



**domínio  
Digital**

O essencial  
para uma presença  
online profissional

**1-outubro**  
10.00 - 11.30

# WEBINAR | Email Profissional: uma vantagem competitiva para o seu negócio

SCAN ME



A perspetiva da cibersegurança:  
riscos do email gratuito

Pedro Castro Henriques | CEO  
Strongstep



## SOBRE NÓS

Na Strongstep, somos uma consultora portuguesa especializada em **melhoria de processos** e **maturidade organizacional**.

## O que fazemos

Ajudamos organizações a implementar e certificar referenciais como:



**ISO 27001**



**CMMI**



**ISO 22301**



**TISAX**



**DORA**



**NIS2**



**ISO 42001**

# Quem Somos?

Porque estamos aqui:



O email continua a ser um dos principais pontos de exposição das organizações.



E é também um dos pontos onde podemos começar a reduzir o risco.

# Nos próximos 20 minutos



Vamos perceber porque é que o email continua a ser uma das principais portas de entrada para um ataque. E, sobretudo, como fechá-la.

## > 01 Porque o email?

Porque é que o email é hoje o alvo nº1 dos ataques às PME portuguesas

## > 02 Como acontece um ataque?

Como funciona, fase a fase, um ataque por email, e como se proteger.

## > 03 Onde está o risco?

Porque uma conta gratuita pode deixar uma PME mais exposta.

## > 04 Como nos protegemos?

3 medidas que pode implementar já, e o que fazer se o ataque já aconteceu.

# O email continua a ser uma das principais portas de entrada

O risco em Portugal, em números

# +1/4

dos incidentes de cibersegurança reportados em Portugal têm origem em phishing e variantes.

## >50%

das PME portuguesas sofreu pelo menos um ciberataque no último ano.

## +36%

de incidentes analisados pelo CERT.PT entre 2023 e 2024.

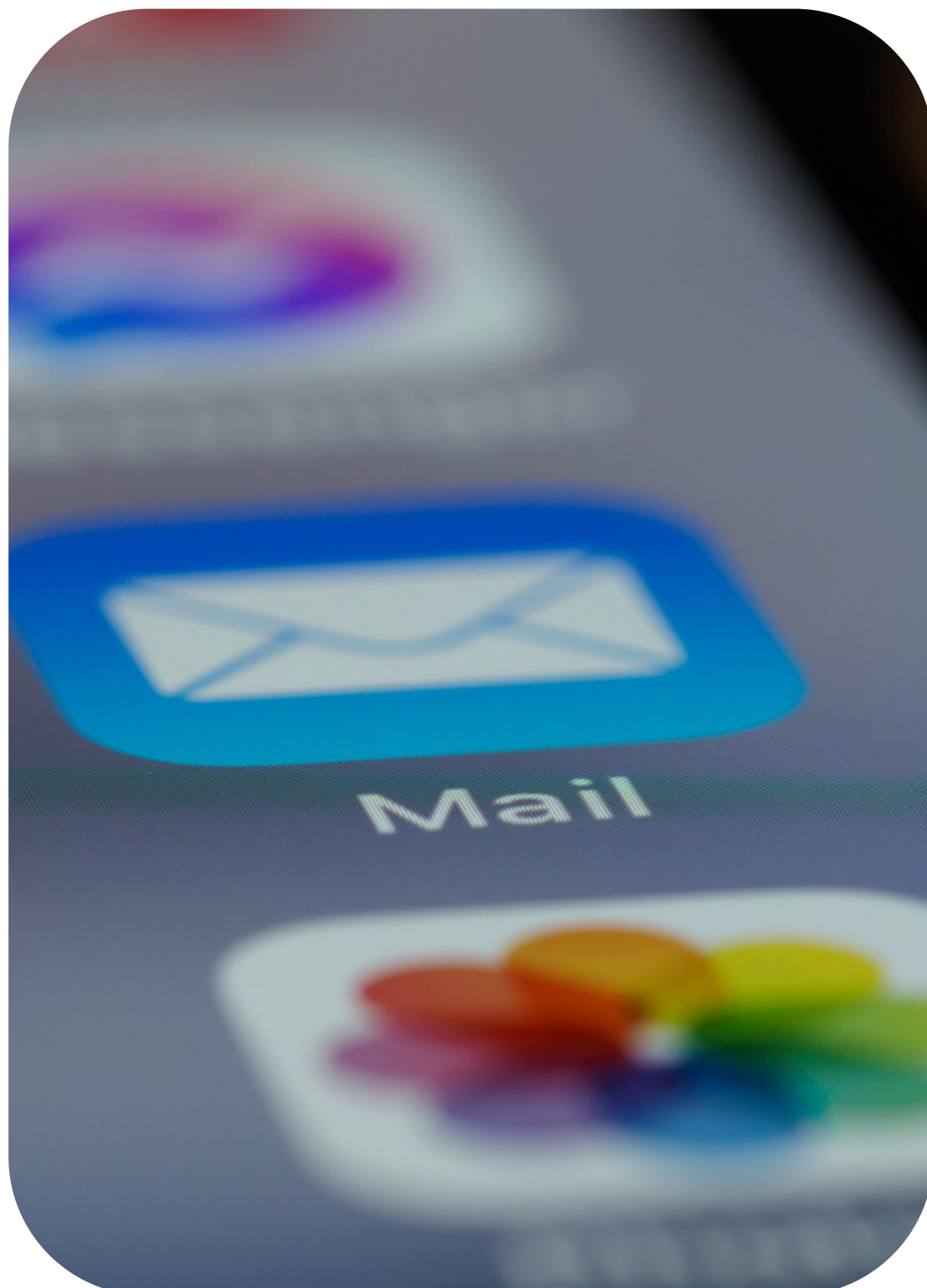
## IA GENERATIVA

permite criar emails de phishing personalizados em minutos.

## O RESULTADO?

Mais ataques, mais personalizados e mais difíceis de identificar.

# 1,23 M€. Uma fatura. Um email.



**Isto não é um cenário teórico. Aconteceram vários semelhantes em Portugal, em 2024.**

## > O email

A entidade portuguesa recebeu um pedido para alterar a conta bancária associada ao pagamento de uma fatura.

## > O engano

O endereço tinha diferenças subtis face ao email real do fornecedor, e passaram despercebidas.

## > A falha

A alteração não foi confirmada diretamente com o fornecedor antes da transferência de 1,23 M€.

## > O que evitou a perda

Os controlos internos detetaram a irregularidade e a conta de destino foi bloqueada a tempo.

**A sua empresa teria detetado isto a tempo?**

# Anatomia de um ataque

Do primeiro reconhecimento à saída do dinheiro

## 01 **Reconhecimento**

Primeiro, estudam a empresa.  
Fornecedores, faturas, pessoas-chave,  
organograma e redes sociais.  
Sem entrar nos seus sistemas.

## 02 **Contacto**

Depois, chega o email.  
Quase idêntico ao de um fornecedor  
ou gestor, muitas vezes num  
momento de pressão. Como férias.

## 03 **Pedido**

É aqui que tentam transformar  
confiança em dinheiro. “Alterámos o  
IBAN.”  
“Precisamos desta transferência hoje.”

## 04 **Execução**

O pagamento é feito.  
O dinheiro é rapidamente movimentado  
entre contas, muitas vezes internacionais,  
dificultando a recuperação.

***A variante mais simples (usurpação de identidade, spoofing,) nem precisa de invadir a sua conta: basta um email parecido com o seu para enganar quem confia em si.***

# Como se proteger de um ataque deste tipo

## Dupla validação

Alterações de IBAN e pagamentos acima de um valor definido exigem uma segunda aprovação.

**Sem exceções.**

## Separar funções

Quem pede, quem aprova e quem executa o pagamento não deve ser a mesma pessoa.

1

2

3

4

## Confirmar por telefone

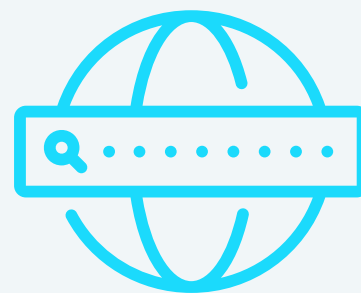
Mudou o IBAN? Ligue para um número já conhecido da empresa, nunca para o contacto indicado no email.

## Desconfiar da urgência

Prazos apertados e pressão para agir “agora” são, em si mesmos, um sinal de alerta.

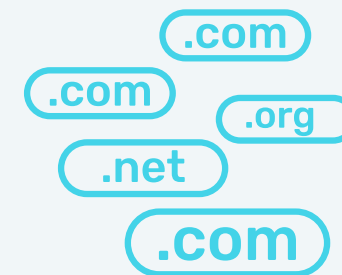
# Porque é que uma conta gratuita agrava o risco

O problema não é ser “gratuita”. É não controlar o domínio a partir do qual a sua empresa comunica.



## O domínio não é seu

Não controla tecnicamente a identidade usada pela empresa para comunicar.



## É mais fácil imitá-lo

Terceiros podem criar endereços semelhantes e fazer-se passar pela sua empresa.



## Não define as regras

Sem controlo do domínio, não consegue configurar políticas como SPF, DKIM e DMARC para proteger o envio em seu nome.



## Perde controlo sobre a confiança

Fica mais difícil proteger clientes, fornecedores e colaboradores contra emails que aparentam vir da sua empresa.

# O que está em jogo, para além do email



## > **Impacto financeiro direto**

Transferências fraudulentas raramente são recuperadas.

## > **Continuidade do negócio**

Indisponibilidade, gestão de crise, tempo consumido a apagar fogos.

## > **Confiança de clientes e parceiros**

Um cliente enganado por um email fraudulento “da sua empresa” pode nunca mais confiar em si.

## > **Exposição contratual**

Clientes maiores, já sujeitos ao NIS2, começam a exigir aos fornecedores garantias mínimas de segurança. Não estar preparado pode significar ficar de fora de concursos e parcerias.

# Medidas para começar esta semana

01

## Domínio próprio + autenticação

(SPF, DKIM, DMARC): a base técnica que prova que os seus emails são mesmo seus. Na prática, funciona como um selo de autenticidade: sem ele, qualquer pessoa pode “assinar” em seu nome.

02

## Autenticação multifator (MFA)

Em todas as contas de email, a medida com melhor relação custo-benefício que existe hoje. Ativa-se em minutos, nas definições de segurança da conta.

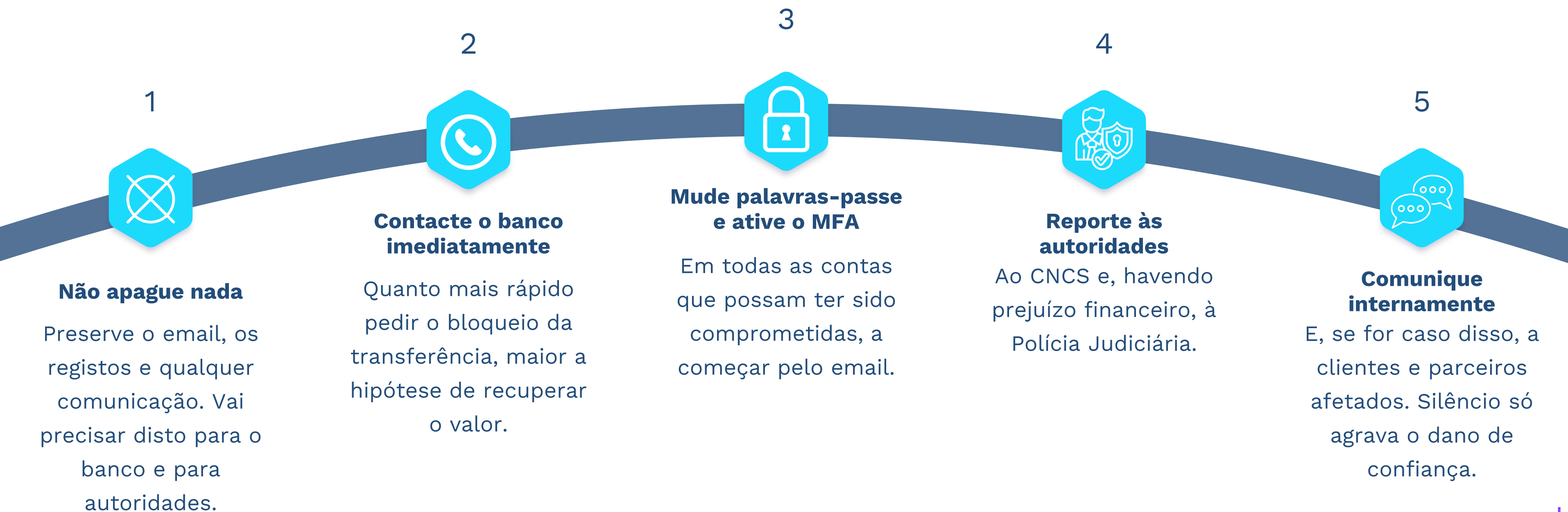
03

## Formação e reflexo crítico das equipas

A maioria dos ataques só funciona porque alguém clica ou confirma um pagamento sem verificar. 15 minutos de formação valem mais do que qualquer software.



# Se desconfiar que foi vítima: os primeiros passos



# Obrigado!

SCAN ME



## Contact:



+351 919 524 450



geral@strongstep.pt



www.strongstep.pt

