Problemas de Segurança Cibernética

- Recebi um e-mail fraudulento (Orientações sobre Phishing)
- Como reportar Phishing na UFLA
- Configuração de Privacidade dos Espaços do Google Workspace

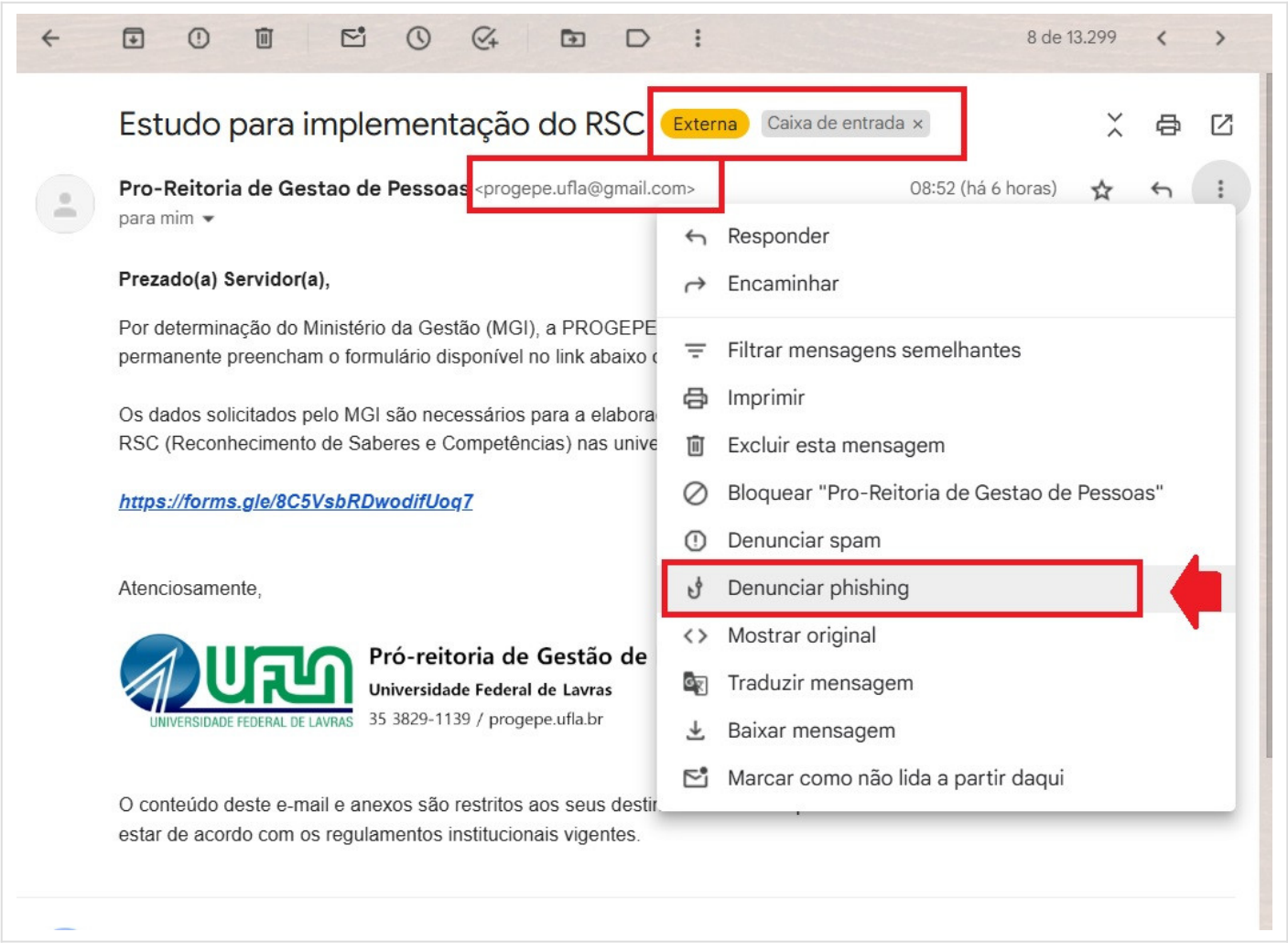
Recebi um e-mail fraudulento (Orientações sobre Phishing)

Procedimento de Operação Padrão (POP) de como proceder ao identificar ou suspeitar de uma tentativa de phishing.

1. **Reconhecer os sinais de phishing**

- **Verifique o remetente**: Confira se o e-mail ou mensagem vem de um domínio legítimo (ex.: nomedousuario@ufla.br);
- **Desconfie de urgência**: Phishing muitas vezes usa táticas de urgência ou pressão para induzir ações rápidas;
- **Cuidado com links e anexos**: Evite clicar em links ou baixar arquivos sem antes verificar sua autenticidade;
- **Erros de gramática**: Mensagens de phishing frequentemente contêm erros ortográficos ou gramaticais.

Obs.: Veja na imagem a seguir como identificar indícios de fraude e como denunciar o e-mail.



2. Não interagir com o conteúdo suspeito

- Não clique em links ou anexos suspeitos;
- Não forneça informações pessoais, financeiras ou senhas em resposta à mensagem.

3. Registrar evidências do ataque

- Tire capturas de tela da mensagem, incluindo remetente, assunto e conteúdo;
- Não apague o e-mail ou mensagem antes de notificar o setor responsável.

4. Reportar a tentativa de phishing

- Informe imediatamente ao setor de segurança da informação ou Diretoria de Gestão de Tecnologia da Informação;
- Caso receba o phishing em um e-mail Institucional, use os mecanismos institucionais para relatar, como "Reportar phishing";
- Envie as evidências coletadas para análise.

5. Realizar ações de mitigação, se necessário

- **Caso tenha clicado em um link ou baixado um arquivo suspeito**:
  - Desconecte-se imediatamente da rede;
  - Faça uma varredura com um software antivírus atualizado.
- **Caso tenha fornecido dados pessoais ou senhas**:
  - Alterar imediatamente as credenciais comprometidas;
  - Informe ao setor de segurança da informação para medidas adicionais.

6. Notificar possíveis afetados

- Caso o ataque tenha impactado outras pessoas ou serviços, informe os usuários e a gestão para adoção de medidas preventivas.

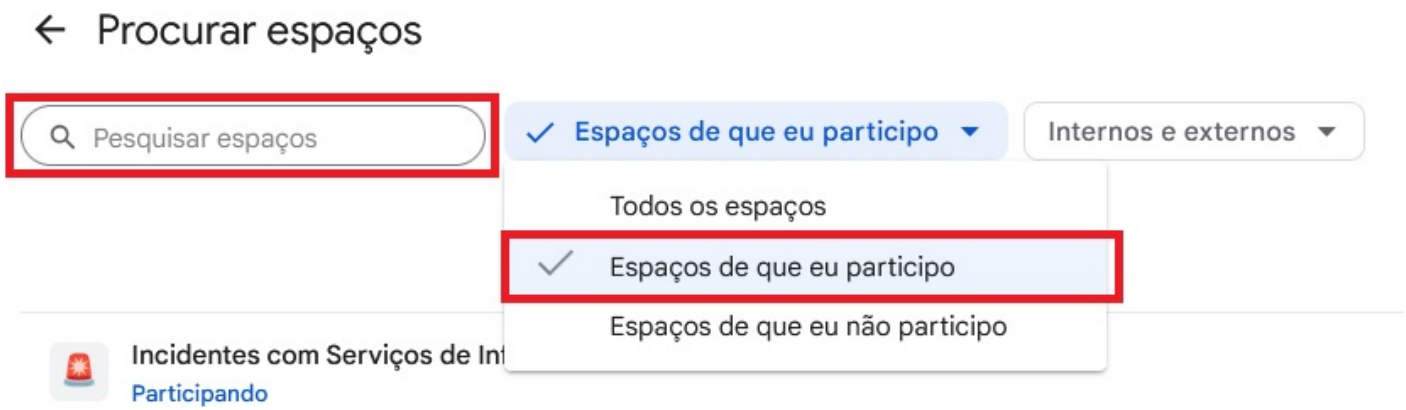
Como reportar Phishing na UFLA

Para relatar um Incidente de Segurança na Rede UFLA, abra um chamado de suporte através do **Catálogo de Serviços de TI** ("servicosti.ufla.br" >> "Segurança da Informação" >> "Notificações de Problemas de Segurança") ou entre em contato conosco pelo e-mail **etir@ufla.br**, ou no telefone **(35) 3829-1512**.

Configuração de Privacidade dos Espaços do Google Workspace

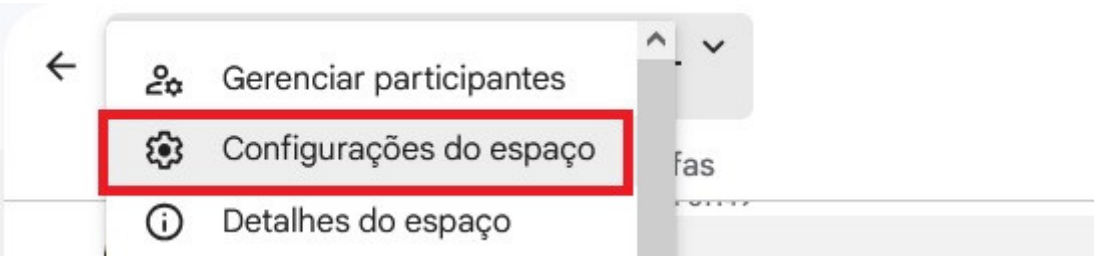
Os espaços criados no Google Workspace possuem uma configuração de privacidade que permite que o conteúdo do espaço fique visível para qualquer membro da comunidade acadêmica que possua uma conta de e-mail institucional. Caso o espaço que você gerencia foi criado com o intuito de estar acessível apenas a um grupo limitado de pessoas de um determinado departamento ou setor, é necessário realizar uma modificação nas configurações de privacidade:

1. Acesse o endereço: https://mail.google.com/chat/u/0/#browse/chat/q=
2. No campo de buscas, selecione a opção de **Espaços que eu participo** ou procure pelo nome do espaço que você gerencia no campo **Pesquisar Espaços**.

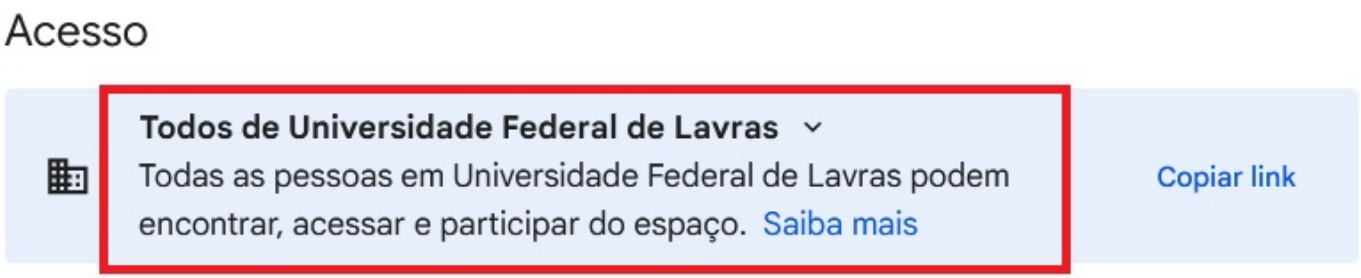


3. Ao encontrar o espaço que você gerencia, clique no **nome do espaço**.

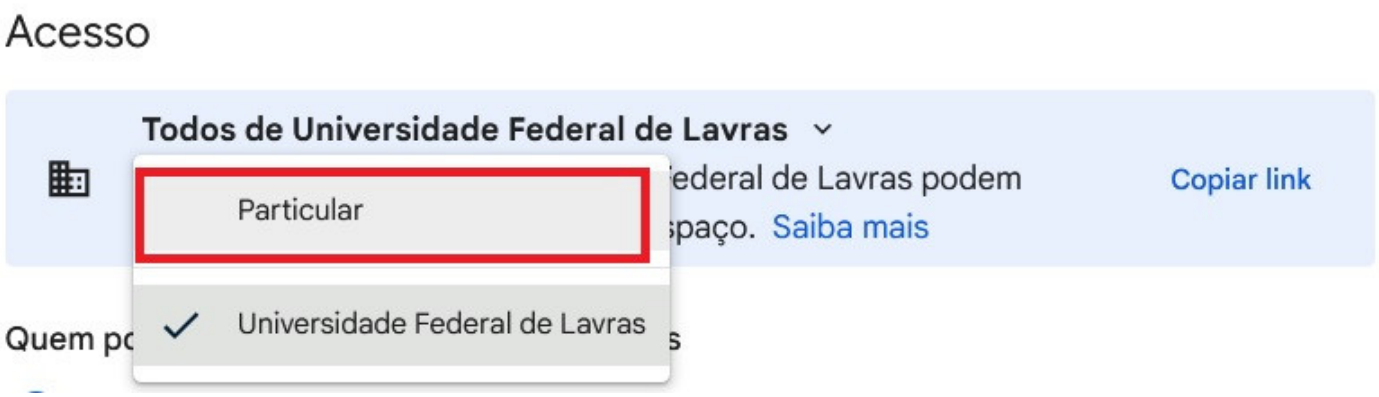
4. Um menu se abrirá abaixo, clique na opção **Configurações do Espaço:**



5. Veja se o parâmetro de Acesso ao espaço está configurado como **Todos de Universidade Federal de Lavras** ou **Particular**.



6. Caso a primeira opção esteja marcada, mude para a opção **Particular**.



7. Após a mudança, o espaço ficará acessível **apenas para os participantes do Espaço** e as conversas não ficarão mais visíveis para terceiros.