SPMS EPE
Serviços Partilhados do Ministério da Saúde

Cibersegurança SPMS

E-mail corporativo seguro

Porque é que a cibersegurança dos e-mails é importante?

O e-mail é uma ferramenta essencial para o trabalho do dia-a-dia dos profissionais, mas também é uma das principais portas de entrada para ataques de cibersegurança.

Garantir a segurança do seu e-mail é proteger-se a si, aos seus colegas, à sua instituição e a todos os cidadãos.

Cuidados ao receber e-mails

Verifique sempre o remetente. Confirme o endereço completo e desconfie de domínios estranhos.

Atenção a mensagens urgentes. Criminosos usam pressão psicológica como "a sua conta será bloqueada" ou "responda agora".

Cuidado com erros de escrita. Emails falsos normalmente têm erros ortográficos, formatação estranha ou não têm referências ou logótipos no rodapé.

Nunca abra anexos inesperados de formatos incomuns mesmo que venham de contactos conhecidos (.exe, .bat, .js, etc.)

Confirme por outros meios. Se receber um pedido estranho (ex: transferência, acesso para documento), confirme por telefone ou mensagem antes de agir.

Antes de clicar num link:

- Passe o cursor por cima e veja o endereço real.
- Copie e cole num editor de texto para analisar.
- Compare o domínio com o site oficial.

Cuidados ao enviar e-mails

Envie apenas para quem realmente precisa da informação. Evite múltiplos destinatários e cuidado com o "responder a todos".

Usar cópia oculta (BCC) quando envia e-mail para muitas pessoas que não se conhecem entre si, para os endereços não ficarem expostos.

Rever o conteúdo antes de enviar. Evite colocar informações sem necessidade, principalmente se for informação confidencial ou pessoal.

Evitar enviar informações pessoais, a menos que seja estritamente necessário ou com controlos de segurança aplicados.

Ao enviar informação confidencial, dados pessoais ou sensíveis:

- Use e-mails criptografados, ou
- Arquivos protegidos por password (ex. .zip ou .rar) enviados por canal separado.

Caso suspeite de um incidente de segurança

- Não interaja com o remetente ou com o conteúdo do e-mail, como links, anexos ou imagens no corpo do texto.
- Reporte imediatamente à equipa de cibersegurança ou de informática da sua entidade ou, em alternativa, à equipa de resposta a incidentes de cibersegurança da SPMS: **csirt@spms.min-saude.pt**