PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA

TODOS CONTAM

FINANÇAS DIGITAIS
PROTEGER DADOS PESSOAIS

01 VANTAGENS DOS CANAIS DIGITAIS

02 REDUZIR O RISCO DE FRAUDE

03 PRÁTICAS FRAUDULENTAS

VANTAGENS DOS CANAIS DIGITAIS

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA
TODOS CONTAM

Os canais digitais permitem que os consumidores utilizem produtos e serviços bancários através do computador, do *smartphone* ou do *tablet*

CONVENIÊNCIA
Em qualquer altura e lugar
De forma rápida

NOVOS PRODUTOS
Com acesso a produtos personalizados e novos serviços

CUSTOS
Os custos poderão ser menores do que os canais tradicionais

REDUZIR O RISCO DE FRAUDE

Práticas para reduzir o risco de fraude:

- Garantir a inserção de palavras-passe e outros elementos de autenticação, em contexto reservado
  - Evitar a inserção de *passwords* e outras credenciais de acesso, em locais com grandes aglomerações de pessoas (como transportes públicos ou centros comerciais, por exemplo), evitando o *shoulder surfing*

Shoulder surfing: consiste em observar a inserção de dados em determinado equipamento (como *passwords* e outras credenciais de acesso), sem que o respetivo utilizador se aperceba, com o objetivo de os utilizar ilegitimamente, em momento posterior

REDUZIR O RISCO DE FRAUDE

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA
TODOS CONTAM

Práticas para reduzir o risco de fraude:

- Evitar partilhar dados pessoais que não são essenciais para o serviço prestado
  - Existem *apps* que pedem autorização para aceder à localização geográfica, contactos, microfone, câmara e fotografias do utilizador. É importante ponderar se as autorizações solicitadas são necessárias e proporcionais para o serviço prestado através dessa *app*

- Verificar as configurações de privacidade e de segurança
  - Antes da utilização de uma nova *app* ou de uma nova conta de utilizador na internet, é importante definir as respetivas configurações de privacidade e de segurança, designadamente quanto ao "como" e "com quem" são partilhadas as informações recolhidas

PRÁTICAS FRAUDULENTAS

Phishing – Prática que consiste no envio de um *e-mail*, que tenta convencer a vítima a clicar num endereço de uma página falsa, que imita uma página verdadeira (de um banco, por exemplo), com o objetivo de recolher os seus dados pessoais, como a palavra-passe de acesso à página verdadeira.

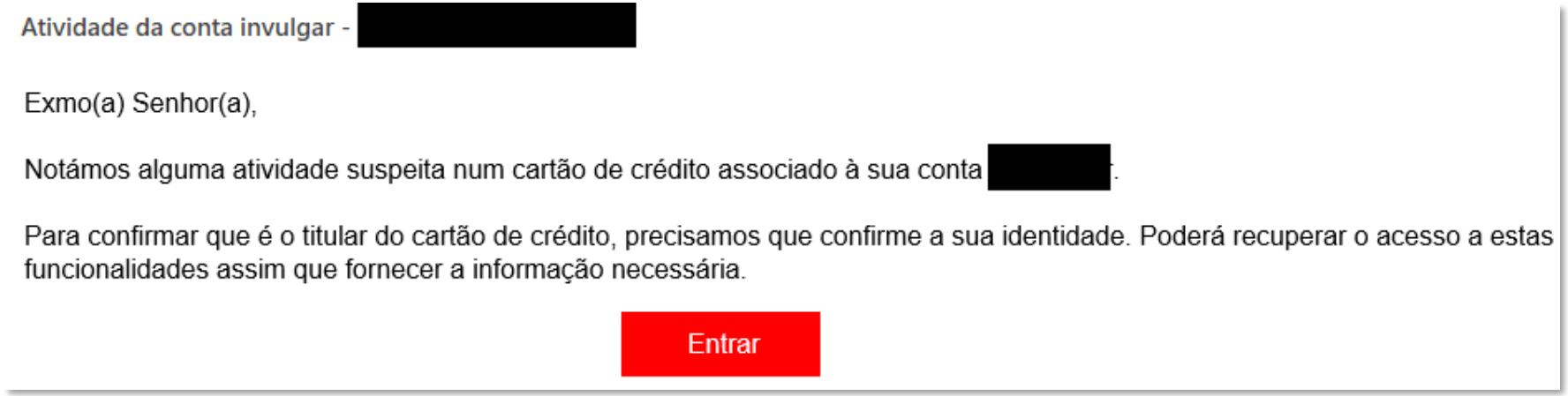
- O burlão pode também tentar obter os dados pessoais da vítima através de uma chamada telefónica (***vishing***) ou do envio de um SMS (***smishing***)

- Por vezes, os piratas informáticos usam o ***spoofing***, um esquema em que copiam os números de telefone ou os endereços de *e-mail* de entidades oficiais, bem como a sua aparência, para tornarem as mensagens fraudulentas mais convincentes

PRÁTICAS FRAUDULENTAS

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA
TODOS CONTAM

Há pessoas que tentam passar-se por outras ou por instituições para obter os dados das suas vítimas, através do recurso à **manipulação psicológica** e à **criação de uma sensação de urgência**


Atividade da conta invulgar - [redacted]

Exmo(a) Senhor(a),

Notámos alguma atividade suspeita num cartão de crédito associado à sua conta [redacted].

Para confirmar que é o titular do cartão de crédito, precisamos que confirme a sua identidade. Poderá recuperar o acesso a estas funcionalidades assim que fornecer a informação necessária.

Entrar

Nestes contactos, aparentemente legítimos, o pirata informático tenta convencer a vítima de que existe um erro ou um problema, e para o corrigir, deve disponibilizar com urgência os seus dados pessoais (diretamente ou através de um link para uma página falsa, muito semelhante à verdadeira)

PRÁTICAS FRAUDULENTAS

Utilização de **técnicas de persuasão** e a **criação de narrativas credíveis** para ter acesso a credenciais de *homebanking* ou dados de cartões de crédito

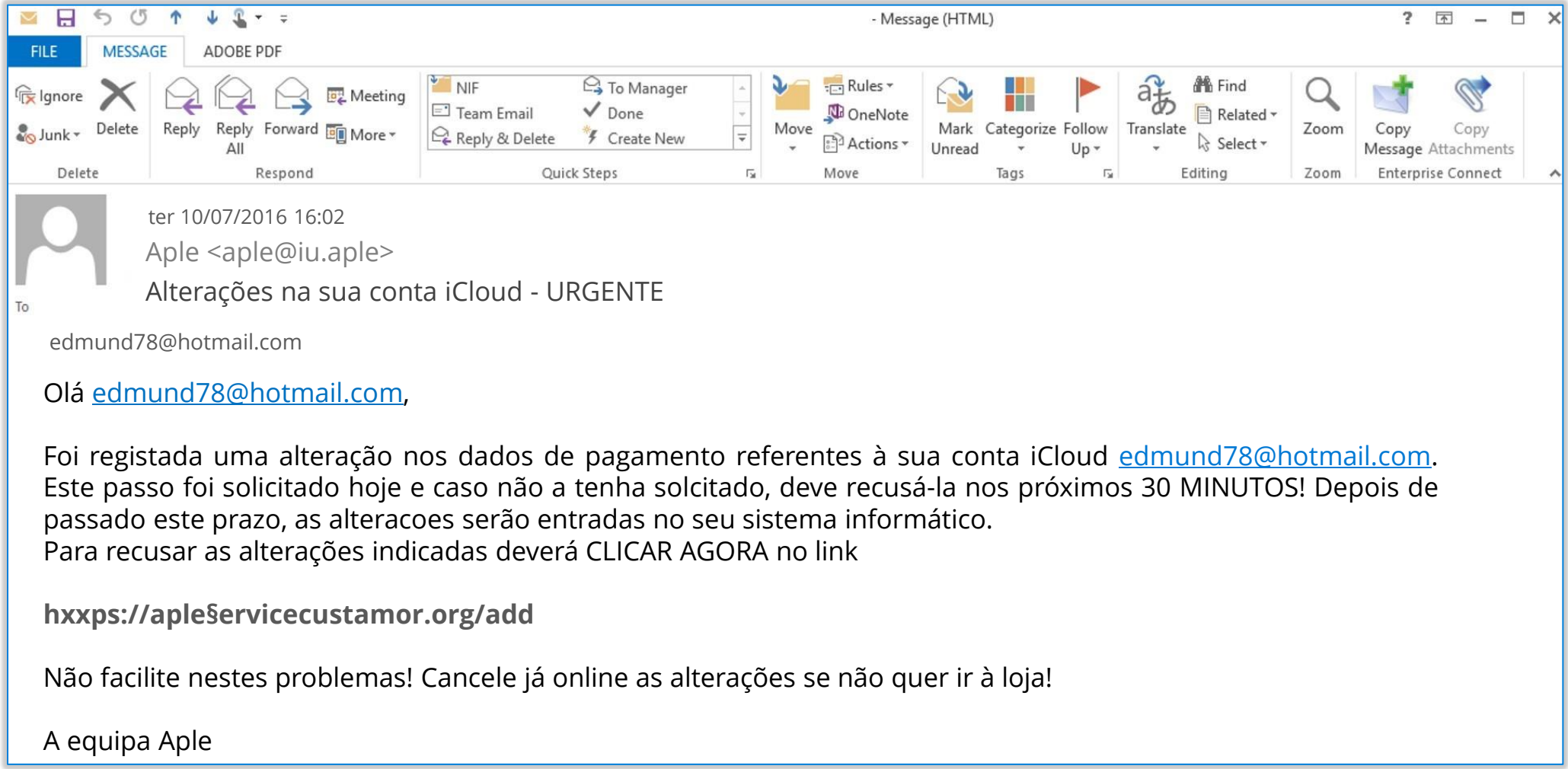
PRÁTICAS FRAUDULENTAS

Como são criadas as narrativas credíveis?

- Entidade credível para conferir autoridade ao contacto
- Cenário credível
- Meios de comunicação credíveis
- Personalização, conhecimento da vítima e do seu contexto
- Apelo à emoção e a uma ideia de urgência que motive uma ação imediata
- Intimidação e consequências negativas, caso a vítima não aja em conformidade

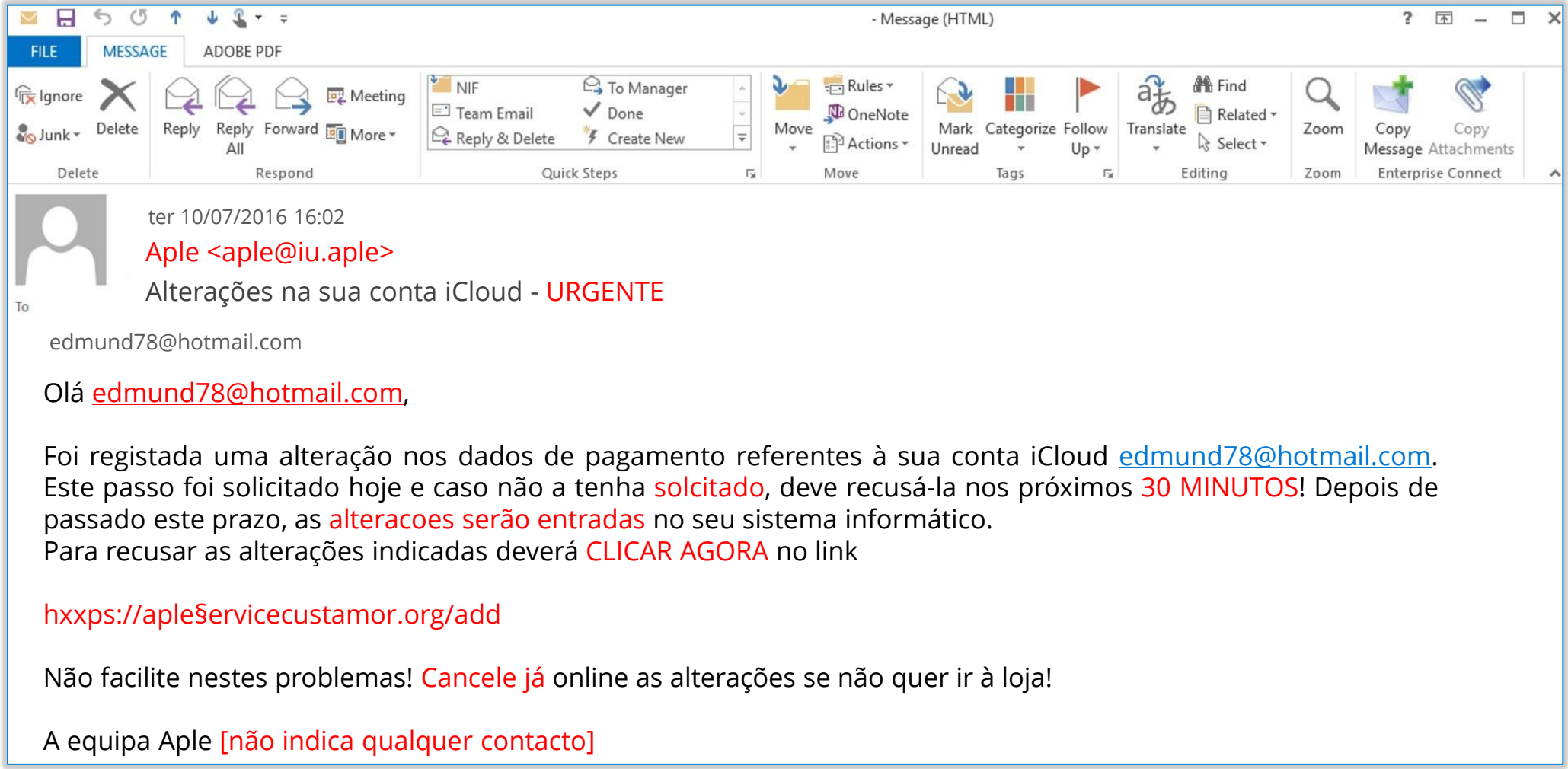
PRÁTICAS FRAUDULENTAS

Um *e-mail* que suscite dúvidas quanto à sua legitimidade, **deve ser imediatamente apagado**



PRÁTICAS FRAUDULENTAS

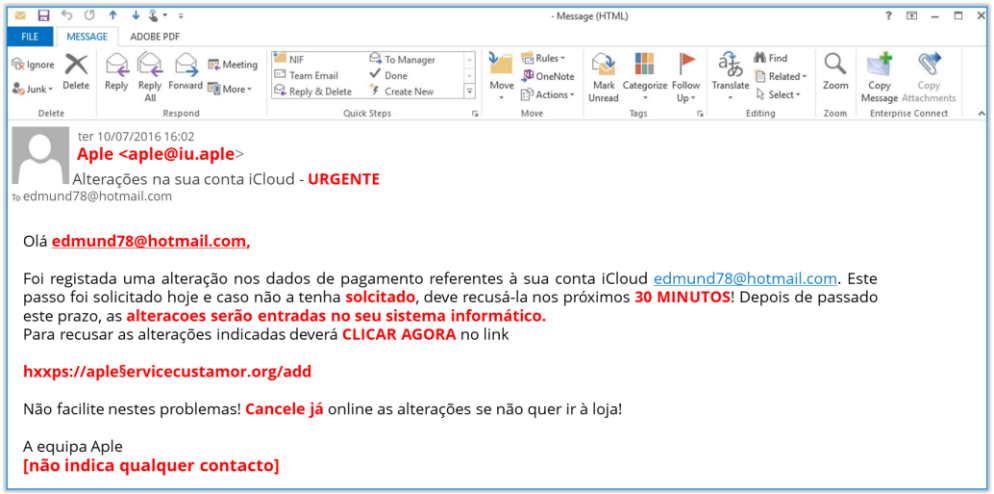
Um *e-mail* que suscite dúvidas quanto à sua legitimidade, **deve ser imediatamente apagado**



PRÁTICAS FRAUDULENTAS

Há várias formas de **verificar a legitimidade do *e-mail*** e detetar indícios de fraude:

- Verificar sempre o endereço do remetente (não só o nome)
- Verificar a linguagem utilizada (eventualmente menos formal,
  com erros ortográficos e de semântica)
- Analisar o tom com que a comunicação está escrita (poderá procurar transmitir ao leitor uma sensação de urgência, dando prazos muito curtos para fazer aquilo que é indicado)



Para **evitar situações de fraude**:

- Não clicar em *links* apresentados no *e-mail* suspeito
- Não executar as ações pedidas, nem programas sugeridos
- Não abrir anexos de fontes desconhecidas
- Não inscrever dados confidenciais e informações pessoais em *sites* cuja autenticidade não esteja assegurada

PRÁTICAS FRAUDULENTAS

Em caso de suspeita de fraude, há procedimentos que devem ser adotados

Contactar imediatamente o **banco**

Participar a ocorrência a um **órgão de polícia** (Polícia Judiciária, PSP, GNR) ou ao Ministério Público