos reservados

Saiba como reconhecer um [e-mail fraudulento](#).

## 5. Phishing em nome da CGD (Setembro 2009)

Foram enviados emails com remetentes falsificados, aparentando ter origem na CGD, que alertam para um suposto bloqueio do Caixadirecta no-line.

## Phishing (1) em nome da Caixa (Setembro de 2009)

From: Caixa Directa Online [onlinebanking@cgd.com]  
To: [redacted]  
Cc: [redacted]  
Subject: [redacted] Message Update:

Remetente falsificado, o email não foi enviado pela Caixa



Seu acesso esteve suspenso.

amavelmente siga a ligação abaixo em ordem restabelecer a sua conta e então assegurar a segurança e segurança de sua conta.

[Clique aqui para restabelecer sua conta](#)

Ns nos desculpamos para qualquer inconveniência causada por esta ao.

Obrigado,  
Caixa Directa on-line.

Link fraudulento, a página acedida não é da Caixa.

Na verdade tratam-se de email de phishing que visam solicitar elementos de acesso ao serviço e instalar vírus no computador utilizado.

## Phishing (2) em nome da Caixa (Setembro de 2009)

From: Caixa Directa Online [mailto:notification@cgd.pt]  
Sent: [redacted]  
To: [redacted]  
Subject: Security Message:

Remetente falsificado, o email não foi enviado pela Caixa



Seu Caixa que conta bancária On-line precisa ser atualizada

**Fracasso para atualizar sua conta conduzir para consertar suspenso.**

amavelmente siga a ligação abaixo em ordem atualizar sua conta e então assegurar a segurança e segurança de sua conta:

[Atualização de perfil](#)

Ns nos desculpamos a tudo de nossos clientes para o inconveniente ns poderamos ter causado e poderamos ter prometido se esforçar mais duro para evitar tal embala no futuro

Obrigado!,  
Caixa Directa on-line

Link fraudulento, a página acedida não é da Caixa.

**Alertamos todos os clientes** e em especial os utilizadores do Caixadirecta on-line para a necessidade de se manterem particularmente atentos à detecção e prevenção deste tipo de fraude.

Saiba como reconhecer um [e-mail fraudulento](#).

## Falso "Comprovante Depósito" (Setembro 2009)

Um outro exemplo de um email de phishing, que apela à curiosidade do leitor ao indicar que foi recebida uma transferência.



O acesso ao suposto comprovativo da transferência despoleta a instalação de vírus no computador.

**Esteja atento à linguagem utilizada.** É frequente encontrar **erros grosseiros ou expressões pouco comuns** nestes textos, que facilmente excluem a hipótese de se estar perante uma comunicação autêntica da Caixa.

Saiba como [proteger o seu computador](#).

## E-mails ilícitos em nome de autoridades policiais (Setembro 2009)

Circulam e-mails de cariz fraudulento, enviados abusivamente em nome de autoridades policiais (Polícia Judiciária e PSP).



## Falso “Alerta Polícia Judiciária Online” (Setembro de 2009)

Subject: [POLÍCIA JUDICIÁRIA] Tentativa de acesso indevido.



POLÍCIA JUDICIÁRIA ONLINE

### ALERTA

Foi detectada varias tentativas de acesso indevido vindo de seu endereço IP. Você deve utilizar o modulo de proteção da **Microsoft** para que isso não aconteça.

[Clique para instalar](#)

(c) 2009 Polícia Judiciária 2009/2009. Todos os direitos reservados



O acesso ao link despoleta o download de **código malicioso**.

É importante assinalar que a página acedida através do link **não** é da Polícia Judiciária.

Na realidade, tratam-se de mensagens forjadas que visam infectar os computadores dos utilizadores que acedam aos links contidos nesses e-mails, para posterior recolha de credenciais de autenticação de clientes de serviços de Internet Banking com fins fraudulentos.

### Falsa "Convocatória Judicial PSP" (Setembro de 2009)



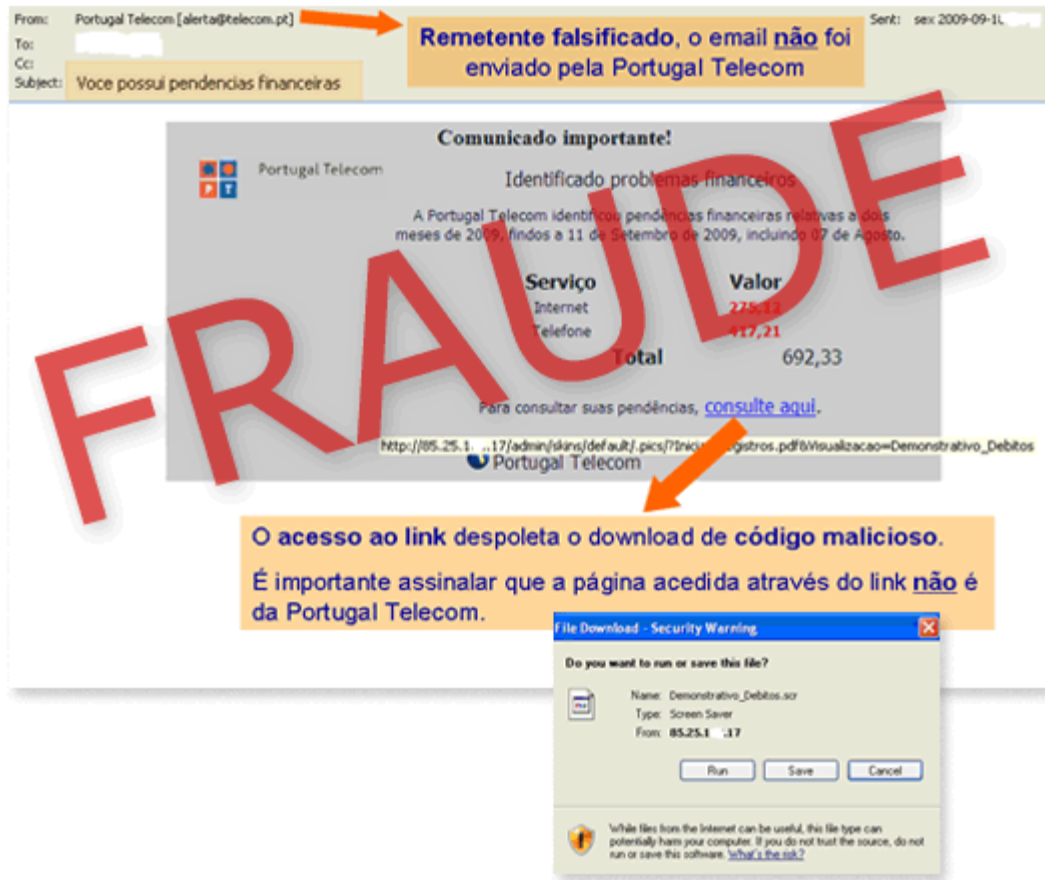
O alegado Anexo é na realidade um [link](#) cujo acesso despoleta o download de **código malicioso**.

É importante assinalar que a página acedida através do link [não](#) é da PSP.

Se recebeu estes *email's*, deverá apagá-los de imediato, não acedendo aos *link's* disponibilizados. Caso tenha utilizado os *link's* contidos nos *email's*, deverá contactar de imediato a linha de apoio 707 24 24 24 e dar conhecimento dessa situação.

### Falso comunicado da Portugal Telecom (Setembro 2009)

Foram recebidos e-mails que simulam ter como remetente a Portugal Telecom, os quais, não tendo efectivamente essa origem, apelam à curiosidade dos seus destinatários mencionando supostos atrasos em pagamentos à entidade. Na realidade, o acesso ao link contido no email visa apenas infectar o computador utilizado, para posterior recolha de credenciais de autenticação de serviços de Internet Banking de diversos bancos com fins fraudulentos.



O acesso ao link deste e-mail despoleta o download de código malicioso passível de infectar o computador que está a ser utilizado. Nos computadores infectados, num próximo acesso ao Caixadirecta on-line ou a outros serviços bancários on-line, são apresentados ecrãs falsificados a solicitar os códigos de acesso e outras credenciais de autenticação do cliente, com propósitos fraudulentos.



## Falso e-mail de fotografias (Setembro 2009)

### Falsa solicitação de códigos após autenticação

Foram recebidos emails falsificados incentivando à visualização de fotos de cariz pessoal. Contudo, o acesso ao link contido no email visa apenas infectar o computador utilizado, para posterior recolha de credenciais de autenticação de serviços de Internet Banking da Caixa e de outros bancos com fins fraudulentos.

O acesso ao link deste e-mail despoleta o download de código malicioso passível de infectar o computador que está a ser utilizado.

Nos computadores infectados, num próximo acesso ao Caixadirecta on-line, Caixa e-Banking ou a outros serviços bancários on-line, são apresentados ecrãs falsificados a solicitar os códigos de acesso e outras credenciais de autenticação do cliente, com propósitos fraudulentos.

Se recebeu estes *email's*, deverá apagá-los de imediato, não acedendo aos *link's* disponibilizados. Caso tenha utilizado os *link's* contidos nos *email's*, deverá contactar de imediato a linha de apoio 707 24 24 24 e dar conhecimento dessa situação.

## 6. Emails fraudulentos (Agosto 2009)

### Falsa solicitação de códigos após autenticação

Este tipo de fraude é baseada em código malicioso que infectou previamente o computador do cliente. Num próximo acesso ao serviço Caixadirecta on-line, neste caso após autenticação do cliente no serviço, é sobreposto um ecrã falsificado a solicitar, com fins fraudulentos, mais de 3 dígitos do cartão matriz bem como o código de acesso. Em fundo permanece a imagem do Caixadirecta on-line.



Os receptores deste email não deverão aceder ao link, pois despoleta a instalação de software malicioso que infecta o computador que está a ser utilizado. Aquando do acesso a serviços de internet banking, seria depois sobreposta uma página falsificada a solicitar a totalidade ou parte das credenciais de autenticação para fins fraudulentos.

Se recebeu este email, deverá apagá-lo de imediato, não acedendo ao link disponibilizado. Caso tenha utilizado o link contido no email, deverá contactar de imediato a linha de apoio 707 24 24 24 e dar conhecimento dessa situação.

Relembramos que deverá sempre desconfiar de emails que disponibilizem links, contenham anexos ou que solicitem a instalação de programas, mesmo que aparentemente o email tenha origem em entidades conhecidas. Apague as mensagens de correio electrónico de origem ou conteúdo duvidoso (ainda que o assunto seja apelativo) sem as ler. Não reencaminhe nem responda a essa mensagem. O mesmo se aplica aos ficheiros em anexo.

## **9. Pedido parcial dos dígitos do cartão matriz após autenticação no Caixadirecta on-line**

Este tipo de fraude consiste em instalar no computador do cliente um código malicioso que faz com que, quando o cliente se autentica no Caixadirecta on-line, sejam solicitados alguns dígitos do cartão matriz. Em background continua visível a imagem do Caixadirecta on-line.

Exemplo deste tipo de fraude:

Em autenticações futuras são solicitadas outras coordenadas do cartão matriz, até que o cliente acabe por introduzir o cartão matriz completo.

**Esteja atento à linguagem utilizada.** É frequente encontrar **erros grosseiros ou expressões pouco comuns** nestes textos, que facilmente excluem a hipótese de se estar perante uma comunicação autêntica da Caixa.

Exemplo de expressão utilizada no texto em cima: "Autenticação>Liberar Secção"

Saiba como [proteger o seu computador](#).

## **10. Envio de e-mails fraudulentos**

Os clientes da Caixa recebem e-mails que não são enviados pela CGD, simulando que o são, com o objectivo de recolher os dados do cartão matriz e os códigos de acesso ao Caixadirecta on-line para posterior utilização fraudulenta.

Exemplo de email fraudulento:

No computador infectado, aquando do acesso ao Caixadirecta on-line é sobreposta uma página falsificada a solicitar as credenciais de autenticação:

A fraude prossegue com a solicitação de todas as coordenadas do cartão matriz e alguns dados adicionais:

**Alertamos todos os clientes** e em especial os utilizadores do Caixadirecta on-line para a necessidade de se manterem particularmente atentos à detecção e prevenção deste tipo de fraude.

Saiba como reconhecer um [e-mail fraudulento](#).

## **11. Pedido de dígitos do cartão matriz no login do Caixadirecta on-line**

A Caixa nunca pede dígitos do cartão matriz no login. No caso de tal já lhe ter acontecido, o PC que está a utilizar talvez tenha instalado software malicioso que compromete a segurança dos seus dados e códigos de autenticação bancários. Não volte a utilizar e contacte-nos de imediato através dos Telefone 707 24 24 24, 96 200 24 24, 91 405 24 24 ou 93 200 24 24.

Para entrar no serviço Caixadirecta on-line apenas são necessários o Número de contrato e o Código de acesso, nunca sendo solicitados dígitos do cartão matriz ou quaisquer outros dados. O Caixadirecta on-line pede apenas 3 dígitos do cartão matriz e exclusivamente para validação de operações solicitadas pelo cliente. Qualquer outro tipo de pedido, mesmo que lhe pareça que é a CGD que lhe está a solicitar, é fraude. Não prossiga com a utilização do serviço e **c o n t a c t e - n o s** **d e** **i m e d i a t o .**

Exemplo deste tipo de fraude no Caixadirecta on-line:

## 12. Pedido da totalidade dos dígitos do cartão matriz após autenticação no Caixadirecta on-line

Este tipo de fraude consiste em instalar no computador do cliente um código malicioso que faz com que, quando o cliente se autentica no Caixadirecta on-line, se abra uma janela de pop-up onde são solicitados a totalidade dos dígitos do cartão matriz. Em background continua visível a imagem do Caixadirecta on-line.

Exemplo deste tipo de fraude:

**Esteja atento à linguagem utilizada.** É frequente encontrar **erros grosseiros ou expressões pouco comuns** nestes textos, que facilmente excluem a hipótese de se estar perante uma comunicação autêntica da Caixa. Exemplos de frases utilizadas no texto em cima:

- "Salve! O Sistema de Activação da sua Conta Cumprimenta você"
- "Por condição a sua conta está bloqueada."
- "Para activar a conta é necessário que preencha o Cartão matriz, que está mais baixo."
- "Insistentemente pedimos que o Senhor / a Senhora não creia nos rodeios dos fraudadores"
- "Desculpamos pelos incómodos."

Saiba como [proteger o seu computador](#).

## 13. Envio de e-mails fraudulentos

Frequentemente, os clientes da Caixa recebem **e-mails que não são enviados pela CGD**, simulando que o são, com o objectivo de recolher os dados do cartão matriz e os códigos de acesso ao Caixadirecta on-line para posterior utilização fraudulenta. Estes e-mails são dirigidos a clientes de vários Bancos.

**Alertamos todos os clientes** e em especial os utilizadores do Caixadirecta on-line para a necessidade de se manterem particularmente atentos à detecção e prevenção deste tipo de fraude.

Saiba como reconhecer um [e-mail fraudulento](#).

### Medidas de protecção e preservação do cartão matriz

---

Para protecção e preservação do cartão matriz deverá ter o mesmo tipo de cuidados que tem com os seus cartões de débito e crédito e com outras credenciais de segurança (PIN, códigos de acesso, etc.).

Deve ter especial atenção às seguintes medidas de segurança:

- Não guardar informação do cartão em suporte digital;
- Não fazer cópias do cartão ou dos números neles constantes;
- Manter o cartão sempre na posse do titular e não o partilhar com ninguém;
- Preservar a confidencialidade dos números contidos no cartão;
- Não fazer anotações no cartão, em particular informação associável ao contrato Caixadirecta on-line (ex: código de acesso, nº de contrato), à conta ou a qualquer tipo de dado pessoal.

A perda ou o furto do cartão matriz deverá ser **comunicado imediatamente à Caixa** (em qualquer Agência ou através do Caixadirecta telefone) para se proceder ao seu cancelamento, de modo a evitar uma eventual utilização abusiva por terceiros. Poderá de seguida solicitar um novo cartão para a sua morada.

Se detectar qualquer operação estranha, tome nota dos detalhes e reporte-nos imediatamente a situação ligando para o Caixadirecta, disponível 24 horas por dia, através dos números 707 24 24 24, 91 405 24 24, 93 200 24 24 e 96 200 24 24.

**Voltar**