



PREVENÇÃO E COMBATE A FRAUDE DIGITAL

Módulo I
Golpe da Prova de Vida

O Golpe da Prova de Vida

O Golpe da Prova de Vida funciona por meio de **engenharia social**, onde os criminosos fingem representar bancos ou instituições previdenciárias como o INSS ou IGEPPS, para induzir a vítima a:

- Fornecer dados pessoais, como fotos e vídeos, documentos e etc;
- Autorizar ativação de dispositivos;
- Autorizar operações bancárias.

Como reconhecer o golpe?

CENÁRIO 1: Contato do “banco” via WhatsApp ou ligação

O golpista entra em contato por telefone ou WhatsApp afirmando ser funcionário de um banco ou da previdência social (INSS ou IGEPPS) e, com linguagem técnica e protocolos falsos, alerta para a necessidade da realização de prova de vida ou atualização do seu cadastro.

O que o golpista pede:

- Uma selfie segurando um documento com foto (RG, CNH);
- Um vídeo curto dizendo uma frase específica (ex: “confirmando que estou vivo e autorizo o uso dos meus dados para prova de vida”);
- Que a vítima clique em um link de acesso falso.

O que o golpista pretende:

- Coletar dados e biometria facial para futuras transações fraudulentas (empréstimos, abertura de contas, etc);
- Burlar os sistemas de autenticação facial.



CENÁRIO 2: Aplicativos ou sites falsos (phishing)

A vítima recebe um e-mail ou SMS com link que direciona para um site ou aplicativo falso, com aparência idêntica aos oficiais da previdência social ou do banco.

O que o site/aplicativo falso solicita:

- CPF, nome completo, data de nascimento;
- Dados bancários;
- Cópia de documentos ou selfies;
- Senhas ou tokens de autenticação.

O que o golpista pretende:

- Instalar um aplicativo falso e capturar dados sensíveis do celular;
- Aplicar golpes como abertura de conta, contratação de empréstimos ou transferência de benefícios.

CENÁRIO 3: Golpe presencial (falso agente da previdência ou do banco)

Criminosos visitam a residência da vítima alegando que foram designados para “*fazer a prova de vida presencial*” devido às dificuldades de locomoção do idoso.

O que o golpista pretende:

- Instalar malware no celular ou computador da vítima e capturar dados sensíveis;
- Aplicar golpes como abertura de conta, contratação de empréstimos ou transferência de benefícios, utilizando os dados coletados na visita.

Dica rápida para reconhecer o golpe:

Se alguém pedir:

-  Uma selfie ou vídeo com documento;
-  Senha, código por SMS ou token;
-  Que clique em um link fora do site oficial.

 **É GOLPE!**

Caiu no golpe?

Denuncie o mais rápido possível!

FRAUD ALERT



CONFIRM

Como se proteger:

- Desconfie sempre de contatos inesperados;
- Nunca clique em links recebidos por mensagem;
- Prova de vida digital só é feita pelo aplicativo oficial do banco ou do instituto de previdência social;
- Nunca forneça informações a estranhos;
- Nunca envie documentos ou fotos por WhatsApp;
- Mantenha seus dados sempre atualizados no banco e no INSS ou IGEPPS;
- Converse com a família sobre segurança digital.

Caiu no golpe, o que fazer?

1 Interrompa imediatamente qualquer comunicação com o golpista
Bloqueie números, e-mails ou perfis usados para o golpe. Não forneça mais nenhuma informação.

2 Informe seu banco ou instituição financeira
Verifique movimentações recentes, solicite bloqueio temporário de conta, recuperação ou reversão da transação, se ainda estiver em andamento.

3 Registre um Boletim de Ocorrência
Detalhe o máximo possível: datas, números de telefone usados, valores transferidos, nomes mencionados.

Comunique o golpe às instituições oficiais

4 INSS - ligue 135 ou por meio do aplicativo “Meu INSS”.
IGEPPS - ligue (91) 3217-7037 ou (91) 3182-3500 (whatsApp).

5 **Alerte familiares e responsáveis!**



Banpará

#JuntosContraFraudes