

Cartilha E-MAILS E MENSAGENS INSTANTÂNEAS SEGURAS



OBJETIVO - FINALIDADE
SEGURANÇA - CONFIABILIDADE
AMBIENTE

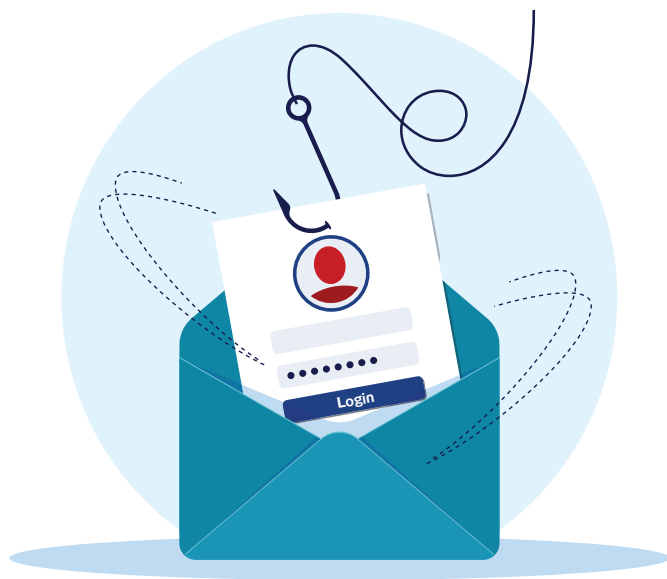


Nesta cartilha, abordaremos as práticas para garantir a segurança nas suas comunicações por e-mails e mensagens instantâneas. Aprenderemos como identificar e evitar scams por e-mail, como evitar clicar em links suspeitos e a importância da criptografia para proteger suas informações pessoais.



SCAM? O que é?

Scam é um golpe, fraude ou esquema ilegal através dos quais os criminosos usam diversas estratégias para obter dados pessoais, de forma criminosa, roubar dinheiro e bens, muitas vezes usando de engenharia social.



Desconfie de:

Correntes e pedidos de ajuda

Endereços de sites estranhos

Mensagens de remetentes desconhecidos

Mensagens de instituições governamentais e bancos

Confiabilidade

Verifique o remetente antes de clicar em qualquer link enviado por e-mail ou mensagem instantânea.

Não clique em links encurtados, use serviços que desvendam o link antes de acessá-lo.

Verifique a URL antes de clicar, passe o mouse sobre o link sem clicar para visualizar a URL completa.

Links suspeitos em mensagens instantâneas, nunca clique.

Não baixe anexos suspeitos ou de fontes não verificadas.

Use autenticação em dois fatores (2FA) para fortalecer a segurança das suas contas.





Criptografia de e-mails e mensagens, Segurança total!!!!

E-mails: Utilize serviços de e-mail que suportam criptografia de ponta a ponta (end-to-end), como PGP (Pretty Good Privacy) ou S/MIME.

Mensagens Instantâneas: Opte por aplicativos de mensagens que ofereçam criptografia de ponta a ponta.

Senhas fortes: Proteja suas chaves de criptografia com senhas fortes.

Compartilhamento seguro de chaves: Se você usa a criptografia de e-mail, compartilhe suas chaves de forma segura.

Mais dicas seguras!!!

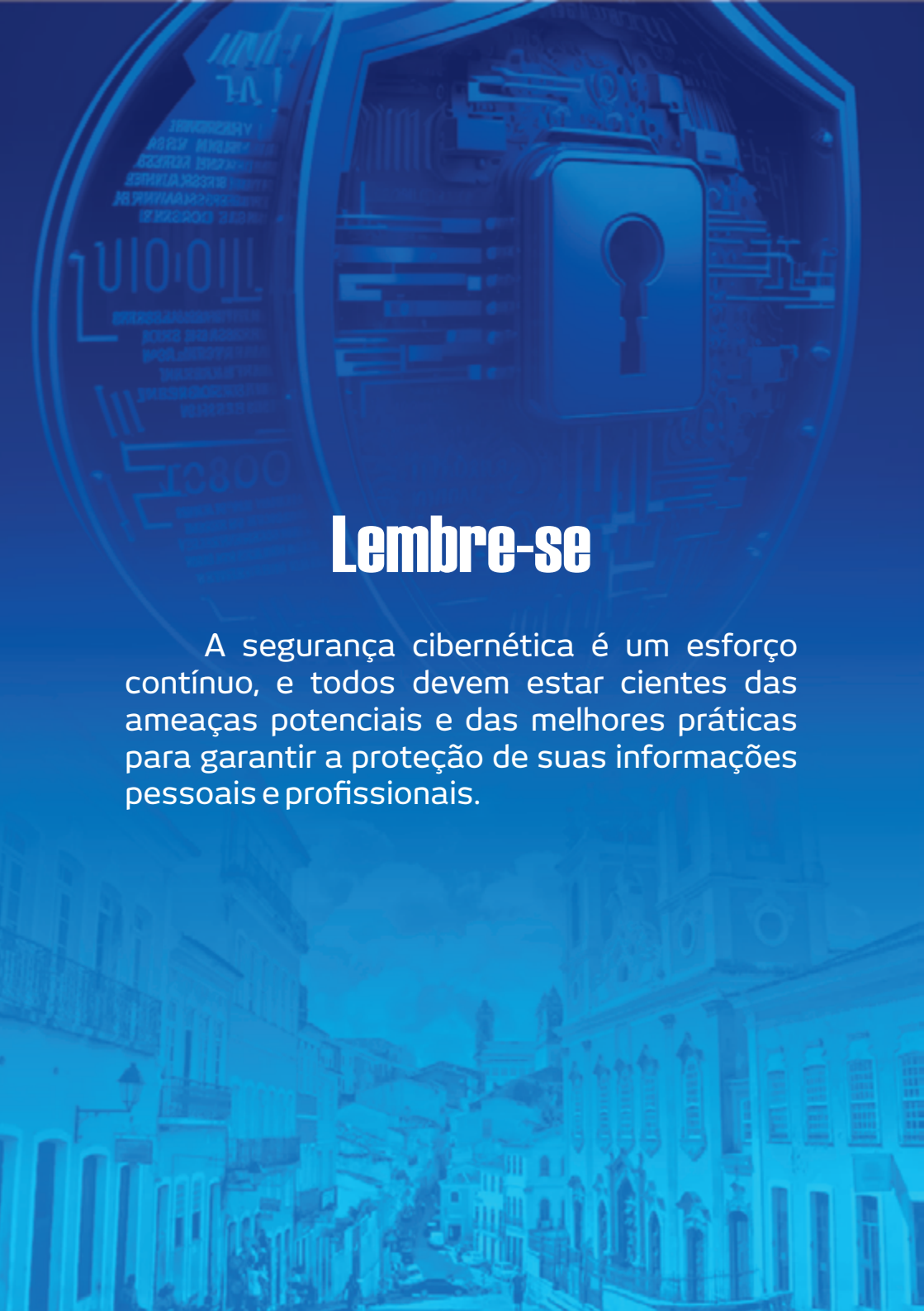
Mantenha seu software, aplicativos e sistemas operacionais sempre atualizados com as versões mais recentes.

Instale e mantenha atualizado.

Não envie informações sensíveis através de redes Wi-Fi públicas e desconhecidas. Utilize redes privadas ou VPN (Rede Privada Virtual) para garantir a segurança.

Seja Consciente! Busque informações sobre as melhores práticas de segurança cibernética.

Faça backups periódicos dos seus dados importantes e armazene-os de forma segura.



Lembre-se

A segurança cibernética é um esforço contínuo, e todos devem estar cientes das ameaças potenciais e das melhores práticas para garantir a proteção de suas informações pessoais e profissionais.



SEJA SEGURO!!!

COGEL

Companhia de Governança
Eletrônica de Salvador

Secretaria
de Inovação
e Tecnologia



SALVADOR
PREFEITURA