GUIA PRÁTICO DE DEFESA DIGITAL

ESCUDO DIGITAL: PIX, WHATSAPP & RASTREAMENTO OCULTO

Manual de proteção comunitária contra golpes de engenharia social, fraudes bancárias e a ameaça invisível dos pixels espiões em e-mails.

DISTRIBUIÇÃO LIVRE | ODS 10: REDUÇÃO DAS DESIGUALDADES | ODS 16: PAZ E INSTITUIÇÕES EFICAZES

ESTRUTURA DA CARTILHA

O que você vai aprender a desarmar

Desenvolvida para idosos, famílias e pequenos comerciantes, esta cartilha reúne as principais táticas de engenharia social e fornece proteções imediatas no celular.

PÁG. 03 // O Golpe do WhatsApp

Como golpistas usam sua foto com números falsos e como ativar o PIN obrigatório.

PÁG. 04 // Pix e Falsa Central

A farsa do 0800, falso gerente bancário e como funciona a devolução oficial (MED).

PÁG. 05 // O Pixel Espião no E-mail

A imagem oculta de 1x1 pixel que avisa quando você abriu a mensagem e revela seu IP.

PÁG. 06 // Passo a Passo: Bloquear Pixels

Desative o carregamento de imagens no Gmail, Outlook e Apple Mail em 3 cliques.

PÁG. 07 // Senhas e Autenticação Forte

Por que senhas repetidas caem em vazamentos e como usar autenticadores.

PÁG. 08 // Checklist dos 10 Mandamentos

Tabela de consulta rápida para colar na geladeira ou deixar ao lado do computador.

PÁG. 09 // Roteiro de Emergência: Caí no Golpe

O que fazer nos primeiros 30 minutos: B.O. online, bloqueio MED e contestação.

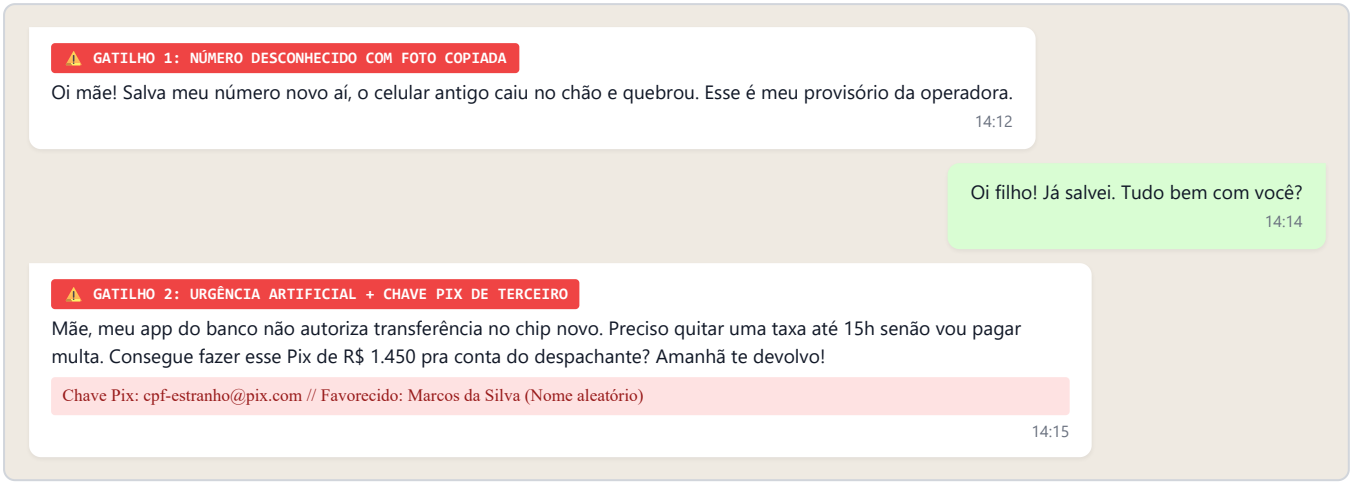
PÁG. 10 // Fontes & Links Clicáveis

Contatos oficiais de delegacias cibernéticas, BCB, CERT.br e Febraban Antifraudes.

AMEAÇA COMUM

O Golpe do "Novo Número" e Roubo de Conta

O WhatsApp é o canal mais explorado no Brasil para extorquir idosos fingindo ser filhos ou parentes pedindo dinheiro urgente.



BLINDAGEM EM 3 PASSOS

1. **Ative o PIN de 6 Dígitos:** Vá em *Configurações* > *Conta* > *Confirmação em duas etapas*. Crie uma senha de 6 números que só você sabe. Sem ela, ninguém rouba sua conta mesmo clonando o chip.
2. **Oculte sua foto de perfil para desconhecidos:** Vá em *Configurações* > *Privacidade* > *Foto de perfil* e marque **"Meus contatos"**. Isso impede que estranhos baixem sua foto.
3. **Regra de Ouro da Chamada de Voz:** Se qualquer parente pedir dinheiro por mensagem escrita, **ligue para o número antigo por chamada normal ou de vídeo** antes de fazer qualquer transferência.

GOLPE DE ALTO VALOR

A Farsa da Falsa Central e Falso Gerente

A Febraban alerta: mais de 70% dos golpes bancários modernos não exploram falhas no sistema bancário, mas sim a ingenuidade da vítima via telefone.

O Roteiro Teatral do Golpe:

Você recebe ligação de um suposto "0800" ou SMS alertando que houve uma compra suspeita de R$ 3.800 nas Casas Bahia. Para cancelar, pedem que você ligue no número indicado ou transfira o dinheiro para uma "conta de segurança protegida".

FATOS INVIOLÁVEIS DO BANCO CENTRAL

1. O Banco NUNCA pede transferências para cancelar fraudes:

Não existe "conta cofre", "chave Pix temporária de segurança" ou "estorno por envio". Todo estorno é feito diretamente pelo sistema interno do banco.

2. O Banco NUNCA pede instalação de aplicativos de suporte:

Desconfie na hora se o atendente pedir para baixar apps como AnyDesk, TeamViewer ou QuickSupport. Esses apps entregam controle remoto do seu aparelho.

3. O Mecanismo Especial de Devolução (MED):

Se caiu num golpe Pix, acione o banco da sua conta em até 80 dias solicitando o MED pelo aplicativo. O banco bloqueia os fundos na conta destino imediatamente para análise.

VULNERABILIDADE TÉCNICA

A Imagem Invisível: O que é o Pixel Espião?

Muitos e-mails parecem simples mensagens de texto, mas escondem um rastreador em miniatura criado para espionar seus hábitos sem autorização.

O QUE FICA ESCONDIDO NO CÓDIGO HTML DO E-MAIL FALSO:

```
<p>Prezado cliente, seu acesso expira hoje. Regularize.</p>
<img src="https://servidor-criminoso.com/beacon.png?alvo=usuario&id=892" width="1" height="1" style="display:none;" />
```

Como funciona o Web Beacon / Spy Pixel:

Trata-se de uma imagem transparente de apenas **1 pixel de largura por 1 pixel de altura** inserida no código HTML da mensagem. Quando seu aplicativo de e-mail abre a mensagem, ele baixa essa imagem do servidor do remetente. Nesse milissegundo, seu aparelho entrega de bandeja:

- O momento exato em que você abriu a mensagem e quantas vezes releu.
- Seu **endereço de IP real**, revelando cidade, bairro e provedor de internet.
- O modelo do seu celular, computador e sistema operacional.

O perigo nos golpes bancários:

O golpista envia um falso alerta de cobrança com pixel espião. Quando você abre, o painel do criminoso acende avisando que você está online lendo. Poucos minutos depois, seu celular toca com a Falsa Central, simulando urgência máxima!

AÇÃO DEFENSIVA IMEDIATA

Como Desativar Imagens Automáticas no E-mail

Ao impedir que imagens sejam baixadas automaticamente, o pixel espião é neutralizado e não consegue transmitir seus dados ao servidor externo.

No GMAIL (Computador e Celular):

1. Abra as **Configurações** (ícone de engrenagem) > *Ver todas as configurações*.
2. Na aba **Geral**, role até a seção **Imagens**.
3. Marque: **"Perguntar antes de exibir imagens externas"**.

Resultado: O Gmail só exibirá imagens se você clicar manualmente em "Exibir imagens".

No MICROSOFT OUTLOOK:

1. Vá em **Arquivo** > **Opções** > **Central de Confiabilidade**.
2. Clique em **Configurações da Central de Confiabilidade** > **Download Automático**.
3. Marque a caixa: **"Não baixar imagens automaticamente em emails HTML padrão"**.

No APPLE MAIL (iPhone / Mac):

1. No iPhone, vá em **Ajustes** > **Mail** > **Proteção de Privacidade**.
2. Ative a opção **"Proteger Atividade do Mail"** (oculta seu IP e bloqueia rastreadores em segundo plano).

SEGURANÇA ESTRUTURAL

O Fim das Senhas Fáceis e Repetidas

Mais de 80% das invasões de contas acontecem porque as pessoas usam a mesma senha na farmácia, na rede social e no aplicativo bancário.

ERROS FATAIS QUE VOCÊ DEVE PARAR:

- Usar data de nascimento, nome de filhos ou placa do carro.
- Usar senhas clássicas como *123456*, *mudar123* ou *senha@2024*.
- Anotar senhas no bloco de notas do celular ou em papéis expostos.
- Reutilizar a mesma senha em múltiplos serviços online.

BOAS PRÁTICAS RECOMENDADAS:

- Use frases longas fáceis de lembrar: *CafeComPao!NaPracinha2026*.
- Ative autenticador gratuito (Google Authenticator ou Microsoft Authenticator).
- Cadastre biometria facial/digital apenas nos apps oficiais do banco.
- Consulte se seu e-mail vazou em *haveibeenpwned.com*.

Atenção ao SMS de Recuperação:

Evite receber código de segurança por SMS comum quando houver opção por aplicativo autenticador. Criminosos podem aplicar o golpe do "SIM Swap" (clonagem do chip telefônico) na operadora para interceptar seus códigos bancários por SMS.

RECORTE E GUARDE

Os 10 Mandamentos da Proteção Digital

Regras de ouro para compartilhar no grupo da família e consultar antes de clicar em qualquer link suspeito.

[01] O BANCO NÃO LIGA PEDINDO PIX: Nenhuma instituição financeira solicita transferências para "proteger conta".

[02] CUIDADO COM A URGÊNCIA ARTIFICIAL: Golpistas criam pânico e desespero para que você aja sem pensar. Respire e desligue.

[03] BLOQUEIE IMAGENS AUTOMÁTICAS: Desative a exibição no e-mail para desarmar pixels espiões e rastreadores.

[04] CONFIRME POR VOZ ANTES DE TRANSFERIR: Parente pediu dinheiro no WhatsApp novo? Ligue no número antigo antes.

[05] ATIVE O PIN DE 6 DÍGITOS NO WHATSAPP: Vá em Conta > Confirmação em duas etapas agora mesmo.

[06] NUNCA INSTALE PROGRAMAS A PEDIDO DE ATENDENTES: AnyDesk e TeamViewer dão controle total do seu celular a terceiros.

[07] VERIFIQUE O DESTINATÁRIO DO PIX: Confira o nome e o CPF/CNPJ de quem vai receber na tela de confirmação antes de digitar a senha.

[08] CUIDADO COM LINKS DE ENCOMENDAS E CORREIOS: Golpistas enviam SMS sobre falsas taxas alfandegárias para roubar dados de cartão.

[09] LIMITE DIÁRIO DE PIX NOTURNO: Ajuste pelo aplicativo do seu banco um teto baixo para transferências entre 20h e 06h.

[10] EM CASO DE GOLPE, ACIONE O MED IMEDIATAMENTE: Notifique o banco nos primeiros minutos para bloquear a conta destino.

PRIMEIROS SOCORROS DIGITAIS

Caí no Golpe: O que Fazer nos Primeiros 30 Minutos

A agilidade nas primeiras horas é o único fator determinante para conseguir recuperar valores e limitar danos jurídicos.

1º **Ligue Imediatamente para o SAC Oficial do seu Banco:**
Use o telefone que está **atrás do seu cartão de crédito físico**. Informe que foi vítima de golpe e solicite a abertura imediata de contestação via **MED (Mecanismo Especial de Devolução do Pix)**. Anote o número de protocolo.

2º **Registre o Boletim de Ocorrência (B.O.) Online:**
Acesse a Delegacia Eletrônica da Polícia Civil do seu Estado. Registre a ocorrência categorizando como *Estelionato por Meio Eletrônico (Art. 171 do Código Penal)*. Anexe os comprovantes de transferência, chave Pix, números de telefone usados pelos criminosos e prints das conversas.

3º **Desconecte Aparelhos e Troque Senhas em Outro Aparelho:**
Se instalou aplicativos suspeitos a mando de criminosos, coloque o celular em Modo Avião ou desligue o Wi-Fi imediatamente. Pegue outro computador ou aparelho seguro e altere as senhas dos seus e-mails e contas bancárias.

4º **Avise a Família e Grupos Próximos:**
Se clonaram seu WhatsApp ou estão usando sua foto em outro número, alerte seus contatos por ligações telefônicas ou perfis de redes sociais para que ninguém faça transferências em seu nome.

CANAIS OFICIAIS E VALIDADOS

Links Clicáveis & Suporte ao Cidadão

Acesse as instituições oficiais para formalizar queixas, consultar direitos e aprofundar seu conhecimento em segurança digital.

[REF_01] **FEBRABAN Antifraudes — Federação Brasileira de Bancos**
antifraudes.febraban.org.br // Orientações contra golpes da falsa central e Pix ↗

[REF_02] **CERT.br / NIC.br — Cartilha de Segurança para a Internet**
cartilha.cert.br // Manuais de privacidade, engenharia social e defesa de redes ↗

[REF_03] **Banco Central do Brasil — Mecanismo Especial de Devolução (MED)**
bcb.gov.br/estabilidadefinanceira/medpix // Regras de contestação e bloqueio de valores ↗

[REF_04] **Delegacia Eletrônica da Polícia Civil (Estelionato Eletrônico)**
policiacivil.sp.gov.br // Registro de Boletim de Ocorrência online ↗

[REF_05] **Have I Been Pwned? — Verificação de Vazamento de Credenciais**
haveibeenpwned.com // Auditoria global de e-mails comprometidos em breaches ↗