Guia de Prevenção, Identificação e Recuperação de Golpes no WhatsApp

CRESOL

Introdução

O WhatsApp faz parte da rotina de milhões de brasileiros, facilitando a comunicação entre pessoas, empresas e instituições. No entanto, a popularidade da plataforma também a torna um dos principais alvos de golpistas, que utilizam diferentes estratégias para obter dados pessoais, acessar contas ou induzir vítimas a realizar transferências financeiras.

Por isso, estar informado é o primeiro passo para se proteger. Neste guia, você encontrará informações sobre os golpes mais comuns praticados no WhatsApp, os recursos de segurança disponíveis no aplicativo, boas práticas de prevenção e orientações sobre como agir e reportar situações suspeitas. Com atenção e conhecimento, é possível reduzir riscos e utilizar o aplicativo de forma mais segura no dia a dia.

Principais Golpes no WhatsApp

O WhatsApp é uma rede de comunicação muito acessível e amplamente utilizada, o que faz com que criminosos a utilizem para aplicar diversos tipos de golpes.
Abaixo estão descritos os golpes mais comuns via WhatsApp e as consequências associadas para as vítimas:

1. Conta Hackeada (Perda de Acesso)

- Quando um criminoso registra o número da vítima em outro aparelho, geralmente após roubar o código de 6 dígitos enviado por SMS (Token de Ativação) ou enganar a vítima para que ela compartilhe esse código.

- **Consequências para a Vítima:**
  - **Perda Imediata de Acesso:** A vítima é deslogada do próprio aplicativo.
  - **Fraude Financeira:** O invasor pode se passar pela vítima para solicitar transferências (PIX) a amigos e familiares.
  - **Bloqueio de 7 Dias:** Se o invasor for rápido e ativar o PIN de Verificação em Duas Etapas, a vítima pode ficar bloqueada da conta por 7 dias (até a redefinição pelo WhatsApp).

2. Perfil Fake (Impostor)

- Quando o criminoso **utiliza** um **número diferente** do da vítima, mas usa a **foto de perfil** e o **nome da vítima** para contatar os amigos e solicitar dinheiro ou favores urgentes.

- **Consequências para a Vítima:**
  - **Tentativa de Estelionato:** O golpe é aplicado contra os contatos, mas a vítima 'original' sofre o dano reputacional e o estresse de ter sua identidade usada em fraudes.
  - **Dano Reputacional:** Contatos podem acreditar que a vítima está envolvida no golpe.

3. Sequestro via QR Code (WhatsApp Web)

- Ocorre quando a vítima é induzida a escanear um QR Code malicioso que, secretamente, conecta a conta a uma sessão do WhatsApp Web controlada pelo criminoso.

- **Consequências para a Vítima:**

  - **Acesso Indevido:** O criminoso tem acesso em tempo real a todas as mensagens enviadas e recebidas e pode enviar mensagens fraudulentas em nome da vítima.
  - **Roubo de Dados:** Vazamento de conversas privadas e mídias.

4. Engenharia Social (Promoções Falsas)

- Método pelo qual o criminoso manipula a vítima para que ela realize uma ação que comprometa sua segurança (geralmente entregar o código SMS), sob falsos pretextos como vagas de emprego, sorteios, acesso a processos, documentos, fotos ou benefícios.

- **Consequências para a Vítima:**

  - **Roubo da Conta:** A vítima perde o acesso, e o invasor pode iniciar fraudes financeiras e extorsão.
  - **Ativação do PIN de Segurança:** O invasor pode ativar o PIN de Verificação em Duas Etapas, dificultando a recuperação da conta.

5. Extorsão e Risco de Vazamento

- Quando o criminoso invade a conta, extrai mídias privadas (fotos, vídeos, dados) e, em seguida, usa essas informações para chantagear a vítima, exigindo dinheiro para não vazar o material.

- **Consequências para a Vítima:**

  - **Extorsão Financeira:** Perda de dinheiro por pressão. O pagamento não garante que os dados não serão vazados.
  - **Vazamento de Dados Privados:** Exposição de informações e mídias sensíveis.
  - **Necessidade de Ação Policial:** É um crime crítico que exige registro de Boletim de Ocorrência e contato policial especializado em crimes cibernéticos.

6. Sequestro de Grupo (Comunidades)

- Ocorre quando o administrador de um grupo ou comunidade é hackeado. O invasor aproveita a conta do administrador para remover outros administradores e disparar links maliciosos (phishing) ou conteúdo fraudulento para todos os membros.

- **Consequências para a Vítima:**

  - **Perda de Controle:** Perda do controle sobre o próprio grupo.
  - **Risco a Terceiros:** A vítima é o vetor do ataque, expondo todos os membros do grupo/comunidade a riscos de phishing e fraude.

7. Sequestro de Linha (SIM Swap)

- É um ataque mais sofisticado onde o criminoso consegue se passar pela vítima junto à operadora de telefonia (Vivo, Claro, Tim, etc.) e solicitar a portabilidade ou a emissão de um novo chip (SIM card) para o número da vítima. A linha original é desativada ("Sem Serviço").

- **Consequências para a Vítima:**

  - **Perda Total de Controle:** O criminoso assume a linha telefônica, tendo acesso ao WhatsApp e a todos os serviços digitais (bancos, e-mails, redes sociais) vinculados ao número, pois ele receberá todos os códigos SMS de autenticação.
  - **Risco de Roubo de Identidade e Financeiro Extremo:** Acesso a contas bancárias, abertura de empréstimos e outros crimes em nome da vítima.

8. Suporte Falso (Phishing Interno)

- Quando uma conta comercial ou perfil com o logotipo do WhatsApp se passa pelo "Suporte Oficial" e entra em contato via chat, solicitando dados pessoais, códigos de segurança ou o PIN da verificação em Duas Etapas.

- **Consequências para a Vítima:**

  - **Roubo de Conta:** Se a vítima fornecer o código SMS ou o PIN, o criminoso obtém o controle da conta.
  - **Roubo de Dados:** Fornecimento de dados pessoais sob falso pretexto.

Ataque de Spyware (Monitoramento)

- Quando o celular da vítima foi comprometido por um software espião (stalkerware) que permite ao invasor monitorar as atividades do dispositivo e, consequentemente, ler as mensagens do WhatsApp em tempo real.

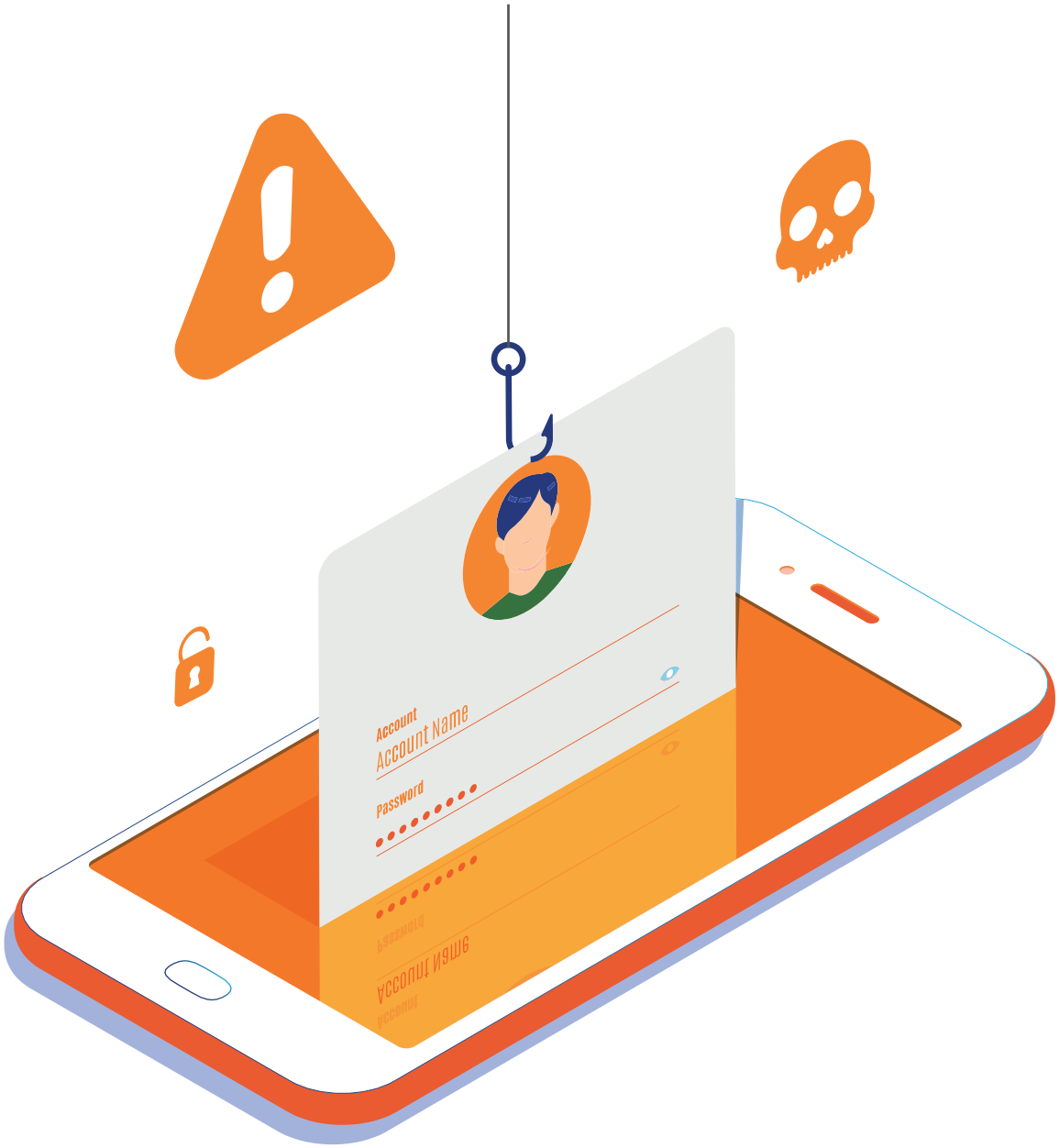
- **Consequências para a Vítima:**

  - **Violação de Privacidade Extrema:** As mensagens e outras atividades no celular (como e-mails, localização, uso de microfone) estão sendo lidas pelo criminoso.
  - **Instabilidade do Dispositivo:** O celular pode apresentar lentidão ou drenagem rápida de bateria e superaquecimento.
  - **Risco a Dados:** Comprometimento da segurança geral do dispositivo. A única forma segura de remover é a restauração do celular para as configurações de fábrica (reset total).

Protocolo de Segurança para WhatsApp

Guia Completo de Prevenção e Recuperação

Saiba como prevenir ataques, identificar comprometimentos e recuperar o controle da sua conta de WhatsApp, minimizando danos financeiros e reputacionais.



1. Prevenção:

O que você deve fazer ***AGORA***, *para impedir que um golpe ou ataque aconteça:*

Ativar a Verificação em Duas Etapas (PIN):

- *O que é:* Uma senha de 6 dígitos que o WhatsApp pede periodicamente e sempre que o número é registrado em um novo aparelho. É a sua maior barreira contra roubo de conta.
- Como fazer: Configurações > Conta > Confirmação em duas etapas > Ativar.
- ⚠️ Crítico: Nunca esqueça este PIN e adicione um e-mail de recuperação seguro.

Privacidade de Foto e Dados:

- Configure quem pode ver sua foto de perfil, "Visto por último" e "Recado". Restrinja para "Meus contatos" para evitar que golpistas usem sua foto em perfis falsos.
- *Como fazer:* Configurações > Privacidade>

A Regra de Ouro do Código SMS:

- **JAMAIS** compartilhe o código de 6 dígitos enviado por SMS pelo WhatsApp. Nenhuma empresa, organizador de sorteio ou suporte técnico legítimo pedirá esse código. Se pedirem, é golpe.

Biometria/Bloqueio de Tela no App:

- Adicione uma camada extra exigindo Face ID ou digital para abrir o WhatsApp.
- Como fazer: Configurações > Privacidade > Bloqueio de tela.

Quando se logar no WhatsApp Web, no computador de terceiros, lembre-se de deslogar e apagar o registro ao sair.

2. Detecção (Sinais de Alerta)

Como saber se você está sendo atacado ou já foi comprometido.

- **Deslogamento Súbito:** Você recebe uma mensagem "Seu número de telefone não está mais registrado neste aparelho". Isso significa que alguém registrou seu número em outro lugar.

- **SMS de Código não solicitado:** Você recebe vários SMS com códigos do WhatsApp sem estar tentando instalar o app. Alguém está tentando forçar a entrada.

- **Atividade Estranha no WhatsApp Web:** Mensagens que você não enviou aparecem nas conversas, ou contatos dizem que você está online em horários estranhos.

- **Celular "Sem Serviço":** Seu sinal de operadora some completamente por muito tempo, enquanto o Wi-Fi funciona.

- **Notificações de Segurança:** Seus contatos recebem avisos de que "O código de segurança de [Seu Nome] mudou".

- **Drenagem de Bateria/Lentidão:** O aparelho esquenta muito e a bateria acaba rápido sem uso intenso, indicando software espião em segundo plano.

3. Resposta Imediata (Protocolo de Emergência)

Ações a serem tomadas nos primeiros minutos após confirmar um ataque.

Se você ainda tem acesso ao seu celular (mesmo que o WhatsApp tenha caído):

1. **Tente Reassumir o Controle:**
   - Abra o WhatsApp imediatamente.
   - Insira seu número de telefone para verificar novamente.
   - Se você for rápido o suficiente, o código SMS chegará ao seu celular e você desconectará o invasor.
   - **Se pedir o PIN de duas etapas e você não souber (o invasor ativou):** Você terá que aguardar 7 dias para redefinir sem o PIN, mas enquanto isso, o invasor também fica bloqueado se não souber o PIN.

2. **Expulse Invasores do WhatsApp Web:**
   - Se você ainda consegue entrar no app: Vá para Configurações > Aparelhos Conectados.
   - Clique em **"Desconectar de todos os aparelhos"** imediatamente. Isso encerra acessos via QR Code.

3. **Contenção de Danos (Aviso aos Navegantes):**
   - Use Instagram Stories, Facebook, Status de familiares ou ligação telefônica para avisar contatos-chave: *"Meu WhatsApp foi hackeado. Não transfiram dinheiro nem cliquem em links enviados por mim."*

4. Ações Técnicas por Cenário Específico

O que fazer tecnicamente além de enviar o e-mail de suporte.

Utilize o formulário de reporte oficial do WhatsApp, conforme instruções no item *Como reportar golpes no WhatsApp* , e execute as seguintes ações em paralelo:

Conta Hackeada / Engenharia Social (Perda de Acesso)

- **Ação Técnica:** Tente reinstalar o WhatsApp e verificar seu número repetidamente. Isso força o sistema a enviar novos SMS para você e desloga o invasor.
- **Se o invasor ativou o PIN:** O WhatsApp mostrará uma tela pedindo o PIN. Clique em "Esqueci o PIN" > Enviar e-mail. Se o invasor não tiver acesso ao seu e-mail, ele não conseguirá resetar. Após 7 dias sem o PIN correto, o WhatsApp permite redefinir a conta (apagando as mensagens, mas recuperando o número).

Perfil Fake (Impostor com outro número)

- **Ação Técnica:** Não adianta contactar o suporte do WhatsApp por e-mail para bloquear um número que não é seu.
- Você e seus amigos devem abrir o perfil do impostor no WhatsApp > Tocar no nome/número > Rolar para baixo > **Denunciar empresa/contato**. Peça para pelo menos 5 pessoas denunciarem para agilizar o bloqueio algorítmico.

Sequestro via QR Code (WhatsApp Web)

- **Ação Técnica:** Como mencionado na Fase 3, vá em "Aparelhos Conectados" e desconecte tudo. Se não reconhecer um navegador (ex: Linux, Chrome em local estranho), é o invasor.

Extorsão e Risco de Vazamento

- **Ação Crítica: Não pague!** O pagamento não garante que os dados não serão vazados e financia o crime.
- Documente tudo (prints das ameaças).
- Vá imediatamente à polícia especializada em crimes cibernéticos.
- Envie o e-mail para o WhatsApp com o assunto "CRÍTICO: Extorsão" solicitando a suspensão imediata da conta para congelar as ações do criminoso.

SIM Swap (Sequestro de Linha na Operadora)

- **Ação Prioritária:** O problema não é no WhatsApp, é na sua operadora (Vivo, Claro, Tim).
- Ligue de outro telefone para a operadora imediatamente, informe que foi vítima de SIM Swap e solicite o bloqueio imediato da linha telefônica (do chip).
- Somente após recuperar o controle do seu número com a operadora é que você deve tentar reinstalar o WhatsApp.

Suspeita de Spyware (Stalkerware)

- **Ação Técnica:** O problema está no sistema operacional do celular, não só no WhatsApp.
- Faça backup das fotos e contatos (fora do celular).
- A única forma 100% segura de remover spyware é r**estaurar o celular para as configurações de fábrica** (reset total).

5. Recuperação e Pós-Incidente

O checklist definitivo depois que a poeira baixar.

Não basta recuperar o WhatsApp. Você precisa garantir que o resto da sua vida digital está seguro e lidar com as consequências legais.

1. **Documentação Legal (Essencial se houve pedido de dinheiro):**
   - Vá a uma delegacia (ou delegacia virtual) e registre um **Boletim de Ocorrência (B.O.).** Tipifique como "Invasão de dispositivo informático" (Lei Carolina Dieckmann) e, se houve tentativa de golpe, "Estelionato". Leve prints e o número do protocolo de atendimento da operadora (se houver).

2. **Proteção Financeira:**
   - Se você tinha cartões cadastrados no WhatsApp Pay ou se dados bancários foram trocados em conversas recentes, avise seu banco preventivamente.
   - Monitore seu CPF no "Registrato" do Banco Central para ver se abriram contas ou pediram empréstimos em seu nome.

3. **Fortalecimento de Contas Vinculadas:**
   - O invasor pode ter acessado seu e-mail para tentar interceptar links de redefinição. **Mude a senha do seu e-mail principal imediatamente.**
   - Ative a verificação em duas etapas também no seu e-mail e redes sociais (Instagram, Facebook, Google).

4. **Varredura de Higiene Digital:**
   - Passe um antivírus confiável no seu celular.
   - Revise quais aplicativos têm permissão para acessar seus contatos e SMS.

Como reportar golpes no WhatsApp

Como reportar esse tipo de golpe?

Todo incidente deve ser reportado através do formulário oficial, no site ou configurações do WhatsApp.

Para preencher a solicitação, escolha o cenário que melhor descreve o seu problema e preencha as informações entre colchetes.

Cenário 1: Conta Hackeada (Perda de Acesso)
Uso: *Quando você foi deslogado e não consegue retomar o acesso.*

Assunto: INCIDENTE: Conta Hackeada - Solicitação de Bloqueio/Recuperação

- **Número da vítima:** +55 [DDD] [Número]
- **Data do incidente:** [DD/MM/AAAA]
- **Circunstâncias:** Recebi um código por SMS e a conta foi deslogada / A verificação em duas etapas foi alterada por terceiros.
- **Titular:** [Nome Completo]
- **E-mail:** [Seu e-mail]

Cenário 2: Perfil Fake (Impostor)
Uso: *Alguém usa sua foto e nome em outro número para pedir dinheiro.*

Assunto: FRAUDE: Conta Fraudulenta - Personificação (Fake)

- **Número do FRAUDADOR:** +55 [DDD] [Número do Golpista]
- **Número REAL da vítima:** +55 [DDD] [Seu Número]
- **Circunstâncias:** O criminoso está usando minha identidade visual para solicitar transferências financeiras (PIX) aos meus contatos.

Cenário 3: Sequestro via QR Code (WhatsApp Web)
Uso: *Quando há acessos estranhos ou mensagens enviadas que você não escreveu.*

Assunto: SEGURANÇA: Acesso Indevido via WhatsApp Web/Desktop

Número REAL da vítima: +55 [DDD] [Número]
Circunstâncias: Sessão ativa via QR Code em site malicioso. Há mensagens sendo enviadas sem meu consentimento. Solicito logout remoto de todas as sessões.

Cenário 4: Engenharia Social (Promoções Falsas)
Uso: *Quando você entrega o código SMS acreditando em um sorteio ou vaga de emprego.*

Assunto: FRAUDE: Engenharia Social - Roubo de Token de Ativação

- **Número da vítima:** +55 [DDD] [Número]
- **Data do incidente:** [DD/MM/AAAA]
- **Circunstâncias:** Fui induzido a fornecer o código de verificação sob pretexto de [Descrever o golpe: ex. vaga de emprego]. O invasor ativou o PIN de segurança.

Cenário 5: Extorsão e Risco de Vazamento
Uso: *Quando o invasor ameaça expor fotos ou dados privados.*

Assunto: CRÍTICO: Incidente de Segurança - Extorsão e Vazamento

- **Gravidade:** ALTA / URGENTE
- **Circunstâncias:** Conta invadida. O criminoso está extraindo mídia privada para fins de chantagem e extorsão financeira. Solicito a suspensão imediata da conta.

Cenário 6: Sequestro de Grupo (Comunidades)
Uso: *Quando o administrador é hackeado e o grupo é tomado por golpistas.*

Assunto: SEGURANÇA: Grupo Comprometido - Administrador Hackeado

Nome/ID do Grupo: [Nome do Grupo]
Circunstâncias: O administrador original foi hackeado. O invasor removeu os outros admins e está disparando links maliciosos/phishing para os membros.

Cenário 7: SIM Swap (Sequestro de Linha)
Uso: *Quando seu celular fica "Sem Serviço" e o hacker assume seu número.*

Assunto: CRÍTICO: Comprometimento via SIM Swap (Sequestro de Linha)

- **Circunstâncias:** Minha linha telefônica foi desativada ilegalmente na operadora e o número foi transferido para um chip do criminoso. Ele assumiu o WhatsApp. Já estou em contato com a operadora.

Cenário 8: Suporte Falso (Phishing Interno)
Uso: *Quando um perfil com logo do WhatsApp te pede dados.*

Assunto: DENÚNCIA: Phishing - Personificação do Suporte Oficial

- **Número do Impostor:** +55 [DDD] [Número]
- **Circunstâncias:** Uma conta comercial fingindo ser o "Suporte do WhatsApp" solicitou meus códigos de segurança via chat.

Cenário 9: Suspeita de Spyware (Monitoramento)
Uso: *Quando o celular se comporta estranhamente e parece estar sendo vigiado.*

Assunto: SEGURANÇA: Suspeita de Comprometimento de Dispositivo / Spyware

Circunstâncias: Suspeito que o dispositivo esteja espelhado ou monitorado por software espião. Mensagens estão sendo lidas em tempo real.

Conclusão

A prevenção continua sendo a melhor defesa contra golpes digitais. Manter os recursos de segurança ativados, desconfiar de solicitações incomuns e verificar informações antes de compartilhar dados ou realizar pagamentos são atitudes simples que podem evitar grandes prejuízos.

Sempre que identificar uma tentativa de golpe, denuncie o contato, bloqueie o número e informe os canais oficiais competentes. Ao compartilhar informações e orientar familiares, amigos e colegas, você também contribui para um ambiente digital mais seguro para todos. A segurança é uma responsabilidade compartilhada, e a informação é uma das ferramentas mais eficazes para combater fraudes.

CRESOL