

E-mails suspeitos e Phishing

02/06/2025 15:06:46

[Imprimir artigo da FAQ](#)

Categoria:	# E-mails suspeitos e Phishing	Votos:	0
Estado:	público (todos)	Resultado:	0.00 %
Idioma:	pt_BR	Última atualização:	Ter 22 Abr 17:09:46 2025 (America/Sao_Paulo)

Palavras-chave

cartilha cert; segurança informações; emails suspeitos; phishing

Dúvida (ou problema) (público)

E-mails suspeitos

Resposta (ou solução) (público)

Fiquem atentos a e-mails suspeitos, mesmo que pareçam vir de dentro da nossa universidade. Golpistas frequentemente se disfarçam de remetentes confiáveis para roubar dados pessoais, informações de acesso e até mesmo solicitar transferências de dinheiro.

Nunca clique em links ou abra anexos de e-mails não solicitados ou de origem duvidosa, e jamais forneça sua senha, informações confidenciais ou realize qualquer pagamento solicitado por e-mail.

Sempre confirme a veracidade da mensagem entrando em contato diretamente com o setor responsável, por meio dos canais oficiais da universidade, mesmo se o suposto remetente informar que não terá condições de responder por outros meios. Essas informações de contato são amplamente divulgadas em nossos sites.

Recomendamos ainda a leitura do excelente material produzido pelo CERT.br, explicando esse tipo de golpe e como se prevenir.
[1]<https://cartilha.cert.br/fasciculos/phishing-golpes/fasciculo-phishing-golpes.pdf>

[1] <https://cartilha.cert.br/fasciculos/phishing-golpes/fasciculo-phishing-golpes.pdf>