

# Dicas de SEGURANÇA BigCard



**Fique atento!** Ciber criminosos estão cada vez mais aprimorando suas técnicas. Pensando nisso, a BigCard traz abaixo algumas dicas que podem te ajudar a se prevenir de armadilhas enviadas por e-mail:



Os **“e-mails” phishing** (uma referência a ‘pescaria’) são utilizados por ciber criminosos para “fisgar” o destinatário da mensagem. Normalmente esse tipo de mensagem tem como objetivo:



Pedir dinheiro



Solicitar os dados do cartão de crédito.



Pedir que sejam compartilhados dados pessoais



Propagar vírus de computador a partir de um clique ou download de algum arquivo

## ALGUMAS DICAS PARA IDENTIFICAR:

### Você ganhou R\$100.00000!

Desconfie de ofertas muito vantajosas.

### E-mail do remetente estranho, muito diferente do habitual.

-----Mensagem original-----  
De: Análise de Crédito - BigCard <[analisedecredito@bigcard.com.br](mailto:analisedecredito@bigcard.com.br)> [[accounts@skinssanicare.com](mailto:accounts@skinssanicare.com)] Enviada em: quarta-feira, 26 de agosto de 2020 12:37

### Transfira um dinheiro ou abra o anexo!

Uma pessoa ou empresa conhecida pede que você faça algo que foge do usual.

### BigKard! Nós vai até você!

Texto escrito de forma errada ou com uma formatação/estilo que não condiz com o padrão normalmente utilizado.

### Links suspeitos. Na dúvida, não clique.

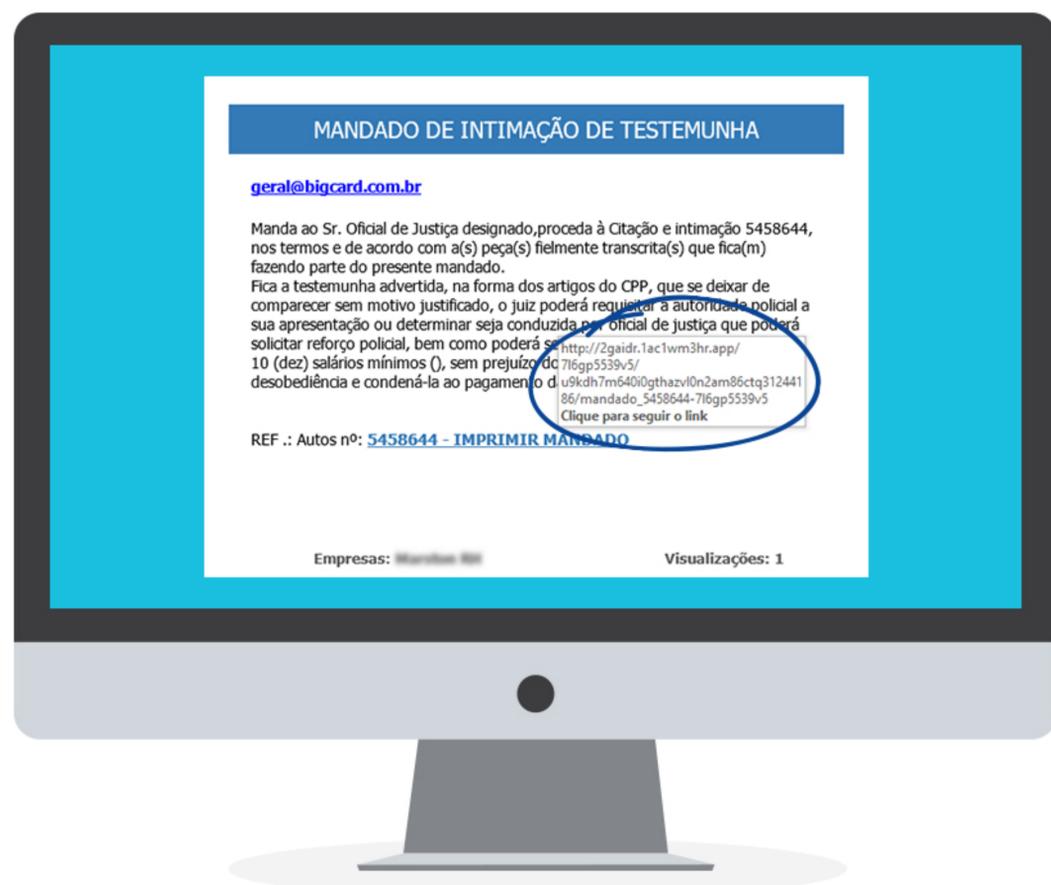
## MEDIDAS QUE VOCÊ PODE ADOTAR:



Não compartilhe suas senhas e logins de acesso a sites e e-mails. Evite senhas muito fáceis;



Antes de clicar em um link, passe seu mouse sobre ele sem apertar nada, para ver onde aquele link vai te levar. Desconfie de links muito estranhos e sem referência com o que a mensagem propõe;



Utilize um bom antivírus. Às vezes o barato pode sair caro demais; antivírus gratuitos nem sempre são uma boa ideia;



Ao acessar um site observe se há um cadeado ao lado da barra de endereços. Isso indica que o site adota alguns padrões de segurança.

