

# A sua experiência cibernética



Um percurso autónomo sobre riscos cibernéticos

## Antes **de** começar:

O objetivo desta experiência é ajudá-lo a **identificar** os seus principais riscos cibernéticos, a **compreender** e a **minimizar** os mesmos

N.º 1

Caracterizar o seu  
**dia de trabalho**

N.º 2

Detetar os seus  
**riscos**

N.º 3

Descobrir  
**histórias da vida  
real**

N.º 4

Aprender **o que  
fazer**



**Estou preparado** →

## Primeiro passo:



Caracterizar **o seu dia de trabalho**

Seguinte →

# Escolha uma personagem com a qual se identifique:

Recebo dezenas  
de **e-mails** por dia



Trabalho  
principalmente  
com **clientes**

Gosto de trabalhar  
em **locais públicos**



Trato de transações  
**monetárias**

**Recebe dezenas de e-mails todos os dias?**



Detetar os seus **riscos**

**Seguinte** →

## Os **riscos**

A sua utilização intensiva do e-mail torna-o especialmente vulnerável a estas formas de fraude:



Phishing



Business-Email-Compromise (BEC)

O que **significa?** →

# Descobrir **histórias da vida real**

As pessoas são vítimas destas fraudes todos os dias.  
Apresentamos-lhe algumas das suas histórias para o ajudar  
a compreender estes riscos



**Seguinte** →

“Aconteceu num daqueles dias em que nem tempo temos para café. **Recebi um e-mail** dos “Recursos Humanos”. Esse e-mail continha um link para um formulário que pedia os meus dados, incluindo o meu e-mail de trabalho e palavra-passe.

Durante o almoço, **descobri que o preenchimento do referido formulário não foi pedido a mais nenhum dos meus colegas.** Fui vítima de phishing?”



**Seguinte** →





## Phishing

"**Recebi um e-mail** de um cliente a pedir-me para o ajudar a aceder aos seus dados. Mencionou que estava prestes a assinar um contrato e que precisava das suas demonstrações financeiras rapidamente, **pelo que partilhei a informação confidencial com ele.**

Mais tarde, quando voltei a olhar para o e-mail, reparei **que o endereço de e-mail estava mal escrito. Até o nome tinha uma gralha.**"

**Seguinte** →

## Business- Email- Compromise (BEC)

"**Recebi um e-mail** do 'Daniel Silva', o meu chefe. No e-mail, pedia-me para **transferir fundos para um fornecedor imediatamente**, uma vez que estávamos em violação de um contrato. Depois de dar rapidamente seguimento ao seu pedido, senti-me como o melhor funcionário.

**Só mais tarde**, quando voltei a olhar para o e-mail, é que percebi **que havia algo de muito errado com ele.**"



**Passo seguinte** →

E agora, para o passo final:

**Aprender o que fazer** 

## 4 dicas sobre como reduzir os seus riscos

- N.º 1 **Analise** o endereço de e-mail do remetente e verifique se é o que espera
- N.º 2 **Contacte a pessoa que solicitou o pedido** através de um tópico ou canal separado (sempre que tiver suspeitas)
- N.º 3 **Passe o cursor sobre os links** para verificar se os URLs remetem para um site conhecido (nos telemóveis, prima e mantenha a pressão sobre o link e será revelado o endereço do site)
- N.º 4 **Esteja atento aos e-mails que o incitam a agir rapidamente.** Estes e-mails devem ser considerados como sinais de alerta.

**Concluído** →

# Trabalha com **clientes**?



Detetar os seus **riscos**

Seguinte →

## Os **riscos**

Trabalhar com muitas pessoas (como funções de serviço de apoio ao cliente) torna-o especialmente vulnerável a estes riscos:



Falsificação de  
identidade



Partilha de informações  
confidenciais

O que **significa?** →

# Descobrir **histórias da vida real**

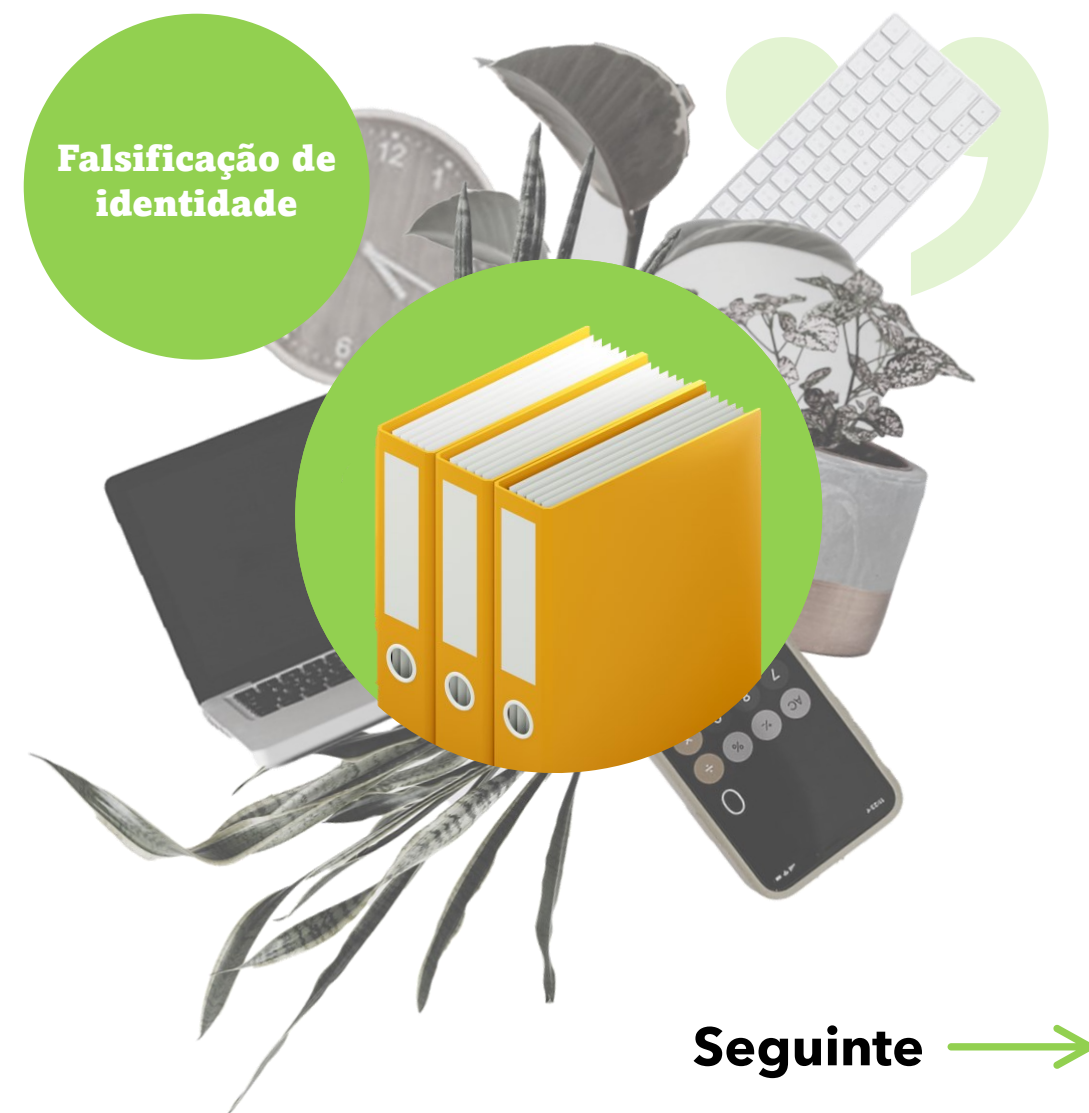
As pessoas são vítimas destas fraudes todos os dias.  
Apresentamos-lhe algumas das suas histórias para o ajudar  
a compreender estes riscos



**Seguinte** →

“**Recebi um e-mail** do ‘Bernardo’, que trabalha no departamento de contabilidade dos clientes, onde me pedia alguns documentos para o projeto em que estava a trabalhar. **Por isso, enviei-os por e-mail.**”

Foi só mais tarde, quando a minha empresa foi processada, que **descobri que não trabalhava nenhum Bernardo no departamento de contabilidade dos clientes.**”







Partilha de  
informações  
confidenciais

**"O meu chefe pediu-me para partilhar a folha de cálculo das receitas anuais** com o Miguel das finanças, **e assim o fiz..** Uma semana mais tarde, o caso estava nas notícias.

**Sucede que enviei o documento acidentalmente para um Miguel de outra empresa do setor."**

**Seguinte** →

“**Recebi um telefonema de uma mulher** a chorar. Pediu-me o registo de chamadas do seu filho de treze anos, pois estava desaparecido. **Senti que tinha o dever de a ajudar** sem a massacrar com demasiadas perguntas.

Só descobri que **tinha enviado as informações a um detetive privado** que estava a investigar um caso de traição no matrimónio depois de termos sido processados.”



**Passo seguinte** →

E agora, para o passo final:

**Aprender o que fazer** 

## 4 dicas sobre como reduzir os seus riscos

- N.º 1 **Verifique sempre** a identidade da pessoa com quem está a conversar
- N.º 2 Antes de partilhar informações relacionadas com os clientes, **verifique cuidadosamente** se as informações podem ser explicitamente partilhadas
- N.º 3 Partilhe informações sensíveis **unicamente através dos canais autorizados.**
- N.º 4 Preste atenção ao **tom do requerente**. Se alguém tentar pressioná-lo, é geralmente um sinal de fraude

**Concluído** →

# Trabalha em locais públicos?



Detetar os seus **riscos**

Seguinte →

## Os **riscos**

Trabalhar em locais públicos torna-o especialmente vulnerável a estes riscos:



Roubo de portátil



Pirataria visual



Ataque Wi-Fi

O que **significa?** →

# Descobrir **histórias da vida real**

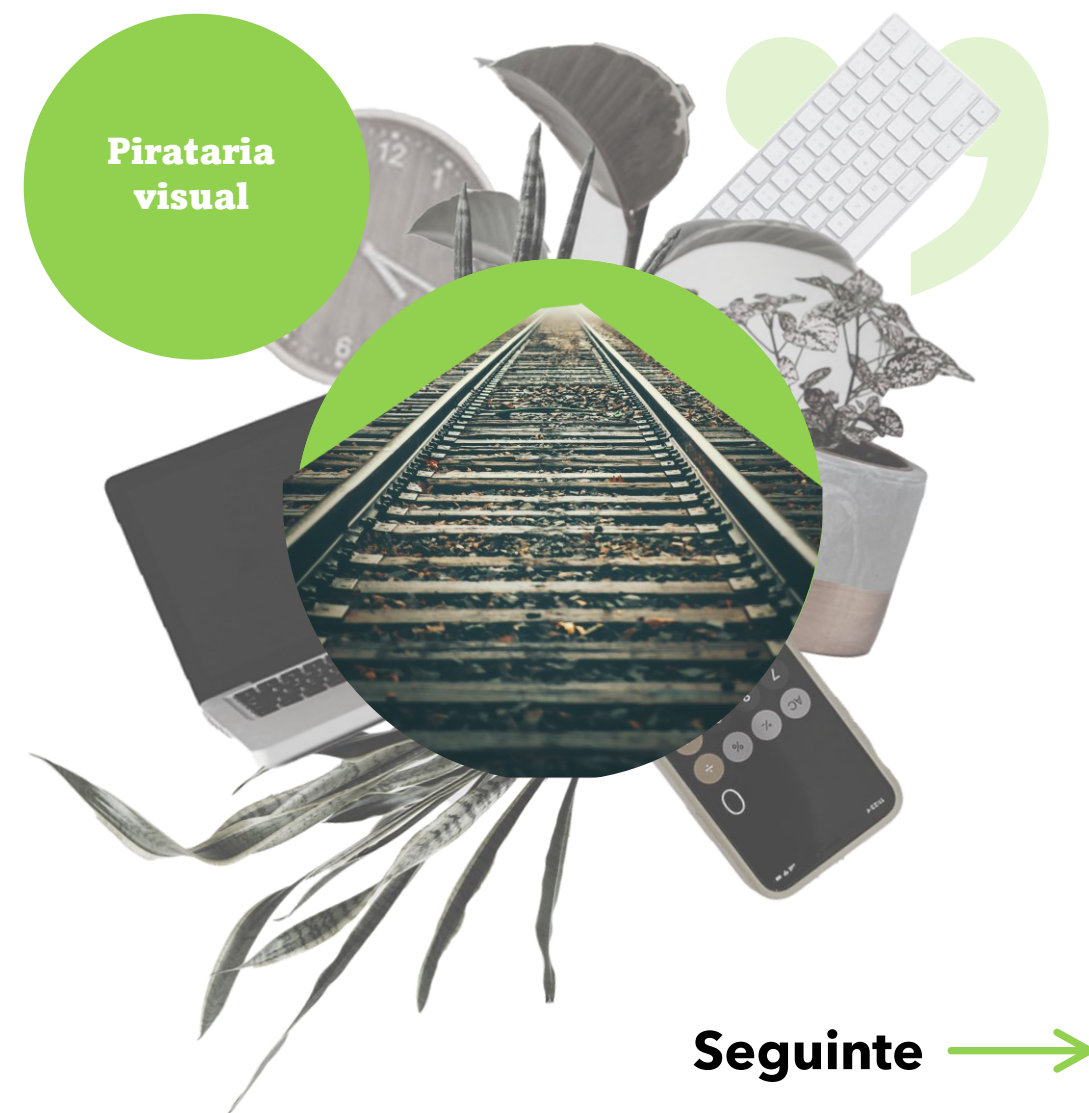
As pessoas são vítimas destas fraudes todos os dias.  
Apresentamos-lhe algumas das suas histórias para o ajudar  
a compreender estes riscos



**Seguinte** →

“Estava a viajar num **comboio** bastante cheio. Uma vez que tinha um relatório importante para terminar, **trabalhei no meu portátil durante a viagem**. No dia seguinte, deparei-me com uma publicação da Reddit que continha **informações privilegiadas sobre a nossa empresa e que constavam do meu documento**.

Será possível que eu tenha sido a origem da **fuga**?”







## Roubo de portátil

“Um dia, enquanto **trabalhava num café** que frequento muitas vezes, **levantei-me** para ir pedir um pastel **e deixei o meu portátil sem vigilância apenas por uns instantes.**”

Quando voltei, **o portátil já não estava lá.**”

**Seguinte** →

"A caminho de um cliente, tive de verificar alguns detalhes. **Por isso, liguei-me ao Wi-Fi gratuito de um café nas proximidades,** verifiquei o que era necessário e desativei o Wi-Fi.

No mês seguinte, **houve um ataque ao nosso sistema** utilizando o meu utilizador. Não consigo deixar de pensar que isto pode ter sido causado pela minha utilização de uma rede Wi-Fi maliciosa."



**Passo seguinte** →

E agora, para o passo final:

**Aprender o que fazer** 

## 3 dicas sobre como reduzir os seus riscos

- N.º 1 **Mantenha o seu portátil** sempre **perto de si**. Ficaria admirado com o número de portáteis roubados todos os anos.
- N.º 2 **Utilize apenas ligações à Internet privadas**, nunca uma ligação pública
- N.º 3 Certifique-se de que é o **único a conseguir ver o ecrã** do seu portátil e notas

**Concluído** →

# Trata de **transações monetárias**?



Detetar os seus **riscos**

Seguinte →

## Os **riscos**

Ter autorização para transferir fundos torna-o vulnerável a estas formas de fraude:



Business-Email-Compromise (BEC)



Falsificação de identidade de fornecedores

O que **significa?** →

# Descobrir **histórias da vida real**

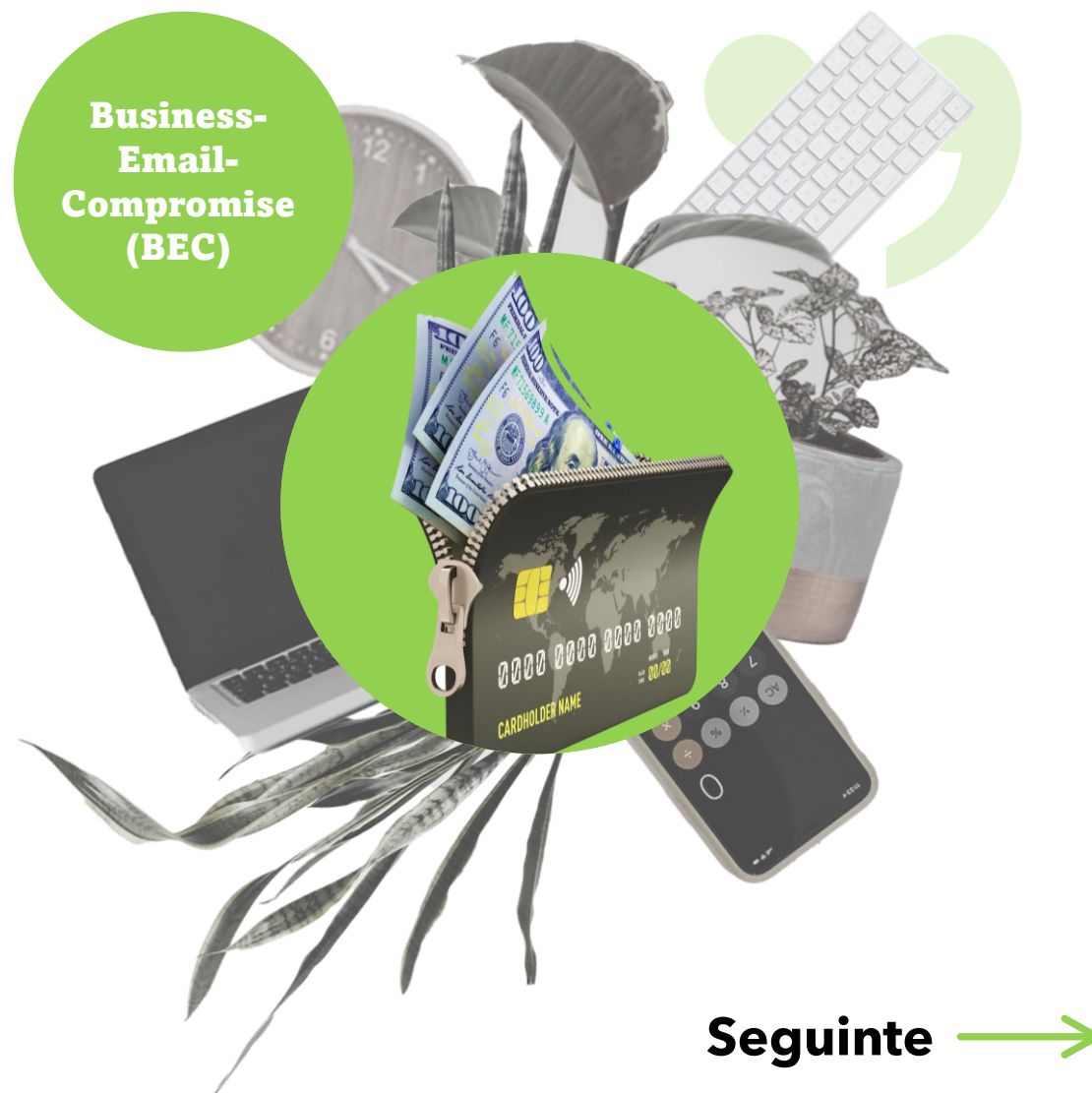
As pessoas são vítimas destas fraudes todos os dias.  
Apresentamos-lhe algumas das suas histórias para o ajudar  
a compreender estes riscos




**Seguinte** →

“**Recebi um e-mail** do meu chefe a indicar-me para **transferir 17.000 dólares para um novo fornecedor**. Ele escreveu: ‘Estou numa reunião. Não posso falar. **Transfira o dinheiro o mais rápido possível**’, e foi isso que fiz.

Apenas um dia depois, no escritório, é que percebi **que ele não fazia ideia do que eu estava a falar.**”







**Falsificação de  
identidade de  
fornecedores**

**“Recebi um e-mail de um gestor financeiro recentemente nomeado** de um dos nossos fornecedores, onde me pedia que os **futuros pagamentos** fossem enviados para uma conta bancária diferente. **Por isso, fiz conforme me pediu.**”

Tratou-se de uma **fraude**, mas como poderia eu sabê-lo?”

**Seguinte** →

“**Recebi um e-mail** dos RH com um tópico extenso. Pediram-me que **comprasse cartões-presente** para a festa de Ano Novo. Só precisavam dos seus números. Por isso, **comprei os cartões e enviei-lhes os números..**”

Como se veio a saber, foi uma fraude, e todo o **dinheiro tinha desaparecido.**”



**Passo seguinte** →

E agora, para o passo final:

**Aprender o que fazer** 

## 3 dicas sobre como reduzir os seus riscos

- N.º 1 Verifique o endereço de e-mail do remetente. Se for diferente do endereço habitual, feche o e-mail e contacte o presumível remetente através de outro canal
- N.º 2 **Confirme qualquer pedido de alteração** do método de pagamento com a sua pessoa de contacto habitual, presencialmente ou por telefone
- N.º 3 Aja com calma. Os hackers tentam levar as pessoas a agir rapidamente para não detetarem sinais de alarme ou para não consultarem outras pessoas

**Concluído** →

# Excelente! Concluiu o percurso



O que gostaria de saber agora?



**Explorar outro percurso**

**Concluir** 

