- **Verifique o Remetente**: Sempre analise o endereço de e-mail do remetente. Cibercriminosos costumam usar endereços que se parecem com os legítimos, mas têm pequenas alterações.
- **Desconfie de Links e Anexos**: Passe o mouse sobre links antes de clicar para ver o URL real. Evite abrir anexos de fontes desconhecidas.
- **Cuidado com Urgência**: Mensagens que criam um senso de urgência, como ameaças de fechamento de conta, são frequentemente tentativas de phishing. Tome seu tempo para verificar a veracidade.
- **Não Compartilhe Informações Sensíveis**: Nunca forneça senhas, números de cartão de crédito ou outras informações pessoais por e-mail ou mensagens.
- **Utilize a Autenticação Multifatorial (MFA)**: Ative a MFA sempre que possível. Isso adiciona uma camada extra de segurança, mesmo que suas credenciais sejam comprometidas.
- **Atualize Seu Software**: Mantenha seu sistema operacional e softwares de segurança atualizados para proteger-se contra vulnerabilidades conhecidas.
- **Eduque-se e Treine Outros**: Participe de treinamentos sobre cibersegurança e compartilhe informações com colegas para aumentar a conscientização sobre phishing.
- **Use um Gerenciador de Senhas**: Um gerenciador de senhas pode ajudar a criar e armazenar senhas complexas, reduzindo a chance de uso de senhas fracas.
- **Verifique a Ortografia e a Gramática**: Mensagens de phishing muitas vezes contêm erros de digitação ou gramática. Desconfie de qualquer comunicação que pareça inadequada.
- **Denuncie Tentativas de Phishing**: Caso receba uma mensagem suspeita, denuncie-a ao seu provedor de e-mail ou à equipe de TI da sua empresa.