

CYBER NEWS

O Boletim Informativo Oficial de Gestão de Riscos em Terceiros



NESTA EDIÇÃO

PROTEÇÃO DE E-MAIL E NAVEGADOR WEB

- O que é?
- Por que é importante?
- Ameaças Comuns
- Sinais de Alertas
- O que fazer?
- Boas Práticas

CONCLUSÃO

Você sabia que e-mails e sites inseguros são as principais portas de entrada para ataques cibernéticos?

Neste volume, vamos explorar boas práticas de segurança no uso do e-mail e do navegador web, mostrando como essas medidas podem proteger sua empresa contra ameaças digitais.

PROTEÇÃO DE E-MAIL E NAVEGADOR WEB

A proteção de e-mail e navegador web é essencial para garantir a segurança digital de usuários e empresas. Esses dois canais são os principais alvos de cibercriminosos, que utilizam técnicas como **phishing**, **malware** e **sites falsos** para roubar dados ou comprometer sistemas.



O que é?

Proteção de E-mail e Navegador Web é um conjunto de práticas e tecnologias voltadas para garantir a segurança durante o uso de e-mails e a navegação na internet.

Esses dois canais são os mais comuns para ataques cibernéticos, como phishing, malware e roubo de dados.

Por que é importante?

- 🔒 Prevenção contra ataques de phishing e roubo de dados;
- 🛡️ Redução do risco de infecção por malware via e-mail e navegação;
- 📄 Conformidade com políticas de segurança da informação;
- 🌐 Segurança na navegação e proteção contra sites maliciosos.

⚠️ Ameaças comuns

- 📎 Anexos maliciosos em e-mails;
- 🔗 Links de phishing em mensagens e redes sociais;
- 🌐 Sites falsos que imitam páginas legítimas;
- 🌿 Extensões de navegador maliciosas.

🔍 Sinais de alerta

- 🐢 Lentidão incomum ao navegar;
- 🌐 Redirecionamentos para sites estranhos;
- 🗨️ Pop-ups constantes e suspeitos;
- 📁 Downloads inesperados.



📌 O que fazer:

- 🚫 Não clique em links ou baixe arquivos suspeitos;
- 📞 Avise o time de TI ou Segurança da Informação;
- 📄 Documente o ocorrido (mensagens, sites acessados, etc.).

Boas Práticas:

- 🔒 Use senhas fortes e únicas;
- 📧 Desconfie de e-mails não solicitados;
- 🌐 Navegue apenas em sites com HTTPS;
- 🛡️ Utilize ferramentas de proteção como antivírus e firewalls.
- ✅ Verifique remetentes e evite clicar em links suspeitos;
- ✅ Utilize autenticação em dois fatores (2FA);
- ✅ Mantenha navegadores e extensões atualizados;
- ✅ Use bloqueadores de pop-ups e extensões confiáveis.

Conclusão

Adotar boas práticas de segurança, manter sistemas atualizados e estar atento a comportamentos suspeitos são atitudes essenciais para proteger os dados da empresa. A prevenção continua sendo a melhor estratégia contra incidentes.

Em caso de dúvidas ou situações incomuns, entre em contato com a equipe de TI ou Segurança da Informação.