PÍLULAS DE SEGURANÇA DE DADOS

Boletim Mensal sobre Segurança da Informação | **JULHO/2024**

GOLPES COMUNS E COMO EVITÁ-LOS:

Confira nesta edição, os tipos mais comuns de golpes e as medidas preventivas que podem ser adotadas para evitá-los, especialmente no contexto de proteção de dados e segurança digital.

- Clonagem de WhatsApp
- Boleto falso
- *Phishing*

http://

Confira todas as edições do Boletim Mensal em nosso site:
hospitalourobranco.com.br/comite-de-protecao-de-dados/

80 ANOS HOSPITAL OURO BRANCO EXCELÊNCIA EM SAÚDE
ACREDITADO

CLONAGEM DE WHATSAPP

Descrição do Golpe (exemplo):
O criminoso entra em contato com a vítima, fingindo ser um funcionário legítimo de um banco ou site de compras, e solicita o fornecimento de um código de verificação que supostamente foi enviado para ela. Ao fornecer o código, a vítima permite que o criminoso acesse sua conta do *WhatsApp*, que é então utilizada para realizar crimes em nome dela.

Como Evitar:
- Confirmação em Duas Etapas: ative a verificação em duas etapas no *WhatsApp*. Isso adiciona uma camada extra de segurança, exigindo um PIN além do código de verificação;
- Desconfie de pedidos de urgência: seja cético em relação a mensagens que solicitam ações imediatas ou urgentes, especialmente se pedirem informações pessoais ou financeiras;
- Não instale aplicativos de terceiros: baixe aplicativos apenas de fontes oficiais, como Apple App Store, etc.

BOLETO FALSO

Descrição do Golpe:
O criminoso envia um *link* falso que altera o código de barras de um boleto, direcionando o pagamento para a conta dele.

Como Evitar:
- Verifique o Beneficiário: sempre confira o nome do beneficiário no boleto;
- Confira o Código do Banco: verifique se o código do banco no boleto corresponde ao banco do beneficiário;
- Confirme com o Emissor: entre em contato diretamente com o emissor do boleto para confirmar a veracidade do documento.

PHISHING

Descrição do Golpe:
O criminoso envia *links*, *e-mails* ou SMS com anexos, explorando emoções como curiosidade, medo ou urgência, para induzir a vítima a clicar em *links* maliciosos ou fornecer informações pessoais.

Como Evitar:
- Evite Redes Públicas: não acesse contas bancárias ou realize compras *online* em redes públicas ou não seguras;
- Não abra *e-mails* duvidosos: desconfie de *e-mails* de remetentes desconhecidos ou com conteúdo suspeito;
- Não execute Programas de fontes não oficiais: baixe e instale programas apenas de sites oficiais;
- Não clique em *links* anexados: evite clicar em *links*, *e-mails* ou mensagens de texto, a menos que tenha certeza de sua autenticidade;
- Compre em sites confiáveis: realize compras *online* apenas em sites conhecidos e confiáveis.