Checklist de Prevenção contra Engenharia Social 2025

Você sabia que 98% dos ciberataques exploram erros humanos? (IBM, 2024) A engenharia social – como phishing, SMS falsos ou deepfakes – custou US$ 12,5 bilhões em fraudes em 2024 (FBI IC3). Este checklist gratuito traz 10 ações práticas para proteger indivíduos e empresas em 2025, sem jargões técnicos. Seja no WhatsApp, e-mail ou reuniões virtuais, mantenha-se um passo à frente dos golpistas. 🚨 #Ciberseguranca2025

Dica: Leia o artigo completo em [No Próximo Nível] para mais detalhes.

---

1. Eduque-se e Treine Sua Equipe

- [ ] Fazer um curso ou assistir vídeos educativos sobre golpes digitais (ex.: phishing, smishing) em fontes como Kaspersky ou Serasa.
  Dica: 45% dos funcionários falham em testes de phishing (KnowBe4, 2025).
- [ ] Simular ataques de phishing.
  - Empresas: usar ferramentas como Hoxhunt para treinar equipes.
  - Indivíduos: testar links suspeitos em VirusTotal.
    Dica: Treinamentos gamificados reduzem cliques em 40% (Proofpoint, 2025).
- [ ] Criar uma política de segurança interna.
  - Proibir o compartilhamento de senhas por e-mail ou WhatsApp.
  - Exemplo: “Nunca envie credenciais sem verificar a identidade.”

2. Implemente Controles Técnicos

- [ ] Ativar autenticação multifator (MFA) em e-mails, aplicativos bancários e redes sociais.
  - Usar apps como Google Authenticator ou LastPass.
    Dica: MFA reduz 99% dos ataques de credenciais (Microsoft, 2024).
- [ ] Instalar filtros de e-mail para marcar mensagens suspeitas.
  - Configurar no Gmail ou Outlook.
    Dica: Filtros bloqueiam 91% dos phishing iniciais (Verizon, 2025).
- [ ] Utilizar ferramentas anti-deepfake.
  - Empresas: adotar soluções como SentinelOne.
  - Indivíduos: desconfiar de chamadas ou vídeos com comportamento estranho.

3. Verifique e Limite Exposição

- [ ] Adotar o princípio Zero Trust.
  - Verificar toda solicitação, mesmo de “chefes” ou “bancos”.
  - Confirmar por canais oficiais (telefone, aplicativo).
    Dica: Zero Trust reduz violações em 50% (Forrester, 2024).
- [ ] Reduzir dados públicos disponíveis.

    - Limitar informações no LinkedIn (e-mail, telefone).
    - Usar o site Have I Been Pwned? para receber alertas de vazamentos.

4. Responda Rapidamente a Incidentes

- [ ] Ter um plano de resposta a incidentes.
    - Indivíduos: congelar contas bancárias em caso de suspeita de golpe (ligar para o banco).
    - Empresas: seguir um plano formal de resposta a incidentes (IR).
      Dica: Um IR rápido economiza até US$ 1,2 milhão (IBM, 2024).
- [ ] Denunciar ataques.
    - No Brasil: contatar ANPD (Agência Nacional de Proteção de Dados) ou a Febraban.
    - Globalmente: reportar ao FBI IC3.
      Dica: 83% das empresas melhoram defesas após análise de incidentes (Varonis, 2024).

Bônus: Dicas Rápidas

- **Desconfie de urgência:** E-mails ou SMS com *“atualize agora”* ou *“pague hoje”* são suspeitos.
- **Verifique links:** Passe o mouse sobre URLs antes de clicar; use apps como Kaspersky para checar.
- **Atualize senhas:** Use senhas únicas (ex.: “Sol4r$2025!”) e troque a cada 6 meses.

Quer Ir Além?

Este checklist é o primeiro passo para segurança digital. No blog, há mais dicas para proteger dados pessoais e empresariais. Visite [link do blog] e junte-se à comunidade.

Baixe o Guia Completo de Cibersegurança 2025

Para mais estratégias, insira o e-mail no blog: [link].

Compartilhe Sua Experiência

Já enfrentou um golpe digital? Qual ação será testada primeiro? Comente no blog ou marque com **#Ciberseguranca2025**.