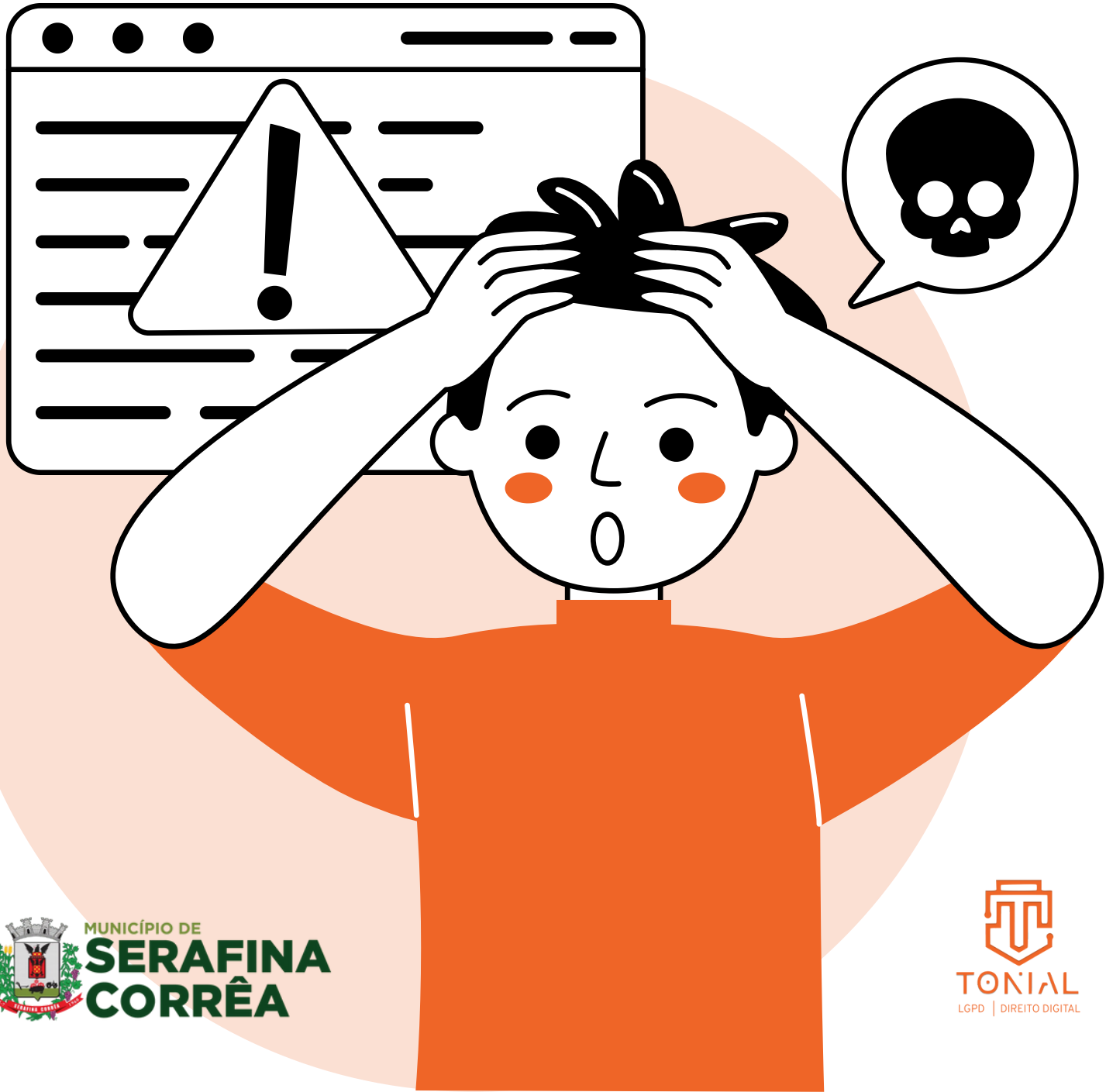
CONTRAGOLPE

Cartilha de Prevenção a Golpes e Fraudes



MUNICÍPIO DE SERAFINA CORRÊA

TONIAL
LGPD | DIREITO DIGITAL

Nome do material:
Cartilha de Prevenção a Golpes e Fraudes

Elaboração:
Tonial Digital – Consultoria em Direito Digital e Proteção de Dados
Em parceria com a Prefeitura Municipal de Serafina Corrêa

Conteúdo elaborado por:

Dra. Maira Tonial – Advogada, Doutora em Direito, Especialista em Direito Digital e Proteção de Dados

Dra. Gabriela Valduga – Advogada, Especialista em Direito Digital e Proteção de Dados

Equipe de apoio:

Equipe Tonial Digital – Pesquisa, Redação e Revisão

Prefeitura Municipal de Serafina Corrêa – Apoio Institucional

Data de publicação:
Setembro de 2025

MUNICÍPIO DE SERAFINA CORRÊA

TONIAL
LGPD | DIREITO DIGITAL

SUMÁRIO

MUNICÍPIO DE SERAFINA CORRÊA

TONIAL LGPD | DIREITO DIGITAL

INTRODUÇÃO

Vivemos em um mundo cada vez mais conectado, mas também mais vulnerável. A tecnologia trouxe inúmeros benefícios, mas também abriu espaço para pessoas mal-intencionadas que se aproveitam da confiança, da distração ou até mesmo da falta de informação das vítimas para aplicar golpes. Das mensagens suspeitas às ofertas “imperdíveis”, as fraudes estão em todos os lugares — e qualquer pessoa pode ser alvo.

Esta cartilha foi elaborada pela Tonial Digital, em parceria com a Prefeitura Municipal de Serafina Corrêa, como parte da preocupação da Administração em auxiliar servidores públicos e suas famílias a reconhecer e evitar situações de risco. Nosso propósito é oferecer um material simples, didático e prático, que funcione como um guia de apoio no dia a dia.

Aqui você encontrará dicas de prevenção, sinais de alerta e orientações claras sobre o que fazer caso você ou alguém próximo seja vítima de um golpe. Mais do que informação, queremos fornecer proteção por meio do conhecimento, transformando a informação em uma verdadeira barreira contra golpistas.

Lembre-se: a melhor defesa é estar bem informado. Leia, compartilhe e ajude a construir uma rede de proteção contra fraudes em nossa cidade. Afinal, prevenir é sempre o melhor caminho!

MUNICÍPIO DE SERAFINA CORRÊA

TONIAL
LGPD | DIREITO DIGITAL

1 - GOLPE DO FALSO SEQUESTRO

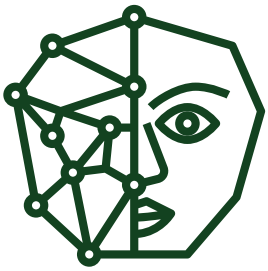
O golpe do falso sequestro é uma prática criminosa em que golpistas tentam extorquir dinheiro da vítima simulando o sequestro de um ente querido.

Eles criam uma situação de pânico e pressão emocional, geralmente com gritos e vozes semelhantes, para que a vítima pague rapidamente o resgate sem questionar a veracidade da história.

PREVENÇÃO

- Mantenha a Calma e tente não se desesperar ao receber esse tipo de ligação;
- Entre em contato com o suposto sequestrado ou outras pessoas próximas para confirmar a veracidade do sequestro;
- Evite fornecer qualquer dado pessoal ou familiar durante a ligação;
- Informe as autoridades sobre uma tentativa de golpe, fornecendo detalhes da ligação;
- Configure suas redes sociais e restrinja a privacidade das informações para evitar que crimes sejam usados para enganá-lo.

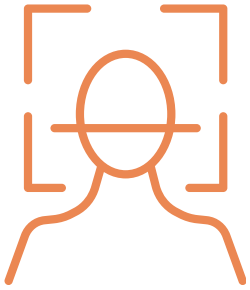
2 – DEEPFAKES



Deepfake é uma tecnologia que utiliza inteligência artificial (IA) para criar vídeos, áudios ou imagens falsificadas de maneira extremamente realista, alterando a aparência, a voz ou os movimentos de uma pessoa para que pareçam genuínos.

O deepfake pode ser usado para criar conteúdo manipulado e enganoso. A popularização do deepfake levou à sua aplicação em atividades fraudulentas.

PREVENÇÃO



Para evitar ser vítima de um golpe, é importante ficar atento a alguns detalhes, como: os movimentos dos olhos e da boca, as proporções do corpo, sombras inconsistentes, dicção e vocabulário, além de pedidos fora do habitual ou suspeitos.

3 – GOLPE DA FALSA CENTRAL DE ATENDIMENTO

Nesse golpe, os criminosos criam uma central telefônica falsa ou interceptam chamadas legítimas para enganar vítimas, se passando por representantes de bancos, operadoras de cartões ou empresas.

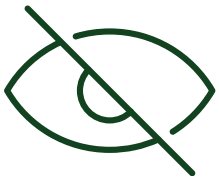
O objetivo é obter dados sensíveis, como senhas, números de cartão e informações pessoais, para realizar fraudes financeiras.

PREVENÇÃO

- Se receber uma ligação inesperada sobre transações ou problemas na conta, desligue e entre em contato diretamente com o banco pelos canais oficiais;
- Bancos e empresas legítimas não pedem senhas, números completos de cartão ou códigos de verificação enviados por SMS;
- Sempre verifique o número da central e evite usar links ou números enviados por mensagens desconhecidas;
- Não compartilhe códigos de autenticação com ninguém, nem mesmo com supostos funcionários do banco.

4 – GOLPE DA MÃO FANTASMA

O golpe “mão fantasma” faz você sentir que há uma mão invisível mexendo no seu celular. Nesse golpe, os criminosos obtêm acesso remoto ao celular ou computador da vítima, por meio de aplicativos ou softwares de controle remoto.



Depois de obter acesso, os criminosos simulam que estão ajudando a vítima, mas na verdade usam o dispositivo para realizar transferências, pagamentos ou outras operações financeiras indevidas, sem que a vítima perceba totalmente o que está fazendo.

COMO FUNCIONA O GgolpE?

1. Os **golpistas entram em contato com a vítima, se passando por representantes de bancos, empresas ou lojas.** Alegam que a conta da vítima foi comprometida, que há problemas no aplicativo bancário ou que precisa "ajudar" a resolver uma suposta falha.

2. A v**ítima é induzida a instalar um aplicativo** de acesso remoto. O golpista justifica a instalação dizendo que é necessário para solucionar o problema.

3. Após a instalação, o **golpista pede que a vítima forneça o código de acesso gerado pelo aplicativo** para controlar o dispositivo remotamente.

4. Com o **acesso ao dispositivo**, o golpista:
   - Navega por aplicativos bancários ou de pagamentos.
   - Realiza transferências, PIX, ou pagamentos de boletos.
   - Pode alterar as configurações ou excluir evidências de fraude.

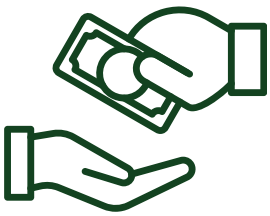
Em tempo real, eles movimentam seu dinheiro, realizando transferências para contas de terceiros, pagando boletos e solicitando empréstimos.

O golpe é perigoso porque ocorre de forma imperceptível, e a vítima pode não notar a atividade suspeita até que o dinheiro já tenha sido desviado.

PREVENÇÃO

- Caso receba uma ligação suspeita, entre em contato diretamente com o banco ou empresa pelo telefone oficial, disponível no site ou no verso do cartão;
- Nunca confie em ligações ou mensagens de supostos representantes de bancos ou empresas solicitando a instalação de aplicativos ou fornecimento de acesso remoto;
- Não baixe ou instale softwares de acesso remoto no celular ou computador a pedido de terceiros;
- Use senhas fortes, autenticação de dois fatores e mantenha seus aplicativos e sistemas operacionais atualizados;
- Nunca forneça códigos gerados por aplicativos de controle remoto ou autenticação.

5 – GOLPE DO EMPRÉSTIMO CONSIGNADO



O golpe do empréstimo consignado é uma prática criminosa em que golpistas utilizam técnicas fraudulentas para realizar empréstimos consignados em nome da vítima, muitas vezes sem seu consentimento, ou para aplicar outros golpes relacionados a promessas de ofertas vantajosas.

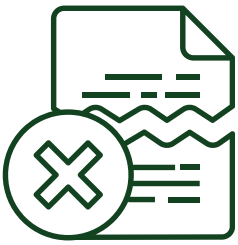
O objetivo dos criminosos é roubar dados pessoais ou se beneficiar financeiramente das custas da vítima.

PREVENÇÃO

- Nunca compartilhe documentos, informações bancárias ou senhas por telefone, WhatsApp ou e-mail, especialmente se não tiver certeza da origem do contato;
- Desconfie de ofertas muito boas, condições como “sem consulta ao SPC/Serasa”, “juros baixos demais” ou “liberação imediata” são sinais de alerta;
- Entre em contato diretamente com o banco ou instituição financeira pelos canais oficiais antes de contratar qualquer serviço;
- Prefira contratar empréstimos diretamente com instituições reconhecidas, evitando intermediários desconhecidos;
- As instituições financeiras legítimas não cobram taxas iniciais para liberar empréstimos.

6 – GOLPE DO PIX ERRADO

O golpe do PIX errado é uma prática criminosa em que os golpistas simulam o envio de um valor via PIX para a conta da vítima e, em seguida solicita o estorno, mas passa a chave de uma terceira conta.



Com isso, aciona o Mecanismo Especial de Devolução (MED) e recebe o valor da vítima, além do valor devolvido pelo banco, deixando a vítima no prejuízo. Esse golpe utiliza a boa-fé das pessoas e a pressa em corrigir o suposto erro para realizar uma fraude.

PREVENÇÃO

- Antes de devolver qualquer valor, verifique diretamente no aplicativo do banco ou no extrato da conta se a transferência foi realmente creditada;
- Não confie apenas em comprovantes, eles podem ser facilmente falsificados. Sempre verifique no sistema do banco;
- Se alguém iniciar para que você devolva o dinheiro rapidamente, mantenha a calma e avalie a situação;
- Evite compartilhar dados como CPF, e-mail ou telefone com pessoas desconhecidas, pois isso pode ser usado para criar novas fraudes.

7 – GOLPE DO BOLETO FALSO

O golpe do boleto falso é um tipo de fraude em que os criminosos criam ou adulteram boletos bancários para desviar o pagamento da vítima para contas fraudulentas. Esse golpe é comum devido ao uso frequente de boletos para compras, pagamento de contas e serviços, especialmente em ambientes digitais.

Essa fraude explora a confiança e a rotina das pessoas em realizar pagamentos. Por isso, atenção aos detalhes e seleção minuciosa são fundamentais para evitar cair nesse golpe.

COMO IDENTIFICAR UM BOLETO FALSO:

Verifique se o nome do beneficiário corresponde à empresa ou pessoa para quem você pretende pagar. 1

2 **Certifique-se de que a sequência numérica do código de barras corresponde ao boleto**. Qualquer divergência é um sinal de alerta.

D**esconfie de boletos enviados por canais não solicitados,** como e-mails ou mensagens de desconhecidos. 3

4 **Preste atenção em erros** de digitação, logotipos mal formatados, falta de dados importantes ou design malfeito.

Boletos fraudulentos podem conter valores diferentes do esperado ou prazos mais curtos para forçar o pagamento imediato. 5

PREVENÇÃO

- Sempre gere e pague boletos diretamente no site oficial da empresa ou instituição;
- Utilize o aplicativo do banco, muitos aplicativos bancários conseguem identificar inconsistências em boletos e alertar sobre possíveis fraudes;
- Confirme os dados do boleto antes de pagar, confirme as informações do boleto diretamente com o emissor, principalmente em valores altos ou boletos recebidos por e-mail;
- Não clique em links de boletos enviados por desconhecidos ou que pareçam suspeitos. Prefira acessar o site diretamente;
- Use um bom antivírus e evite acessar informações financeiras em redes Wi-Fi públicas.

8 – GOLPE DO JOGO DO TIGRINHO

O "Jogo do Tigrinho" , também conhecido como Fortune Tiger, é um jogo de cassino online que simula máquinas de caça-níqueis, prometendo ganhos financeiros rápidos e elevados. No entanto, existem inúmeros relatos de pessoas que jamais conquistaram os ganhos financeiros prometidos pelo Jogo do Tigrinho e outros semelhantes.

Mesmo quando a pessoa se sente lesada e acumula prejuízos, não há muito o que possa ser feito por ela pois a plataforma em questão é hospedada fora do país e não possui registro ou representantes no Brasil.

9 – GOLPE DA FALSA PREMIAÇÃO

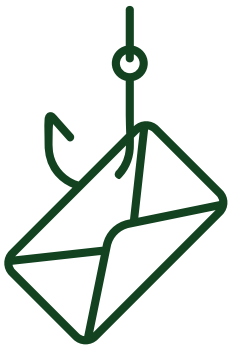
O golpe da falsa premiação é uma fraude em que os criminosos entram em contato com as vítimas, alegando que eles ganharam um prêmio ou sorteio inexistente. O objetivo é obter vantagens financeiras ou informações pessoais das vítimas.

Golpistas informam que a vítima ganhou um prêmio, mas que é necessário pagar uma taxa para recebê-lo. Após o pagamento, a vítima nunca recebe o prêmio.

PREVENÇÃO

- Se alguém entrar em contato afirmando que você ganhou um prêmio que você não se lembra de ter participado, desconfie;
- Nenhuma premiação legítima exige a realização de outros pagamentos para liberar o prêmio;
- Não confie cegamente em promoções divulgadas por influenciadores ou anúncios;
- Fique atento a mensagens com erros ortográficos ou em tom informal.

10 – PHISHING



Phishing é uma prática fraudulenta utilizada por cibercriminosos para enganar pessoas e obter informações temporárias, como senhas, números de cartões de crédito, dados bancários ou outras informações pessoais.

Geralmente, o ataque é realizado por meio de e-mails, mensagens de texto ou sites falsos que simulam organizações legítimas.

CUIDADO COM O SPOOFING

Spoofing é uma técnica de fraude cibernética em que o golpista manipula informações ou disfarça sua identidade para se passar por uma fonte confiável. O objetivo do spoofing é enganar a vítima, obter dados acessíveis ou realizar ações maliciosas.

PREVENÇÃO

- Não clique em links ou baixe anexos de remetentes desconhecidos;
- Passe o mouse sobre os links para verificar a URL antes de clicar. O site deve começar com https:// e possui um cadeado na barra de endereços;
- Empresas legítimas não pedem senhas, números de cartão ou outros dados necessários por e-mail ou mensagem;
- Adicione uma camada extra de segurança às suas contas, como autenticação por SMS ou aplicativos específicos;
- Mantenha seu sistema operacional, navegador e software atualizados.

11 – GOLPE DO “NOVO NÚMERO” DO WHATSAPP

O golpe do "novo número" no WhatsApp é uma prática cada vez mais comum, em que golpistas se passam por amigos ou familiares da vítima, alegando ter mudado de número, para solicitar dinheiro. Esse tipo de golpe é muito eficaz porque explora a confiança e a urgência emocional das vítimas.

SE ESTIVEREM SE PASSANDO POR VOCÊ:

1. **Informe seus contatos imediatamente:** Informe-os para não fornecerem dinheiro ou informações sem antes confirmar com você por outra forma de comunicação e peça para que denunciem o número pelo WhatsApp.

2. **Verifique a segurança da sua conta:** Acesse o WhatsApp no seu dispositivo e certifique-se de que a conta não foi desconectada ou clonada e ative a verificação em duas etapas.

3. **Proteja e monitore a sua conta:** Desconecte a conta de outros dispositivos e continue monitorando suas conversas no WhatsApp e esteja atento a qualquer comportamento suspeito. Aproveite para revisar o backup e as configurações de privacidade de sua conta.

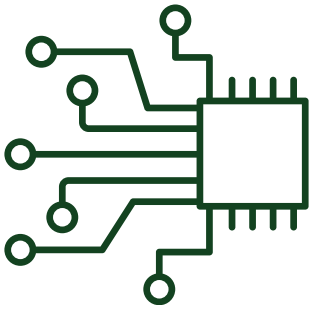
4. **Registre um Boletim de Ocorrência:** Ele poderá ser útil para futuras investigações e medidas de proteção!

PREVENÇÃO

- Antes de enviar qualquer dinheiro, confirme a história com outros conhecidos;
- Só salve o "novo número" após confirmar com o contato original;
- Limite quem pode ver suas informações no WhatsApp (como foto de perfil e status) nas configurações de privacidade.
- Isso dificulta que sua conta seja clonada ou usada em golpes semelhantes.

12 – GOLPE DO SIM SWAP

O golpe do SIM Swap (ou troca de chip) é uma prática em que golpistas transferem o número de telefone da vítima para um chip controlado por eles. Esse golpe permite aos criminosos assumir o controle de contas online que usam o número de telefone para autenticação, como bancos, redes sociais e e-mails.



O golpe do SIM Swap é perigoso porque explora uma vulnerabilidade na dependência de números de telefone como identificadores.

COMO FUNCIONA ESSE GOLPE?

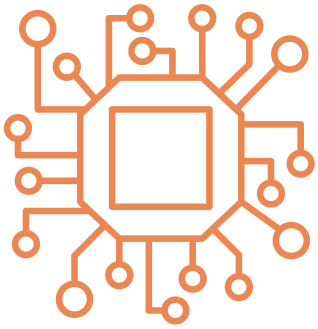
1. **Coleta de Informações:** Os golpistas obtêm dados pessoais da vítima, como nome completo, CPF, RG, endereço e até números de telefone, por meio de: Phishing, Vazamentos de dados, Redes sociais, Documentos perdidos ou roubados.

2. **Contato com a Operadora:** Com os dados da vítima, o golpista entra em contato com a operadora de telefonia, fingindo ser o titular da linha. Ele alega, por exemplo, que perdeu o chip e solicita a transferência do número para um novo chip.

3. **Habilitação do Novo Chip:** A operadora transfere o número para o chip do criminoso, desativando o chip original da vítima.

4. **Com o número, o golpista consegue:** Receber códigos de autenticação enviados por SMS; Redefinir senhas de contas bancárias, e-mails e redes sociais; Assumir o controle de contas protegidas por autenticação de dois fatores via SMS.

PREVENÇÃO



- Acompanhe se seus dados foram comprometidos em vazamentos e tome medidas para reforçar sua segurança;
- Fique atento a notificações de atividades suspeitas em suas contas, como tentativas de redefinição de senha;
- Não compartilhe publicamente dados pessoais, como número de telefone, CPF, ou endereço;
- Prefira métodos de autenticação em dois fatores que não dependam de SMS, como aplicativos de autenticação;
- Entre em contato com sua operadora e solicite um bloqueio adicional para solicitações de troca de chip. Algumas operadoras oferecem senha ou autenticação extra.

13 – GOLPE DA COMPRA PELA INTERNET

O golpe da compra pela internet é uma prática fraudulenta em que golpistas enganam consumidores em plataformas online para roubar dinheiro, informações pessoais ou dados bancários.

Esses golpes podem ocorrer em sites falsos, marketplaces, redes sociais ou até mesmo em anúncios fraudulentos.

MODALIDADES DE GOLPE

Sites Falsos: Golpistas criam sites que se parecem legítimos. Eles usam fotos e descrições de outras fontes ou até mesmo inventam. Esses sites falsos podem ser difíceis de distinguir de lojas genuínas.

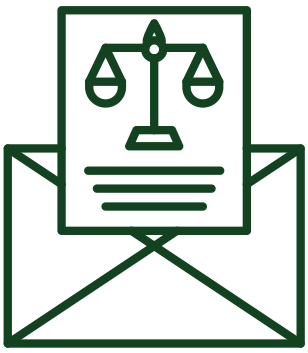
Produtos Inexistentes: Os golpistas podem listar produtos a preços baixos para atrair compradores. No entanto, esses produtos não existem ou não são como descritos.

Pagamentos Adiantados: Para garantir a "compra" do produto, os golpistas solicitam pagamentos adiantados. Por meio de transferência, cartão ou pagamento online. Uma vez que recebem o pagamento, os golpistas desaparecem e os compradores nunca recebem os produtos.

PREVENÇÃO

- Ofertas que parecem “boas demais para ser verdade” geralmente são golpes;
- Pesquise o nome, CNPJ, ou o site da loja em plataformas de reclamação como o Reclame Aqui;
- Verifique se lojas anunciadas em redes sociais têm CNPJ, telefone, endereço e avaliações confiáveis;
- Nunca aceite pagar diretamente via Pix, transferência ou boleto ao negociar em marketplaces como Mercado Livre, OLX ou Shopee;
- Verifique o domínio (URL) do site e certifique-se de que ele usa HTTPS;
- Antes de comprar, busque o produto ou vendedor para verificar possíveis alertas de golpe.

14 – GOLPE DA FALSA INTIMAÇÃO



O golpe da falsa intimação é uma fraude em que golpistas se passam por representantes do Judiciário ou de escritórios de advocacia para enviar notificações falsas de intimação. Essas notificações têm o objetivo de assustar a vítima e levá-la a realizar pagamentos ou fornecer informações pessoais confidenciais.

Esse golpe tem sido cada vez mais comum e pode ocorrer por e-mail, mensagem, correspondência física ou até ligações.

PREVENÇÃO

- Confirme no site oficial do tribunal ou ligue para o órgão citado na intimação para verificar se o documento é real;
- Utilize o número do processo (se fornecido) para verificar a existência da ação judicial;
- Tribunais não exigem pagamentos por intimações ou audiências;
- Não clique em links nem baixe anexos de mensagens ou e-mails suspeitos;
- Intimações verdadeiras geralmente são entregues por oficial de justiça ou carta registrada, e não por mensagens ou ligações.

CAÍ NO Ggolpe, E AGORA?

1. **Identifique o tipo de golpe:** Financeiro, Roubo de Identidade, Golpe Digital, Chantagem...

2. **Entre em contato com o banco:** Solicite o bloqueio imediato do cartão ou conta, e informe sobre a transação e peça a tentativa de reversão, especialmente no caso de PIX ou transferências bancárias.

3. **Acompanhe seu CPF:** Monitore movimentações em serviços como o Meu INSS ou Receita Federal.

4. **Alteração de senhas:** Troque imediatamente as senhas de contas comprometidas e ative a autenticação em dois fatores.

5. **Reúna provas:** Salve mensagens, e-mails, comprovantes de pagamento e capturas de tela.

6. **Procure um advogado:** Para entrar com ações judiciais com a finalidade de buscar ressarcimento dos valores perdidos, e aconselhar sobre as melhores estratégias para minimizar os danos e proteger seus direitos.

7. **Registre um boletim de ocorrência:** Compareça a uma delegacia ou utilize serviços online (se disponível no seu estado) para registrar o ocorrido.

8. **Denuncie à plataforma ou site:** Denuncie perfis falsos, anúncios fraudulentos ou atividades suspeitas diretamente na plataforma (WhatsApp, Instagram, e-commerce, etc.). No caso de marketplace ou app de Compras, notifique a plataforma (Mercado Livre, OLX, Shopee, etc.) sobre o golpe.

SINAIS DE ALERTA DE GgolpES

- **Abordagem inesperada:** Você é abordado na rua por um desconhecido com uma história urgente ou emocionante.

- **Pressão para decisão rápida:** Os golpistas criam um senso de urgência, pressionando você a tomar uma decisão, sem tempo para pensar ou consultar alguém.

- **Oferta irrealista:** Os golpes geralmente se apresentam como uma grande vantagem financeira, sendo necessário desembolsar uma quantia pequena para supostamente receber uma quantia muito maior.

- **Pedido de sigilo:** Pedem que você não conte a ninguém sobre a transação realizada.

- **Seguidores em potencial:** Se há alguém caminhando atrás de você ou acompanhando seus passos.

- **Chegada sem aviso prévio:** Pessoas se passando por técnicos, entregadores ou representantes de empresas, que não agendaram visita.

- **Distração planejada:** Golpistas tentam distrair você enquanto digita a senha em transações, geralmente chamando atenção para algo ou conversando.

- **Pedido para repetir a operação:** O golpista pode sugerir que a operação não foi concluída e pede que você insira o cartão novamente.

SINAIS DE ALERTA DE GOLPES

- **Desbloqueios ou mudanças de dados suspeitas:** Alterações no perfil da sua conta, como mudança de senha ou endereço, sem sua autorização.

- **Ligações ou e-mails do "banco":** Recebe contato de supostos representantes pedindo para confirmar dados do cartão ou a senha. Isso pode ser uma tentativa de phishing.

- **Pedido de transferências ou pagamentos:** Alegam que é necessário realizar transferência para uma "conta segura" para proteger seu dinheiro.

- **Solicitação de um documento assinado:** Sempre verifique o que você está assinando, muitas vezes sua assinatura pode ser usada em fraudes.

- **Pedido para instalar aplicativos ou programas:** O golpista solicita que você instale ferramentas de acesso remoto, alegando que são necessárias para "ajuda técnica".

- **Exigência de compartilhamento de códigos:** Pedem códigos de acesso para concluir o "suporte" ou resolver problema no dispositivo.

- **Foco em contas bancárias ou apps de pagamento:** Solicitam que você abra aplicativos bancários, carteiras digitais ou ambientes de pagamento online enquanto têm controle do dispositivo.

- **Transferências em horário de limite bancário:** Golpistas podem dizer que fizeram a transação em horário de limite bancário (fim de expediente ou à noite) para justificar a ausência de saldo imediato.

SINAIS DE ALERTA DE GOLPES

- **Desconfie ao pedir reembolso:** Em alguns casos, os golpistas fingem que o Pix foi duplicado e solicitam um "reembolso" imediato, tentando fazer a vítima devolver o dinheiro inexistente.

- **Transações não reconhecidas:** Aparecem compras ou saques em locais que você não visitou ou valores que não reconhece em seu extrato.

- **Erro em valores e detalhes:** O valor mencionado pode não bater com o suposto comprovante, ou os dados do remetente são vagos ou inconsistentes.

- **Pedido de verificação em ambientes não oficiais:** Alegam que o comprovante só pode ser verificado em plataformas externas, como e-mails, PDFs enviados por aplicativos ou capturas de tela.

- **Solicitação de pagamento em nome de terceiros:** A empresa supostamente emissora alega ter alterado os dados de pagamento ou que agora trabalha com intermediários desconhecidos.

- **Falta de informações do beneficiário:** Boletos falsos frequentemente omitem ou adulteram informações do emissor, como CNPJ, nome da empresa ou endereço.

- **Esquema de pirâmide ou marketing multinível:** Incentivam você a recrutar novos investidores, prometendo ganhos extras para cada pessoa indicada, o que geralmente é um indício de pirâmide financeira.

SINAIS DE ALERTA DE GOLPES

- **Recusa em permitir saques:** Quando você tenta retirar o suposto lucro ou capital investido, surgem desculpas ou barreiras, como a exigência de mais pagamentos.

- **Links ou anexos suspeitos:** Links levam a sites falsos que imitam páginas legítimas (bancos, redes sociais, lojas online).

- **Erros de ortografia ou formatação:** Mensagens de phishing frequentemente contêm erros de gramática, ortografia ou formatação que não são típicos de organizações legítimas.

- **Ofertas ou benefícios irrealistas:** Promessas de grandes prêmios, descontos enormes ou vantagens financeiras em troca de clicar em um link ou fornecer informações.

- **Desempenho lentificado na rede:** A rede se torna anormalmente lenta ou desconexa, dificultando a navegação na internet, o acesso a sistemas ou a transferência de dados.

- **Erros ou interrupções em sistemas:** No caso de quedas frequentes de sistemas ou servidores ou mensagens de erro incomuns ao acessar serviços online.

- **Pop-ups e anúncios excessivos:** Aparecimento de janelas pop-up frequentes, mesmo quando nenhum navegador está aberto.

SINAIS DE ALERTA DE GOLPES

- **Recebimento de cartões ou documentos não solicitados:** Chegada de cartões de crédito, cheques ou documentos que você não solicitou.

- **Notificação de solicitação de empréstimos:** Informações de que seu CPF foi consultado para aprovação de crédito ou empréstimos que você não pediu.

- **Contato de cobrança de dívidas falsas:** Ligação ou correspondência de cobradores sobre dívidas ou serviços contratados que você desconhece.

- **Perda repentina de sinal no celular:** O celular perde sinal de forma inesperada e não consegue se conectar à rede, mesmo em áreas com boa cobertura.

- **Dificuldade em realizar chamadas ou enviar mensagens:** Não é possível realizar chamadas, enviar mensagens de texto ou acessar dados móveis.

- **Exigência de pagamento adicional:** O entregador alega que você precisa pagar uma taxa extra por entrega, embalagem ou algum outro serviço que não foi informado previamente.

- **Comunicação não oficial:** Multas de trânsito chegam por canais não confiáveis, como e-mails genéricos, SMS ou WhatsApp, sem identificação oficial.

SINAIS DE ALERTA DE GgolpES

- **Rápido envolvimento emocional:** A pessoa demonstra interesse romântico ou sexual de maneira acelerada, criando uma conexão superficial.

- **Solicitação de nudes ou vídeos íntimos:** Insistência para trocar imagens ou vídeos íntimos, com pretextos como "confiança mútua" ou "aproximar a relação".

- **Perfis falsos ou duvidosos:** Perfis com poucas informações, fotos genéricas ou imagens de pessoas muito atraentes (muitas vezes retiradas da internet).