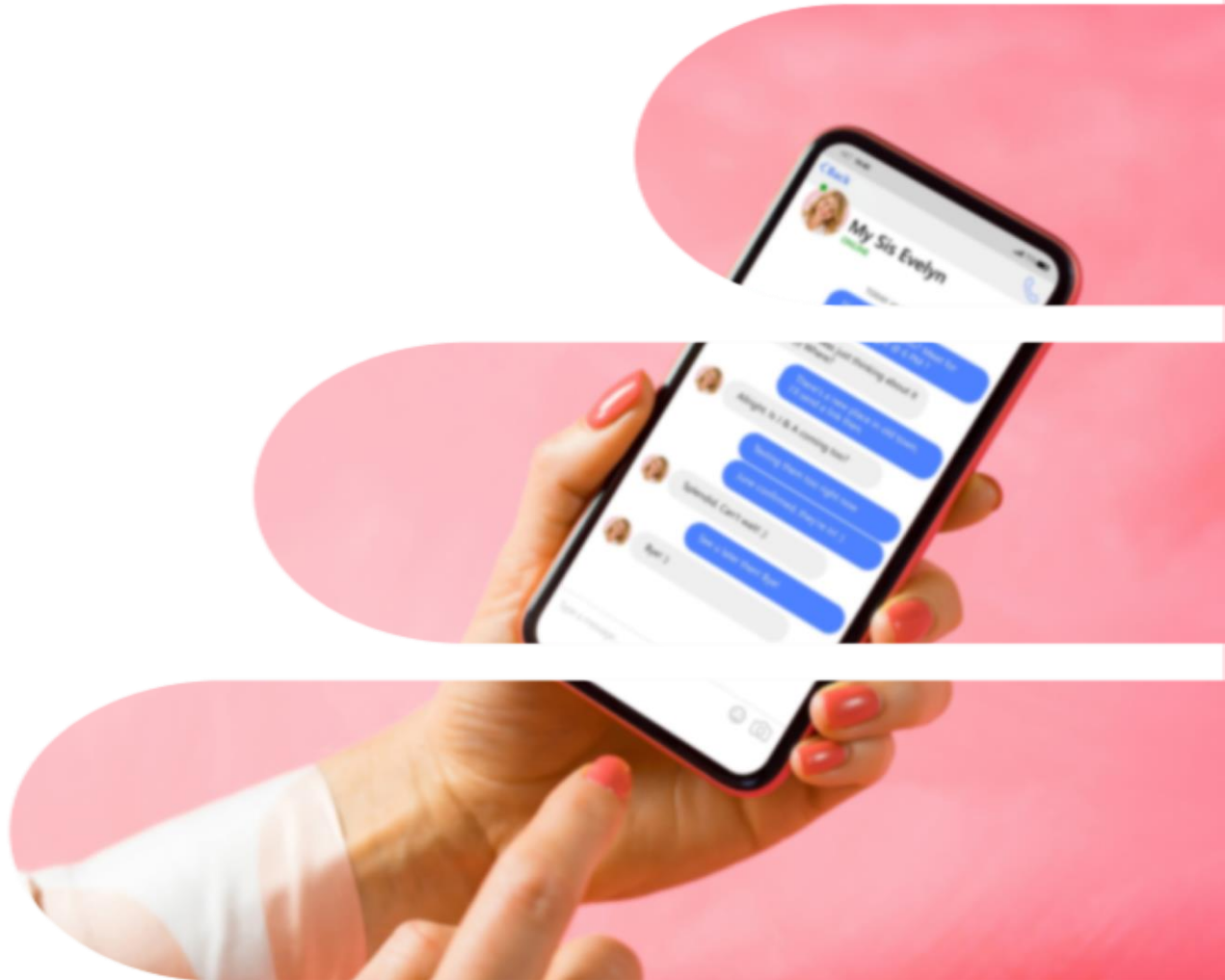




# Proteja-se contra o smishing



**O «Smishing» é um tipo de phishing que utiliza mensagens**

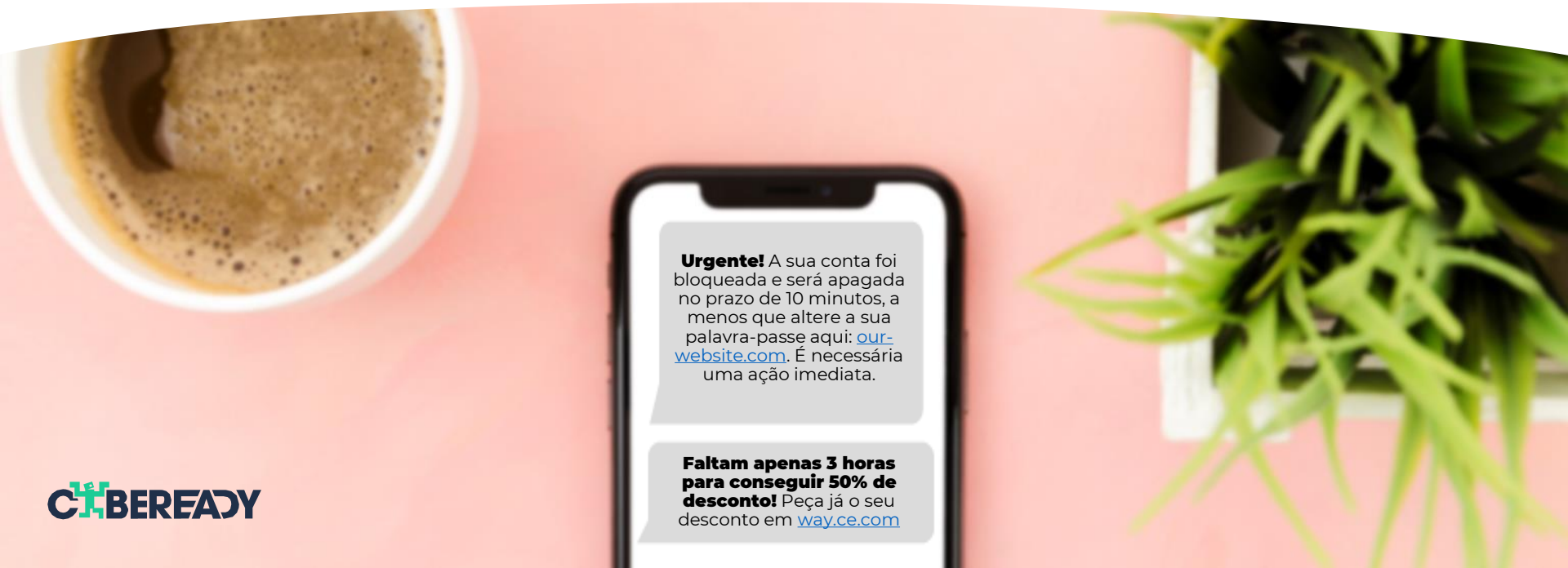
para induzir as pessoas a enviar dinheiro, palavras-passe ou informações pessoais e financeiras.

O smishing pode ocorrer em todas as plataformas de mensagens (não apenas por SMS) como o WhatsApp, WeChat, mensagens diretas nas redes sociais, etc.





A maioria das tentativas de smishing incluem um **prazo urgente, uma ameaça ou uma oferta apelativa** para encorajar os destinatários a agir rapidamente.



The background of the left side of the slide features a large, light pink curved shape. Within this shape are two white speech bubbles. The bubble in the foreground has three red dots inside it. The bubble behind it has a red paperclip icon inside it.

Algumas mensagens contêm  
**anexos ou ligações  
maliciosas,**

enquanto que outras pedem  
que o destinatário **responda  
diretamente** com  
informações pessoais.

## Os ataques típicos de smishing incluem:

### #1:

Notificações de encomendas falsas que imitam mensagens reais de encomendas por correio aproveitam-se dos nossos hábitos de compras online e do nosso desejo de seguir as entregas.



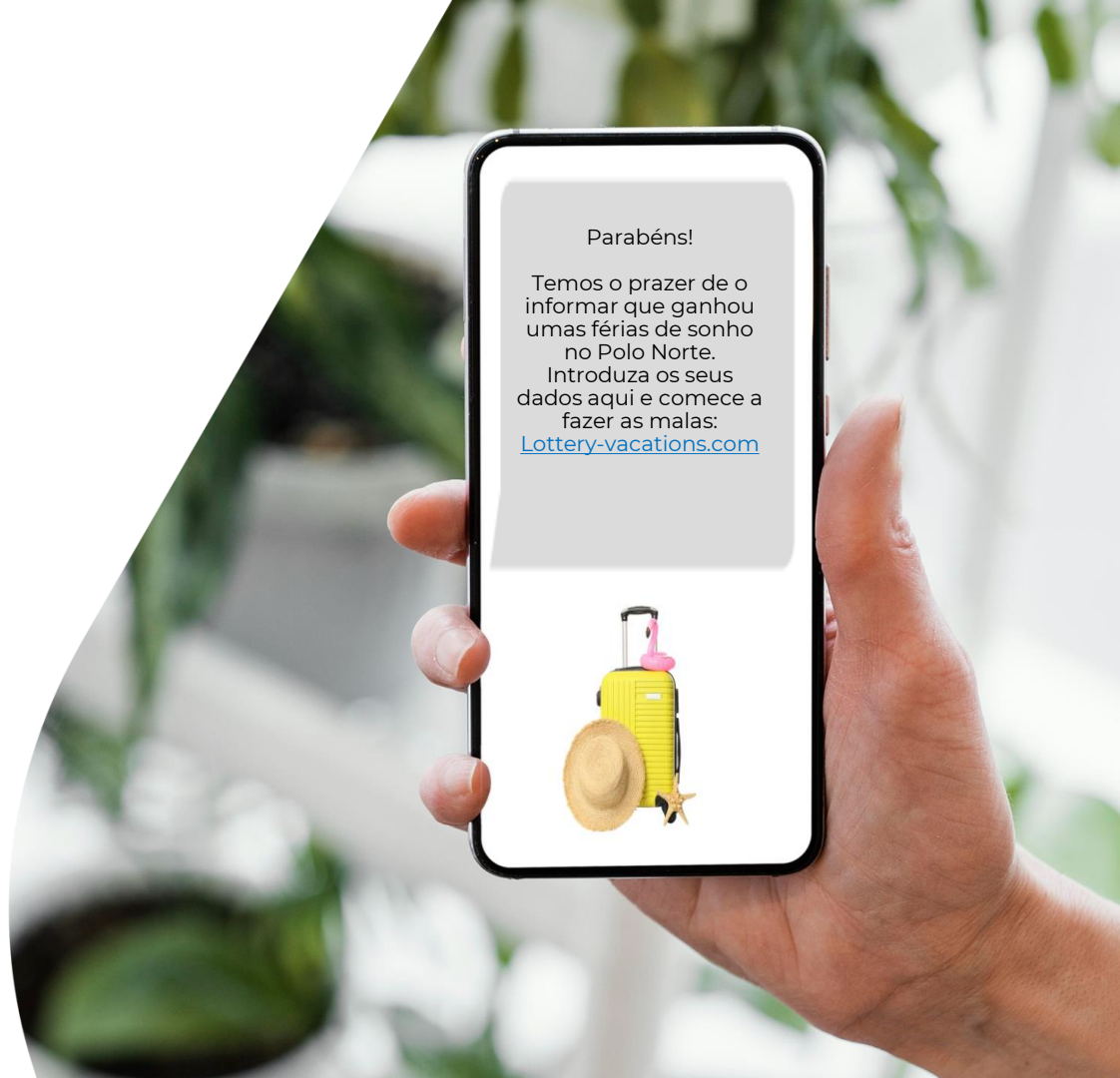
## #2:

Notificações falsas sobre a atividade da conta.

Mensagens como estas podem ser extremamente preocupantes, levando as pessoas a reagir de forma precipitada e descuidada.

### #3:

Mensagens que informam os destinatários de um prémio. Com o entusiasmo, as pessoas muitas vezes não se apercebem do absurdo que é ganhar um concurso ou um sorteio em que nunca participaram.





A hand with light-colored nail polish holds a black smartphone. The screen displays a chat interface with four messages. The background of the image is a blurred bokeh of warm, golden lights.

A sua conta de eletricidade  
está à sua espera aqui:  
[electric.com](http://electric.com)

Obrigado por ter pago a  
conta da eletricidade. A sua  
confirmação de pagamento  
é 39JE9

Uma nova atualização  
espera por si no site.

Tem uma dívida por  
pagar. Se o pagamento  
não for recebido no prazo  
de 24 horas, ser-lhe-á  
cortado o serviço. Pague  
aqui: [paynow.com](http://paynow.com)

## Preste atenção:

Recebeu uma mensagem nova com  
um tópico reconhecido e existente?  
Não é necessariamente fiável!

**Os hackers podem inserir  
mensagens maliciosas em  
conversas anteriores para que  
pareçam ter vindo da mesma fonte  
legítima.**



## O que nos torna **vulneráveis** ao smishing?

- Muitos de nós acreditam, erradamente, que as mensagens de texto são mais seguras do que outras formas de comunicação.
- Estamos habituados a receber muitas mensagens de números desconhecidos por dia.
- Os dispositivos móveis têm ecrãs pequenos, o que torna mais difícil prestar atenção a pequenos pormenores.



## O que pode fazer?

**Considere que qualquer mensagem de texto com ligações ou anexos não é segura**

e evite clicar nelas.

**Os botões de «Cancelar subscrição» também podem conter ligações maliciosas**

Não clique nesses botões.

**Não responda a mensagens de números desconhecidos**

por mais inocentes que pareçam.

**Preste atenção às expressões persuasivas**

como «atualização urgente» e «oferta por tempo limitado», uma vez que estas são criadas para o levar a clicar rapidamente.





## **Recebeu uma mensagem do seu banco ou da empresa de cartões de crédito?**

Verifique se a informação é apresentada no site ou na aplicação móvel.

Ou

Contacte um representante da empresa.

\*Não utilize quaisquer ligações ou números fornecidos na mensagem.





## **Recebeu uma notificação de entrega de encomenda?**

### **Se a empresa for muito conhecida:**

Sem clicar em qualquer ligação da mensagem, consulte o site da empresa e introduza aí o número da encomenda.

Verifique se os detalhes correspondem a um produto que encomendou e, em caso afirmativo, pode inserir a ligação da mensagem.

Se os detalhes da encomenda não forem encontrados, a mensagem é provavelmente falsa.



### **Se não estiver familiarizado com a empresa de entregas:**

- Utilize as redes sociais para avaliar a credibilidade da empresa.
- Se não conseguir encontrar qualquer prova da sua fiabilidade, ignore a mensagem.



## Lembre-se:

Se algo parecer estranho, é melhor não clicar ou responder.  
As mensagens maliciosas não podem prejudicá-lo se as **ignorar**.

