PÍLULAS DE SEGURANÇA DE DADOS

Boletim Mensal sobre Segurança da Informação
JUNHO/2025

O que é Engenharia Social?

Engenharia social é uma tática que explora a confiança, curiosidade ou até a boa vontade das pessoas para obter acesso não autorizado a dados, sistemas ou áreas restritas. Ao invés de forçar tecnicamente um sistema, o atacante manipula os funcionários para conseguir o que deseja.

🚨 Sinais e Exemplos de Ataques de Engenharia Social:

Telefonemas ou mensagens urgentes: uma pessoa, fingindo ser técnico de TI ou gerente, liga solicitando sua senha ou dados de acesso "para resolver um problema urgente".
E-mails falsos: recebimento de mensagens que parecem oficiais solicitando atualizações de cadastro, confirmação de informações pessoais ou links para redefinição de senha.
Visitas presenciais: alguém alegando ser fornecedor ou novo colaborador tenta circular livremente pela empresa ou obter informações em balcão de atendimento.
Pedidos de ajuda: solicitações por telefone ou pessoalmente, por exemplo: "Estou com problemas para acessar o sistema, você pode me passar seu login rapidinho?"

🔒 Como se Proteger na Prática:

Desconfie de solicitações inesperadas: nunca compartilhe senhas, códigos ou dados pessoais, mesmo se o pedido vier de alguém dizendo ser parte da equipe interna. Sempre confirme a identidade usando canais oficiais.
Não clique ou baixe sem verificar: ao receber e-mails ou mensagens com links ou anexos, especialmente se vierem com senso de urgência, analise o remetente e procure sinais de fraude antes de qualquer ação.
Evite "atalhos" de segurança: jamais permita o acesso de terceiros ao seu computador, nem compartilhe informações sigilosas em conversas informais ou por aplicativos não oficiais.
Reporte tentativas imediatamente: se receber qualquer contato ou abordagem suspeita, comunique imediatamente ao setor de segurança da informação. Agir rapidamente pode evitar incidentes maiores.

PERGUNTA DO MÊS: "Posso confiar em e-mails que parecem oficiais, mas pedem meus dados ou exigem ação rápida?"
RESPOSTA: Não confie automaticamente! Sempre verifique o remetente, leia com atenção e, se houver qualquer dúvida, consulte o setor de TI ou segurança antes de responder ou clicar em links.