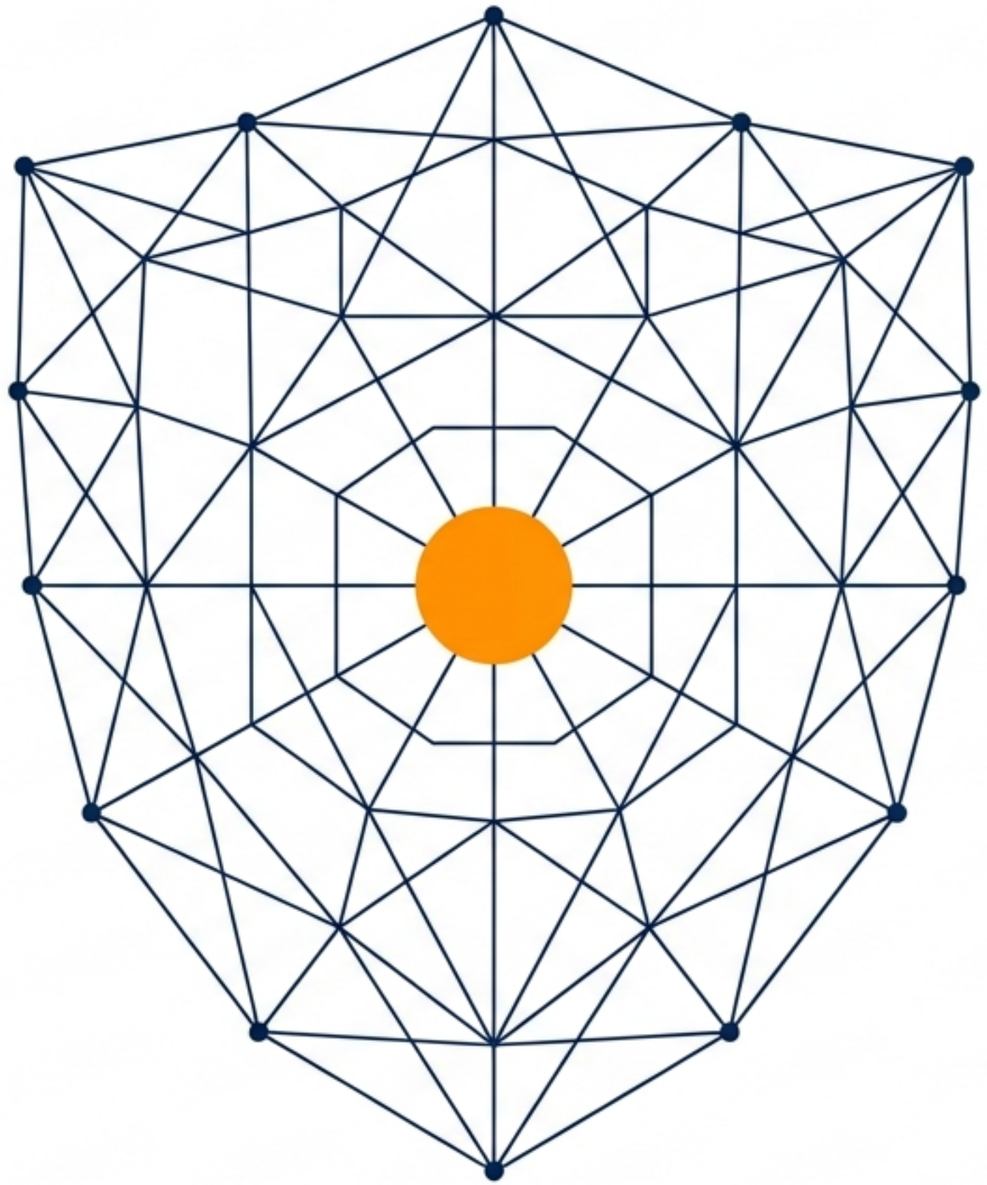
O Escudo Digital

A evolução dos golpes de WhatsApp, a anatomia do hackeamento humano e o framework tático de defesa.

Instituto para Valorização da Educação e da Pesquisa no Estado de São Paulo (IVEPESP)



O alvo deixou de ser o seu dispositivo. O alvo é a sua mente.

Nos últimos anos, a **natureza do cibercrime mudou**. O criminoso contemporâneo não escreve códigos complexos para invadir seu aparelho; ele utiliza engenharia social e **manipulação** psicológica para **induzir** decisões precipitadas.

O Passado:
Hardware e Software

Vínculos Afetivos
(Confiança familiar)

Sensação de Urgência
(Pressão de tempo)

Autoridade Falsa
(Instituições ou gerentes falsos)

O problema deixou de ser apenas tecnológico e passou a ser educacional, cultural e institucional.

Matriz de Ameaças: O Arsenal da Extorsão Digital

Uma taxonomia dos 8 golpes mais utilizados atualmente nas plataformas de comunicação instantânea.

Falsificação de Identidade

- Criação de números falsos com fotos reais de familiares.
- Mensagens clássicas de ‘Mudei de número’.

Manipulação Financeira

- Pedidos urgentes de PIX sob pretexto de emergência.
- Golpes envolvendo falsas centrais bancárias.

Sequestro Técnico

- Clonagem direta de contas de WhatsApp.
- Clonagem direta de contas de WhatsApp.
- Solicitações enganosas de códigos de SMS.

A Nova Fronteira (IA)

- Invasão profunda via engenharia social avançada.
- Uso de voz sintética para simular familiares em tempo real.

A Anatomia do Sequestro da Confiança

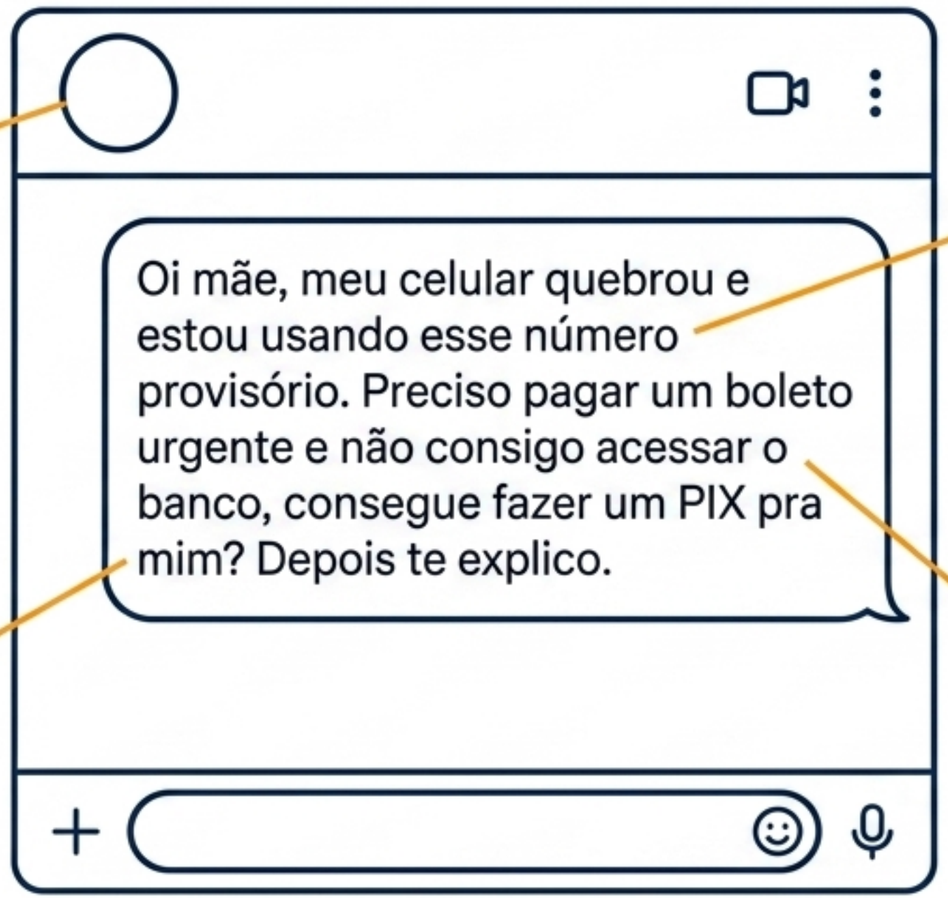
Como os criminosos estruturam uma mensagem para desativar seu pensamento crítico.

Isla de Confiança

Uso de foto real roubada das redes sociais para baixar a guarda da vítima.

O Álibi

Justificativa crível para o número desconhecido e para a impossibilidade de receber ligações.



Evasão

Bloqueio de qualquer tentativa de questionamento lógico imediato.

Gatilho de Pressão

Criação de pânico para forçar uma ação rápida sem verificação.

O Multiplicador de Risco: O Fator Inteligência Artificial

O avanço da IA torna obsoleta a antiga crença de que "se for golpe, dará para perceber pela escrita". A falsificação agora é multissensorial.

Golpe Tradicional	Ameaça Potencializada por IA
• **Formato:** Mensagens de texto impessoais ou com erros gramaticais.	• **Voz:** Clonagem de voz exata a partir de áudios curtos de redes sociais.
• **Limitação:** Dificuldade em manter conversas longas ou naturais.	• **Visual:** Geração de imagens falsas contextualizadas (Deepfakes).
• **Evidência:** Uso apenas de fotos estáticas roubadas.	• **Interação:** Mensagens altamente convincentes e simulação perfeita de linguagem.

Isso torna indispensável uma nova cultura de desconfiança saudável e verificação multifator.

Manual Tático de Defesa IVEPESP

9 orientações fundamentais organizadas em um framework de 3 camadas de proteção.

Camada 1: Verificação Comportamental

O Filtro Humano

Focado na atitude do usuário perante a ameaça.

Camada 2: Blindagem Tecnológica

A Barreira de Software

Focado na configuração correta do aplicativo e do aparelho.

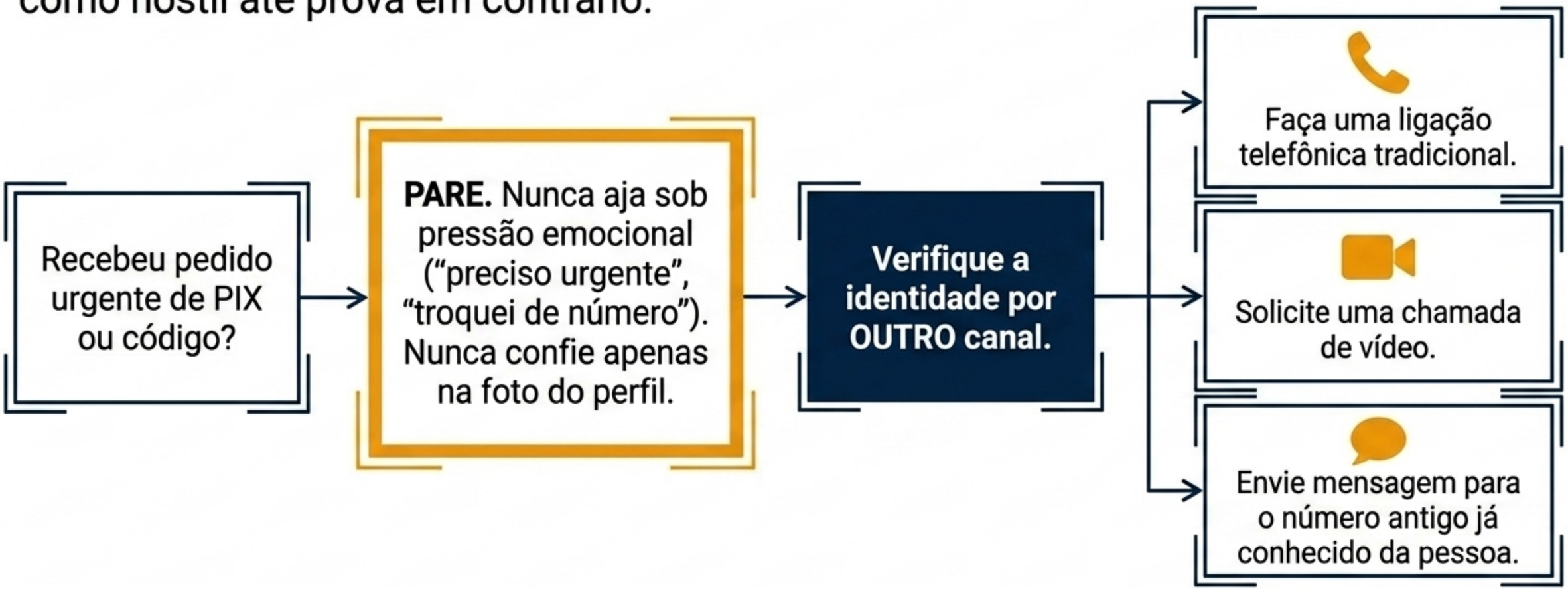
Camada 3: Reação Pós-Incidente

O Protocolo de Crise

Focado na contenção de danos se o golpe for consumado.

Pilar 1: Verificação Comportamental

Interrompa a urgência. Toda solicitação financeira sob pressão deve ser tratada como hostil até prova em contrário.



A verificação deve ser sempre independente da plataforma onde a mensagem chegou.

Pilar 2: Blindagem Tecnológica

Configure barreiras de segurança para impedir a tomada de controle da sua conta.

Nunca envie códigos de SMS. Criminosos usam isso para sequestrar sua conta. Nenhuma empresa séria pede este código por mensagem.

Ação A: Ativar Duas Etapas

Configurações -> Conta -> Confirmação em duas etapas

(Mecanismo vital que reduz invasões drasticamente)

Ação B: Limpar Dispositivos

Configurações -> Aparelhos conectados

(Remova sessões desconhecidas imediatamente)

Pilar 3: Reação Pós-Incidente (Protocolo de Crise)

Em caso de tentativa de golpe ou fraude financeira consumada, a agilidade na documentação é crucial para acionar autoridades.

1

1. Isolar a Ameaça

- Bloquear o contato no aplicativo.
- Denunciar o perfil na plataforma.
- **Nota:** Não apague a conversa antes do passo 2.

2

2. Preservar a Cena

- Salvar capturas de tela (prints) da conversa.
- Registrar números de telefone, horários e contas bancárias fornecidas pelo golpista.

3

3. Acionar a Defesa Institucional

- Registrar Boletim de Ocorrência (B.O.).
- Comunicar imediatamente o banco para solicitar mecanismos de reversão do PIX.

O Elo Mais Importante: O Fator Humano

O melhor antivírus é o diálogo contínuo dentro das famílias.

Grande parte das vítimas pertence a grupos com menor familiaridade digital. A proteção exige um esforço coletivo e paciência.

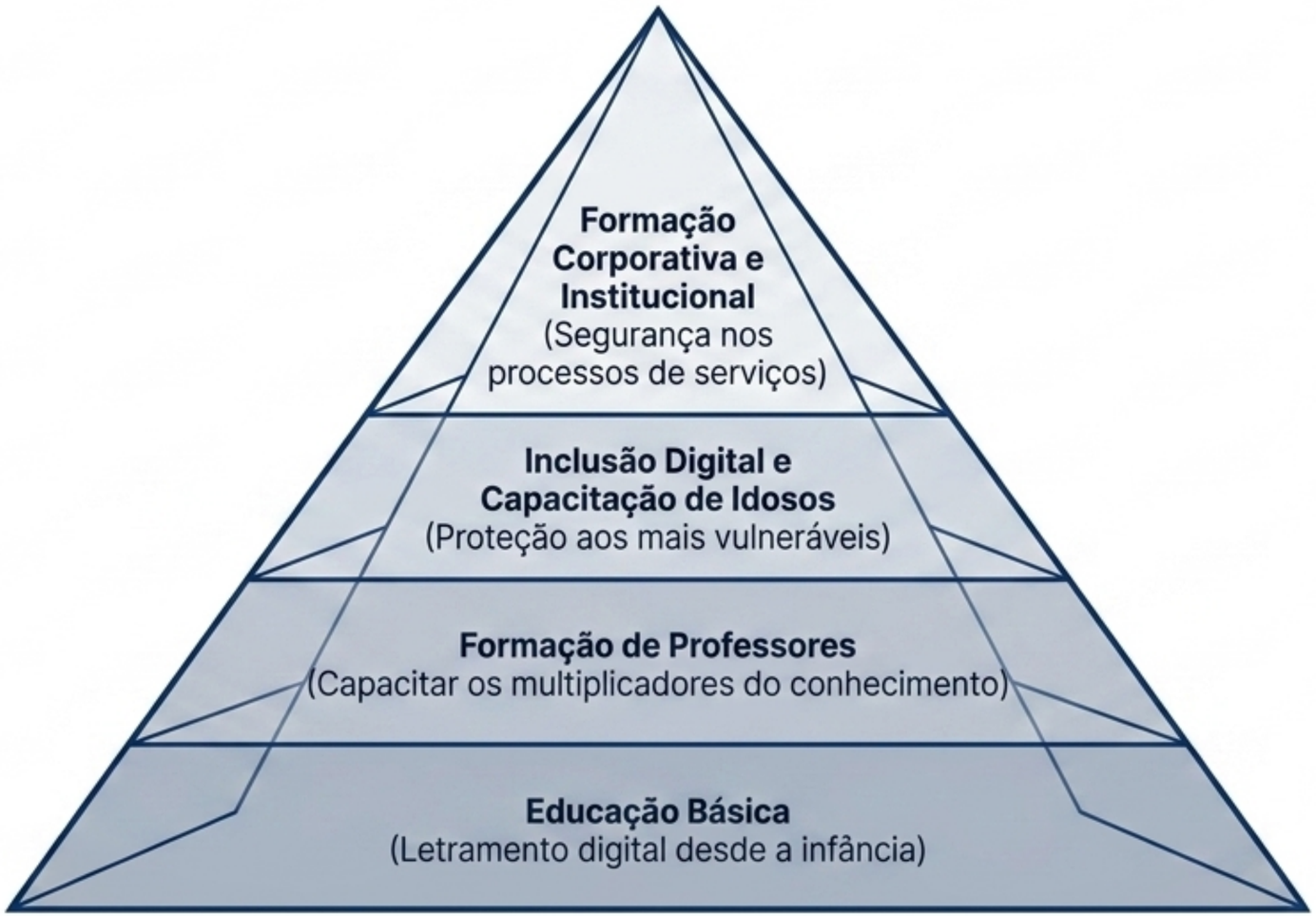
Ação Recomendada:

- **Compartilhe** estas **orientações** de forma **didática** com familiares e idosos.

- Estabeleça uma "**palavra-senha**" **familiar** para uso em caso de **emergências reais**, garantindo autenticidade quando não houver vídeo.

A Visão do IVEPESP: Segurança Digital como Política Pública

O combate aos golpes não depende apenas da tecnologia, mas da construção de uma sociedade estruturalmente preparada e letrada.



Protegendo a Sociedade Contemporânea

> **A proteção da confiança social tornou-se um dos grandes desafios da era digital.**
>
> **— Prof. Dr. Helio Dias, Presidente do IVEPESP.**

IVEPESP - Instituto para Valorização da Educação e da Pesquisa no Estado de São Paulo

Entidade de Utilidade Pública.

Contato:
contato@ivepesp.org.br
(11) 99699-4434

Apoie nossos projetos (Doe via PIX):
CNPJ 15.151.763/0001-00