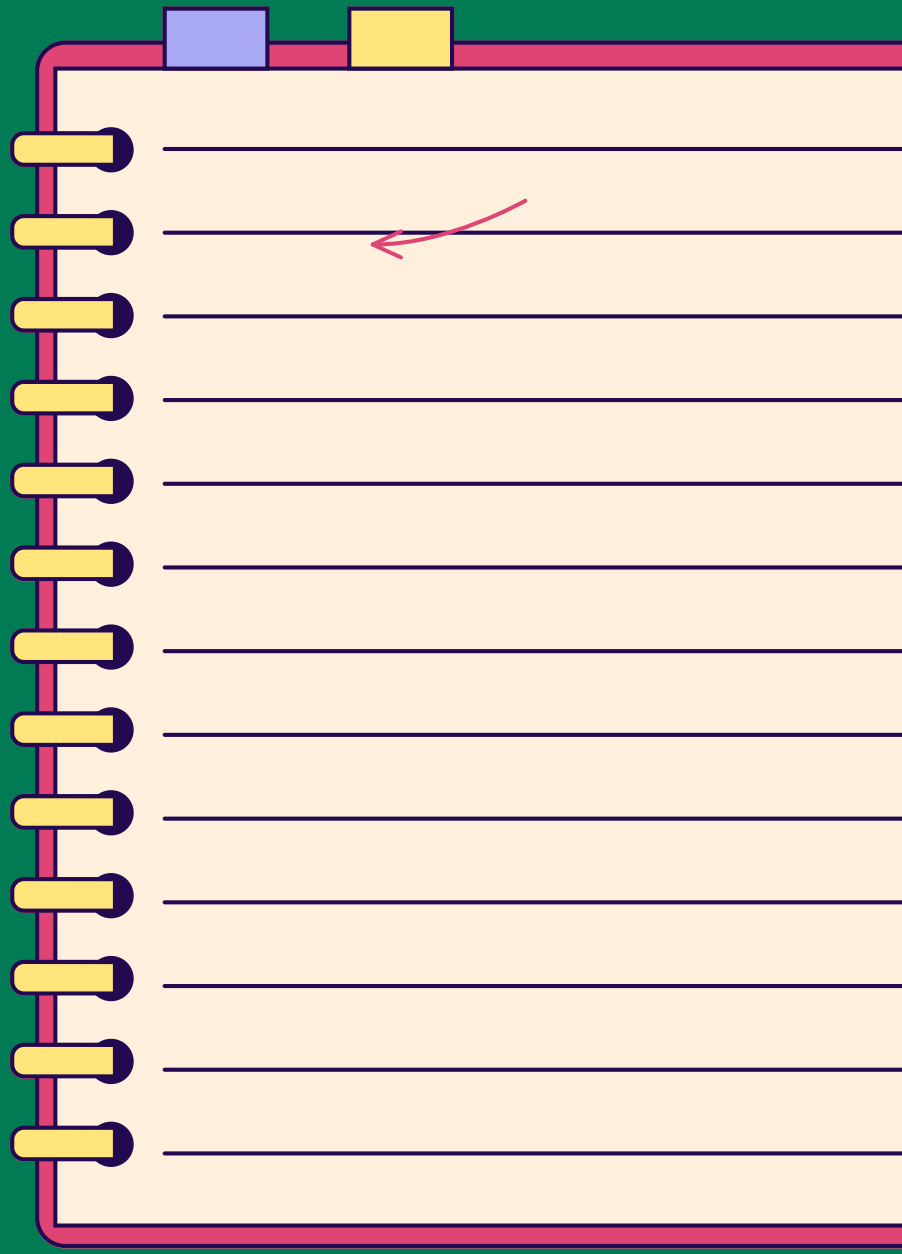
MÓDULO 12 - GOLPES ONLINE

CAPÍTULO 1

QUAIS SÃO AS DIFERENTES BURLAS E COMO DETECTÁ-LAS?

Skills to Connect



INTRODUÇÃO

Na era digital, as burlas online estão a tornar-se cada vez mais sofisticadas e diversificadas. Quer se trate de phishing, spoofing ou fraude nas compras, é essencial saber como funcionam para poder identificá- las e proteger-se de forma mais eficaz.

Neste capítulo, vai aprender sobre as fraudes mais correntes, como identificá-las através de sinais distintivos e como adotar boas práticas para navegar em segurança. No final deste módulo, será capaz de detetar os golpes online e adotar os reflexos certos para se proteger.

1 TIPOS DE BURLAS

PHISHING

O QUE É PHISHING?

Técnica em que um indivíduo mal-intencionado envia mensagens fraudulentas por correio eletrónico ou mensagem, muitas vezes **contendo uma hiperligação**, para incentivar os destinatários a divulgar informações pessoais, **como senhas, números de cartões de crédito ou dados bancários.**

CARACTERÍSTICAS DO PHISHING

- Uma mensagem urgente, que desperta emoções:
  - "A sua conta Google foi pirateada".
  - "Foi efectuada uma transferência de dinheiro fraudulenta".
- Linguagem estranha
  - Erros ortográficos, de sintaxe, etc.
  - Línguas diferentes (mistura de inglês, francês, etc.)
  - Caracteres específicos? Por exemplo: è§°!µ£...
- Logótipo falso, nome de empresa errado, roubo de identidade
- É convidado a clicar num link
- Endereço de correio eletrónico ou número de telefone estranho, não parece oficial

Mais detalhes sobre os sinais a que deve estar atento na página 8!

1 TIPOS DE BURLAS

USURPAÇÃO DE IDENTIDADE

Uma prática em que um indivíduo ou programa finge ser uma pessoa de confiança falsificando os seus dados, como o endereço IP, o endereço e-mail ou o identificador de chamadas, para enganar as vítimas e obter as suas informações pessoais e sensíveis.

POR E-MAIL

O spoofing (falsificação de correio eletrónico) é uma técnica utilizada nas mensagens de spam e phishing para enganar os indivíduos alvos, levando-os a acreditar que uma mensagem provém de uma pessoa ou organização conhecida ou de confiança. Os criminosos modificam os cabeçalhos dos e-mails para que o endereço visível do remetente pareça diferente (e, portanto, familiar!) e para dar à mensagem um aspeto autêntico, especialmente porque o endereço de e-mail parece estar correto.

POR SITE

No caso de spoofing através de um website, os autores da fraude fazem-se passar pelo website de um banco, loja ou organização de confiança. Esta operação é frequentemente acompanhada por uma mensagem de correio eletrónico ou de texto falsa. Se clicar na hiperligação da mensagem, será direcionado para um site falso que tem uma aparência idêntica à do site real. Será então solicitado a introduzir os seus dados de contacto e códigos secretos.

POR TELEFONE

No caso do spoofing telefónico, os burlões utilizam um número de telefone existente. Fazem-se passar por funcionários do seu banco, da polícia ou de outra instituição conhecida e tentam obter as suas informações confidenciais e códigos com uma série de desculpas. Em seguida, esvaziam a sua conta bancária ou pedem-lhe que efectue uma transferência. Os golpistas podem também incentivá-lo a telefonar para um número de tarifa majorada sem que o saiba. Depois, fazem-no ficar em linha o máximo de tempo possível até a sua fatura telefónica atingir números astronómicos.

1 TIPOS DE BURLAS

GOLPES NAS COMPRAS

FRAUDE NAS COMPRAS

Uma situação em que os compradores ou vendedores online são induzidos em erro por anúncios de produtos fictícios, sites de comércio eletrónico fraudulentos em que os pagamentos são feitos mas não entregues, resultando em perdas financeiras.

FRAUDE TRIANGULAR

Um cenário em que um criminoso utiliza informações roubadas do cartão de crédito para comprar bens a um vendedor legítimo e depois revende esses bens a uma vítima insuspeita, muitas vezes a um preço com desconto. A vítima recebe o produto, o vendedor legítimo é pago, mas o verdadeiro titular do cartão de crédito é cobrado por uma transação que não autorizou.

2 SINAIS A QUE DEVE ESTAR ATENTO

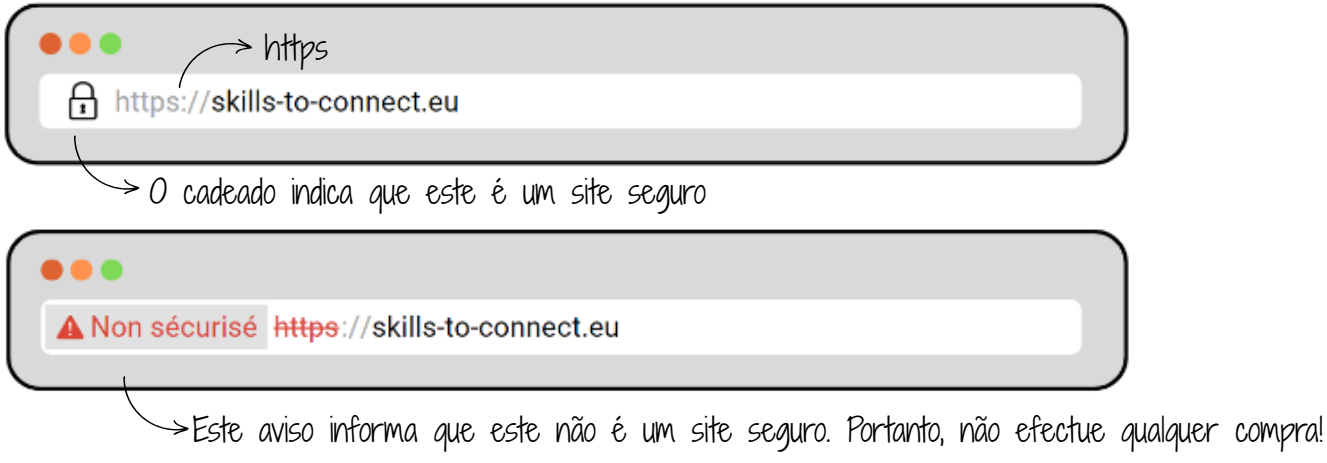
COMO RECONHECER UM SITE FRAUDULENTO

Pode ser difícil saber se um website é verdadeiro ou falso, especialmente se não estiver habituado a verificar esta informação. Eis algumas **dicas simples** para o ajudar a detetar sites fraudulentos:

VERIFIQUE A SEGURANÇA DO SITE, UTILIZANDO UMA SÉRIE DE SINAIS:

Verifique o endereço do site (ou URL), que pode ser encontrado na parte superior do navegador, na barra de endereços. Um website seguro começa sempre por "https://". O "s" significa "seguro". Também deve ver um pequeno cadeado junto ao endereço.

Cuidado com os endereços que parecem verdadeiros mas têm erros ou alterações!



Verifique também o nome do domínio!

Os autores de fraudes copiam frequentemente os endereços de sites conhecidos, alterando apenas um pequeno pormenor.

- Site verdadeiro: https://www.amazon.com
- Site falso: https://www.amaz0n-shop.com (um "0" substitui o "o").

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UM SITE FRAUDULENTO

OBSERVE O DESIGN E O CONTEÚDO DO SITE

- Num site verdadeiro, tudo costuma estar bem apresentado: os textos são claros, sem erros, e as imagens (como os logótipos) são de boa qualidade.
- Num site falso, é frequente encontrar erros ortográficos, logótipos desfocados ou um design que "parece estranho". Às vezes, as hiperligações não funcionam.

PROCURE AS INFORMAÇÕES DE CONTACTO

- Um site sério apresenta os seus dados de contacto: endereço, número de telefone e, por vezes, um formulário de contacto. É frequente encontrar estas informações na parte inferior da página (no "aviso legal").
- Se estas informações não existem ou parecem estranhas (por exemplo, um simples correio eletrónico como contact@gmail.com), tenha cuidado.

CUIDADO COM AS OFERTAS DEMASIADO BOAS PARA SEREM VERDADEIRAS

- Se um produto custar muito menos do que em qualquer outro sítio (por exemplo, um iPhone por 100 euros), é muito provável que se trate de uma fraude.

  → Dica: Compare os preços noutros sites conhecidos para ver se o valor parece realista.

VEJA OS MÉTODOS DE PAGAMENTO DISPONÍVEIS

- Os sites genuínos utilizam métodos de pagamento seguros, como cartões bancários ou PayPal.
- Tenha cuidado se lhe for pedido para pagar por transferência bancária, criptomoeda ou qualquer outro método de pagamento atípico. Depois do dinheiro ser enviado, geralmente nunca será possível recuperá-lo.

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UM SITE FRAUDULENTO

OBSERVE O DESIGN E O CONTEÚDO DO SITE

- Antes de confiar num site, pesquise o nome no Google seguido da palavra “avaliação” ou “fraude”.
- Consulte sites de avaliação fiáveis, como o :
  - Trustpilot: é uma plataforma de avaliação em que os utilizadores partilham as suas experiências com empresas, tanto positivas como negativas.
  - Signal-Arnaques: um site colaborativo dedicado especificamente a denunciar burlas e fraudes, permitindo que outros utilizadores sejam alertados para potenciais fraudes.
  - ScamDoc: uma ferramenta online que analisa automaticamente a fiabilidade de um website ou de um endereço de correio eletrónico com base em informações técnicas e nas avaliações dos utilizadores.

↳ Utilize estas ferramentas para verificar a fiabilidade do site! Se vir muitos comentários a dizer "encomenda nunca recebida" ou "pagamento cobrado mas nada recebido", é provável que se trate de um site falso.

ATENÇÃO AOS ANÚNCIOS E POP-UPS

- Os sites falsos contêm frequentemente anúncios por todo o lado. Se vir janelas que estão sempre a abrir ou mensagens que lhe dizem que ganhou um prémio, feche tudo e saia do site.

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UMA MENSAGEM FRAUDULENTA

As burlas podem assumir a forma de correio eletrónico, mensagens SMS ou até chamadas telefónicas. Os golpistas tentam induzi-lo a fornecer-lhes os seus dados pessoais. Eis como os detetar:

ENDEREÇO DO REMETENTE OU NÚMERO DE TELEFONE É SUSPEITO

Os golpistas utilizam frequentemente endereços ou números fraudulentos. Há alguns sinais a que deve estar atento para ter a certeza de que a pessoa a quem está a telefonar não é um impostor:

- **IDENTIFICAR UM ENDEREÇO E-MAIL FRAUDULENTO:**

  Os autores de fraudes utilizam frequentemente endereços de correio eletrónico que se assemelham aos das empresas oficiais, mas com pequenos erros. Por exemplo, em vez de apoio@banco.com, um golpista pode utilizar banco-apoio@mail.com. Isto pode ser difícil de ver à primeira vista, mas se olhar com atenção, pode detetar a diferença.

  Se o endereço de correio eletrónico parecer estranho ou contiver erros, é provável que se trate de uma burla. Verifique sempre o endereço no site oficial da empresa antes de responder.

- **DETECTAR UMA CHAMADA FRAUDULENTA:**

  As chamadas fraudulentas podem ser efectuadas a partir de números desconhecidos ou ser anónimas (em que não aparece nenhum número no seu telefone). Os autores de fraudes também podem utilizar números que se parecem com números de empresas, mas que têm uma ligeira diferença. Por exemplo, uma chamada pode parecer ser do seu banco, mas o número apresentado não é o que está habituado a ver.

  Se a chamada for feita de um número anónimo ou desconhecido, ou se o número não corresponder ao da empresa, é preferível não atender. Contacte diretamente a empresa utilizando as informações oficiais para verificar se a chamada é legítima.

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UMA MENSAGEM FRAUDULENTA

DETECTAR UM SMS FRAUDULENTO

- Algumas empresas utilizam números curtos ou números especiais, como 8000, 8080 ou outros, para enviar SMS oficiais, como alertas ou promoções. No entanto, os autores de fraudes também podem utilizar estes números para mascarar a sua verdadeira identidade e enganá-lo.
- Se o SMS for proveniente de um número curto desconhecido ou de um número estranho (por exemplo, um número que comece por +44 ou +1), ou se o conteúdo parecer demasiado urgente ou demasiado bom para ser verdade, é provável que se trate de uma burla. Por exemplo, um SMS que diz ser do seu banco, mas que lhe pede para clicar numa hiperligação ou fornecer informações confidenciais, é suspeito.

Se não reconhecer o número ou se a mensagem parecer suspeita, não responda nem clique nas hiperligações. Contacte diretamente a empresa através do seu número oficial para verificar.

A MENSAGEM É ESTRANHA

As mensagens fraudulentas, quer sejam recebidas por correio eletrónico, por SMS ou mesmo por chamada telefónica, contêm frequentemente erros gramaticais, erros de sintaxe ou uma formulação estranha. Estes erros são um sinal de que se trata provavelmente de uma tentativa de burla.

MENSAGENS FINGINDO SER EMPRESAS:

Uma mensagem que comece com “Caro Utilizador” em vez de utilizar o seu nome próprio ou um “Olá Senhor/Senhora” é suspeita. As empresas legítimas, como os bancos ou os sites de comércio eletrónico, geralmente personalizam as suas mensagens incluindo o seu nome no título ou no corpo do texto. Se não vir o seu nome ou se a mensagem for demasiado genérica, é um sinal de alerta.

- ✕ **FRAUDULENTO: CARO UTULIZADOR, A SUA CONTA SERÁ SUSPENSA.**
- ✓ **LEGÍTIMO: OLÁ ____, TEMOS UMA ATUALIZAÇÃO RELATIVA À SUA CONTA.**

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UMA MENSAGEM FRAUDULENTA

MENSAGENS QUE FINGEM SER SERVIÇOS PÚBLICOS OU GOVERNAMENTAIS:

Se receber um SMS ou um e-mail que pareça vir de um serviço público (por exemplo, alertas fiscais ou da segurança social), mas com erros ortográficos, é um grande sinal de alerta. As mensagens oficiais do governo são geralmente escritas de forma clara e profissional. Os golpistas tentam por vezes fazer-se passar por instituições públicas, mas nem sempre têm cuidado com a qualidade da sua escrita.

- **FRAUDULENTO: O SERVIÇO DE FINANÇAS DEVE-LHE DINHEIRO, CLIQUE AQUI PARA O PEDIR DE VOLTA**
- **LEGÍTIMO: O SERVIÇO DE FINANÇAS INFORMA-O DE QUE TEM DIREITO A UM REEMBOLSO. PARA MAIS INFORMAÇÕES, ACEDA AO SEU ESPAÇO PESSOAL**

MENSAGENS QUE FINGEM SER UM AMIGO OU UMA PESSOA DE CONTACTO

Por vezes, as burlas podem parecer vir de amigos ou contactos que conhece, especialmente se a conta deles tiver sido pirateada. Se uma mensagem do seu amigo parecer estranha, tiver erros ou o tom for inabitual (por exemplo, “Encontrei um plano fantástico para ti!”), pode ser uma tentativa de phishing.

- **FRAUDULENTO: EI, VÊ ESTE VÍDEO FANTÁSTICO, ACHO QUE VAIS GOSTAR!**
- **LEGÍTIMO: OLÁ___, ENVIO-TE O VÍDEO DE QUE TE FALEI, VÊ-O QUANDO TIVERES UM MOMENTO 😊**

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UMA MENSAGEM FRAUDULENTA

A MENSAGEM É URGENTE

Os golpistas tentam muitas vezes fazer com que reaja rapidamente, colocando-o sob pressão, com mensagens urgentes ou ameaçadoras.

MENSAGENS URGENTES

Uma mensagem pode indicar-lhe que a sua conta vai ser bloqueada ou que tem de agir imediatamente para evitar um problema:

- **A SUA CONTA SERÁ SUSPENSA DENTRO DE 24 HORAS!**
- **RESPONDA AGORA PARA EVITAR QUE A SUA CONTA SEJA ENCERRADA**

OFERTAS MUITO URGENTES

Por vezes, os golpistas dizem-lhe que ganhou um prémio, mas que tem de reagir imediatamente para o receber:

- **GANHOU 1.000 EUROS - CLIQUE AQUI ANTES DE HOJE À NOITE PARA OS RECEBER!**

OFERTAS MUITO URGENTES

Podem também tentar assustá-lo com ameaças de multas ou acções judiciais se não responder rapidamente.

- **DEVE PAGAR ESTA MULTA NO PRAZO DE 48 HORAS OU SERÁ OBJETO DE UMA AÇÃO JUDICIAL!**

A MENSAGEM PEDE OS SEUS DADOS PESSOAIS

- Se uma mensagem lhe pedir informações sensíveis, como a sua senha, números de cartões bancários ou código PIN, é um sinal claro de fraude.
- **Nenhuma empresa séria lhe pedirá estas informações por correio eletrónico, SMS ou telefone!**

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UMA MENSAGEM FRAUDULENTA

A MENSAGEM PEDE OS SEUS DADOS PESSOAIS

- Se uma mensagem lhe pedir informações sensíveis, como a sua senha, números de cartões bancários ou código PIN, é um sinal claro de fraude.
- **Nenhuma empresa séria lhe pedirá estas informações por correio eletrónico, SMS ou telefone!**

CONVÉM SABER

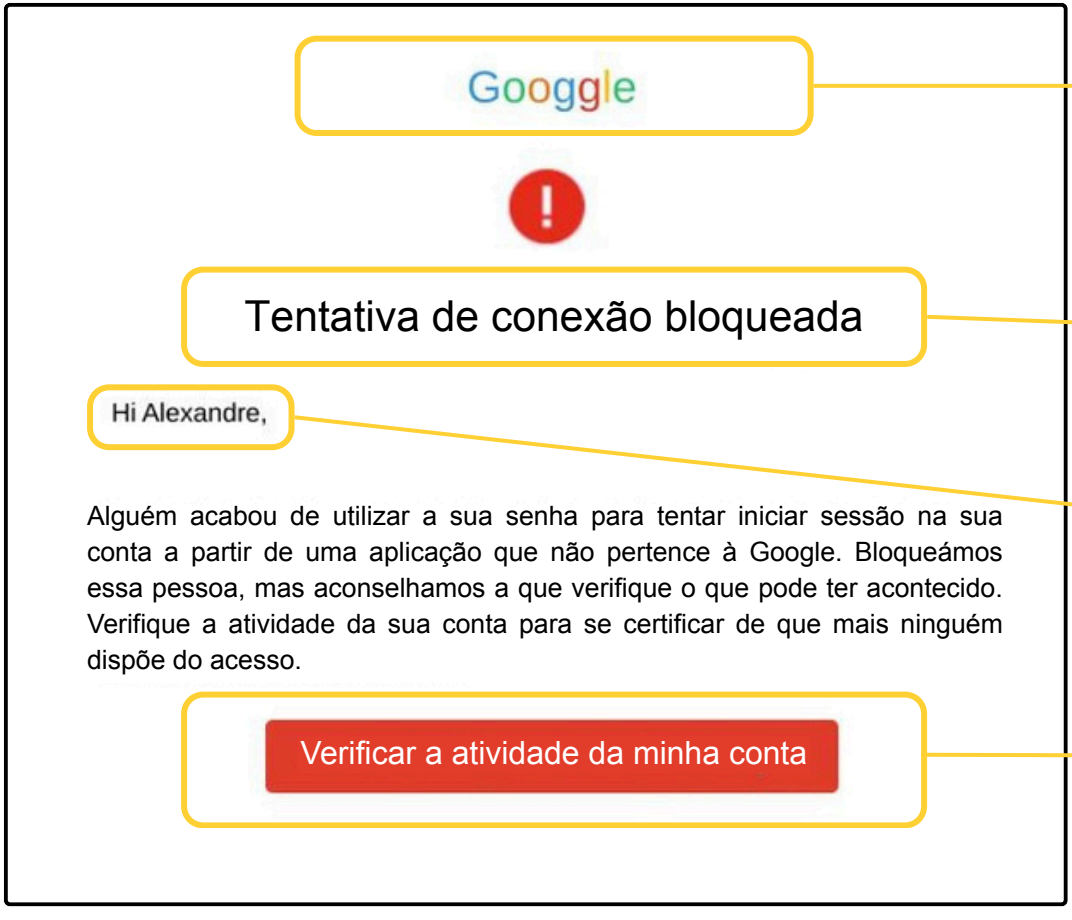
- Um funcionário de um banco nunca lhe pedirá os seus dados pessoais sensíveis, como a sua senha, por telefone. Os bancos não precisam da sua senha para aceder às suas informações ou para o ajudar com um problema. Se receber uma chamada de um consultor que lhe pede a sua senha ou outras informações confidenciais (como o seu código PIN ou o número do seu cartão bancário), trata-se provavelmente de uma tentativa de o aldrabar. Não responda e contacte diretamente o seu banco através dos dados de contacto oficiais.

- Para aceder aos serviços públicos online **na Bélgica**, é preciso conectar-se através da plataforma CSAM (plataforma de serviços da administração pública belga) ou ITSME, uma aplicação de segurança. Por exemplo, nunca receberá qualquer comunicação oficial sobre os seus impostos por correio eletrónico. Só pode consultar as suas informações fiscais na plataforma MinFin. Se receber um e-mail que lhe peça para clicar numa hiperligação para aceder à sua declaração de impostos, trata-se de uma tentativa de phishing. Este tipo de fraude pode também afetar outros serviços públicos, como o Ma Pension ou outros serviços públicos. Esteja atento e nunca clique numa hiperligação suspeita de um e-mail.

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UMA BURLA

EXEMPLOS DE PHISHING



Logotipo falso

o verdadeiro logótipo da google é o seguinte

Google

Mensagem de emergência

Usa as emoções, o stress e um sentido de urgência para o levar a agir sem pensar

Atípico

Mistura de inglês e português

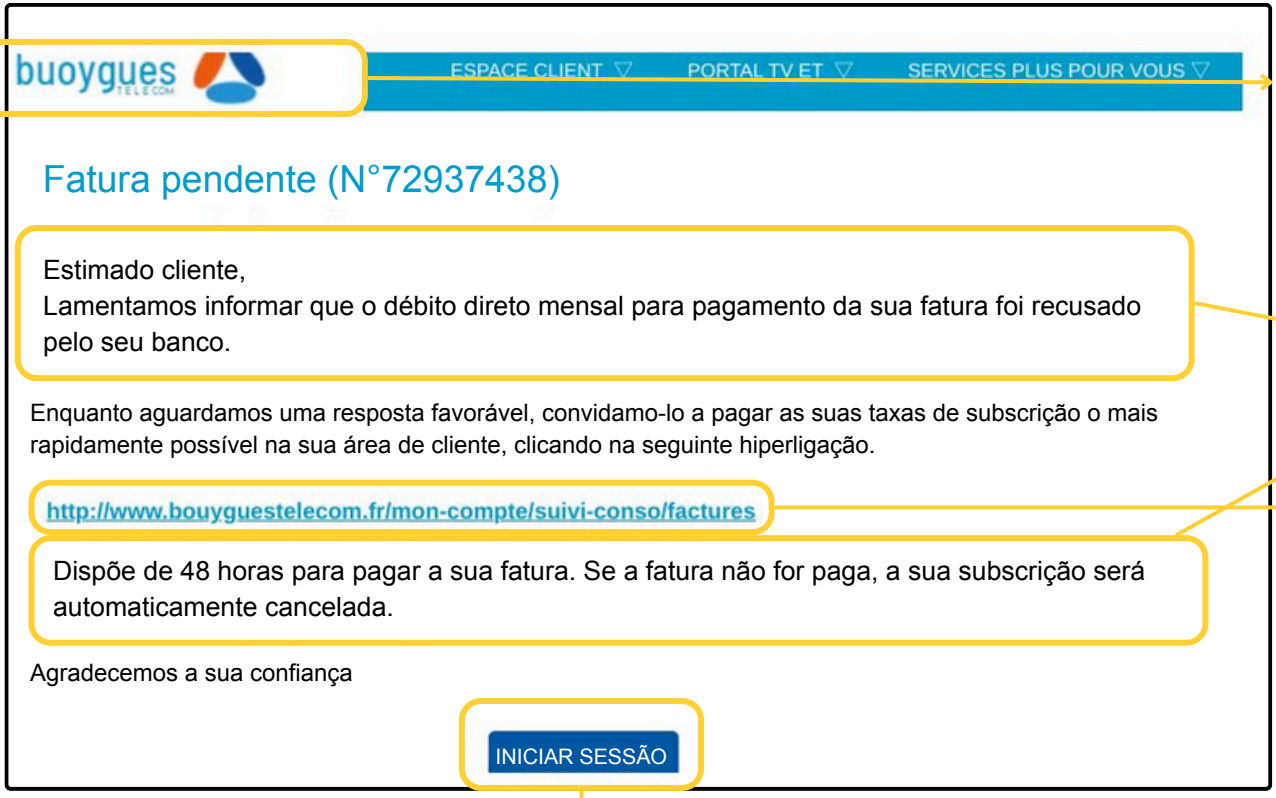
Impulso à ação

Uma hiperligação fraudulenta encontra-se por detrás deste botão

2 SINAIS A QUE DEVE ESTAR ATENTO

COMO RECONHECER UMA BURLA

EXEMPLOS DE PHISHING



Nome escrito incorretamente

É Bouygues, não Buoygues

Mensagem de emergência

Usa as emoções, o stress e um sentido de urgência para o levar a agir sem pensar

Link fraudulento

O link não é seguro: começa com "http" e não "https"!

Impulso à ação

Uma hiperligação fraudulenta encontra-se por detrás deste botão

PARA LEMBRAR!

As burlas online assumem muitas formas, incluindo phishing, spoofing e fraude em compras. É essencial manter-se vigilante face a estas tentativas de fraude. Um sinal revelador de uma burla pode ser uma mensagem a pedir informações pessoais ou uma mensagem que pareça demasiado urgente ou demasiado boa para ser verdade. Verifique sempre o endereço de correio eletrónico, o número de telefone e as hiperligações contidas nas mensagens. Erros gramaticais ou um tom ameaçador são frequentemente indicadores de fraude. Por último, se tiver dúvidas, não hesite em contactar diretamente a empresa ou organização através de um canal oficial para verificar a legitimidade da mensagem. **Proteger-se contra estas fraudes começa por saber reconhecê-las!**