

GOLPES ONLINE



**SAIBA COMO SE PROTEGER
DOS PRINCIPAIS GOLPES
CIBERNÉTICOS!**



Autor: Esp. Fernando Bracalente – CISSP

Revisor: Dr. Paulo Perrotti

PROTEJA-SE.

INFORME-SE.

AJA.

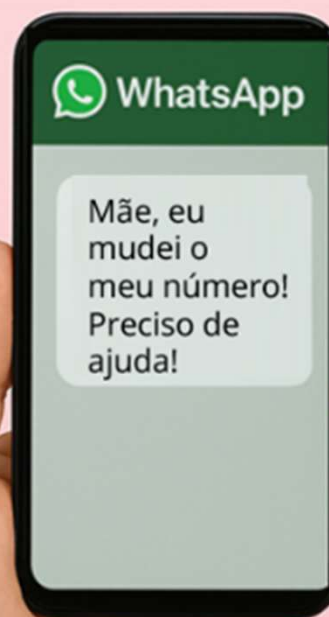
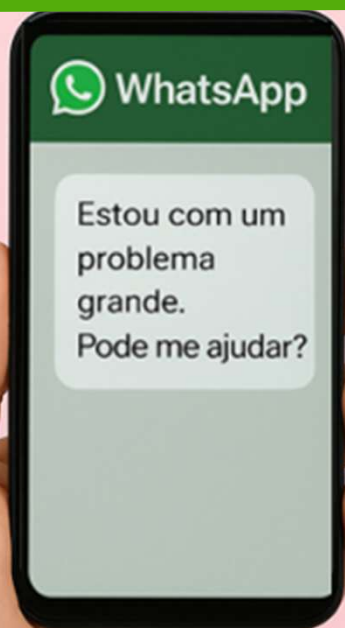
COMPARTILHE.

Apoio: <https://ciberaventuras.com.br/>
Descubra como utilizar a internet de forma segura!

ÍNDICE

Golpes do WhatsApp	3
Golpe da Maquininha	4
Golpe do Aniversário	5
Golpe do Falso Emprego	6
Golpe na Compra Online	7
Golpe do Falso Colaborador	8
Golpes e Crimes em Jogos Online	9
Golpe do Amor	10
Golpes na Black Friday	11
Furto do Perfil em Redes Sociais	12
Fui vítima, o que fazer agora?	13

Golpe do WhatsApp



O **golpe do WhatsApp** é uma tentativa de fraude que utiliza o aplicativo de mensagens para **enganar as pessoas**, geralmente com o objetivo de se apropriar de dados pessoais, senhas ou fazer com que a vítima realize transferências **financeiras indevidas (como Pix)** para os criminosos.

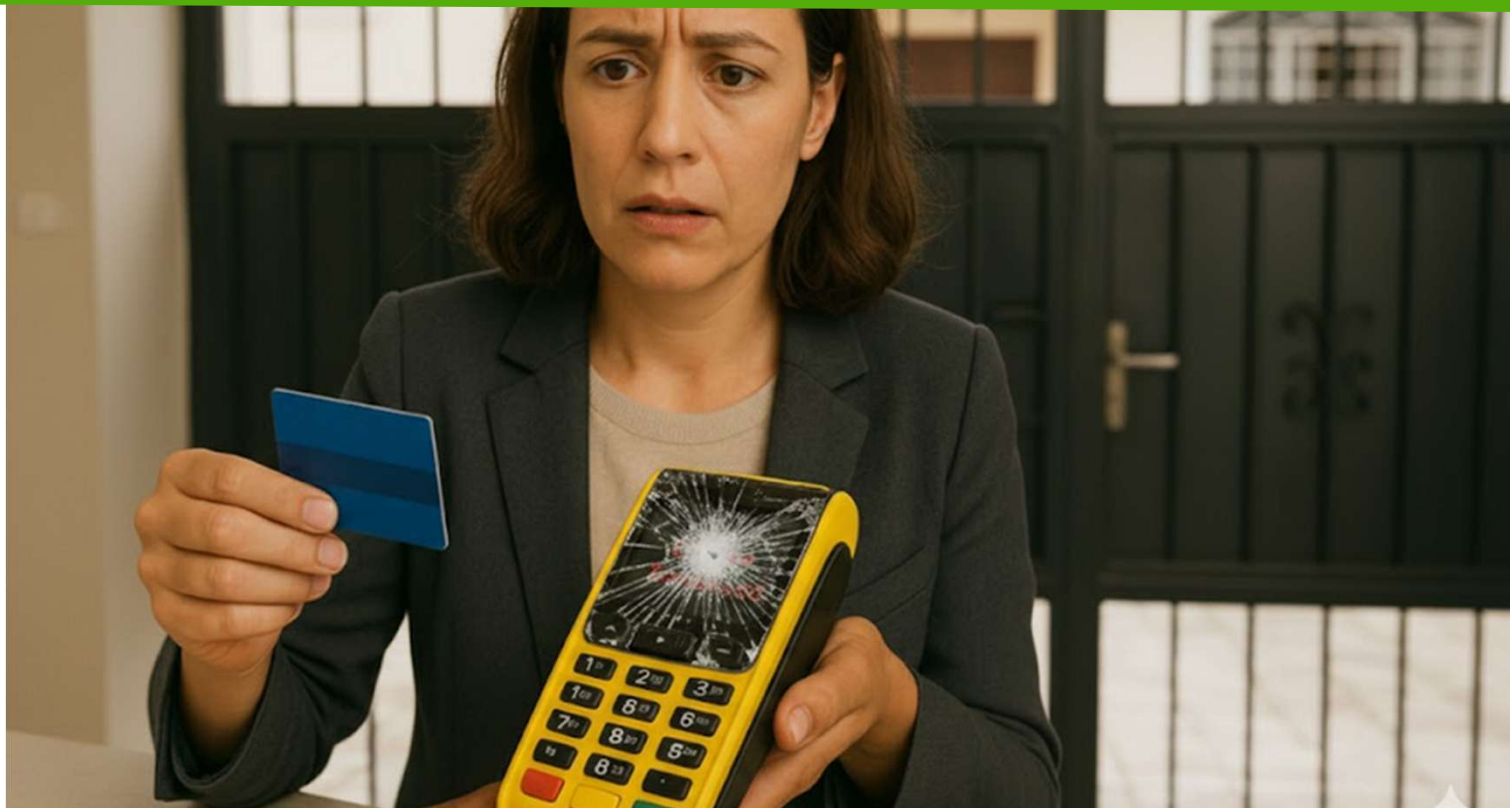
Faça

- **Ative a verificação em duas etapas no WhatsApp** (nas configurações de conta).
- **Desconfie de mensagens pedindo dinheiro**, mesmo que pareçam ser de amigos ou parentes.
- **Confirme por outro canal** (ligação, vídeo chamada ou pessoalmente de preferência) antes de tomar qualquer atitude.
- **Reporte e bloqueie números suspeitos** no aplicativo.

Não Faça

- **Não envie dinheiro** sem confirmar antes com a pessoa por outro meio como videochamada, presencialmente, ligação ou envie mensagem para o **número antigo**.
- **Não clique** em links enviados por desconhecidos ou que prometem prêmios e vantagens.
- **NUNCA compartilhe códigos do WhatsApp**, mesmo que alguém diga ser da equipe do banco, polícia, do app, etc.
- **Desconfie de mensagens com urgência** ("preciso agora!", "é urgente!", "o carro quebrou", etc.) isso pode ser tática de golpista.

Golpe da Maquininha



O **golpista esconde a tela da maquininha** (dizendo que “está quebrada” ou “com problema”) e digita um valor muito maior do que o combinado, **a vítima sem perceber**, aprova o pagamento e só **descobre o prejuízo depois** ao olhar o extrato ou a fatura do cartão.

Faça

- **Veja sempre o valor na tela antes de digitar a senha.**
- **Peça para segurar a maquininha** você mesmo, não aceite que a pessoa esconda o visor.
- **Confirme o valor em voz alta com o vendedor** antes de aprovar.
- **Exija o comprovante impresso** ou digital e confira o valor imediatamente.
- **Apenas use maquininhas com tela visível e em bom estado** de conservação, **NUNCA** pagar em dispositivos com visor trincado, escuro ou coberto.
- **Ative a notificação** do seu cartão de crédito ou de débito.

Não Faça

- **Não digite a senha se não conseguir ver o valor.**
- **Não aceite justificativas** como “a tela quebrou” ou “confia, é o valor certo”.
- **Não deixe ninguém distrair você enquanto paga.**
- **Não use maquininhas que pareçam adulteradas** ou antigas demais.
- **Nunca entregue seu cartão a outra pessoa** para ela “ajudar” a passar.

Golpe do Aniversário



Alguém envia uma mensagem **dizendo que você ganhou um presente** e só precisa **pagar o frete**. Se você clicar no link e inserir seus dados ou pagar com cartão na maquininha do entregador, os criminosos podem copiar suas informações e fazer **débitos ou compras sem sua autorização**.

Faça

- **Desconfie de mensagens que prometem prêmios ou presentes fáceis.**
- **Verifique o remetente**, veja se o site ou número é realmente da empresa.
- Procure o nome da empresa no Google e veja se há reclamações ou alertas.
- **Use cartões virtuais ou pré-pagos** em compras online para evitar fraudes maiores.
- **Monitore seu extrato bancário** para identificar cobranças suspeitas rapidamente.

Não Faça

- **Não clique em links enviados por WhatsApp, SMS ou e-mail desconhecido.**
- **Não digite seus dados pessoais e de cartão de crédito em sites suspeitos.**
- **Não acredite em mensagens genéricas** ("Parabéns pelo seu dia!").
- **Não compartilhe mensagens de desconhecidos com amigos ou grupos.**
- **Não forneça códigos recebidos por SMS** nem para "entregar o presente".
- **Nunca tire foto se algum desconhecido pedir** principalmente se for durante a entrega de algo que você **não solicitou**.

Golpe do Falso Emprego



Esse golpe acontece quando golpistas se **aproveitam de pessoas que estão procurando trabalho**. Eles publicam **vagas falsas em sites**, redes sociais ou mandam mensagens e e-mails com promessas de salário alto e trabalho fácil. O objetivo é **enganar a vítima e receber dinheiro e/ou dados pessoais das vítimas** de forma fraudulenta.

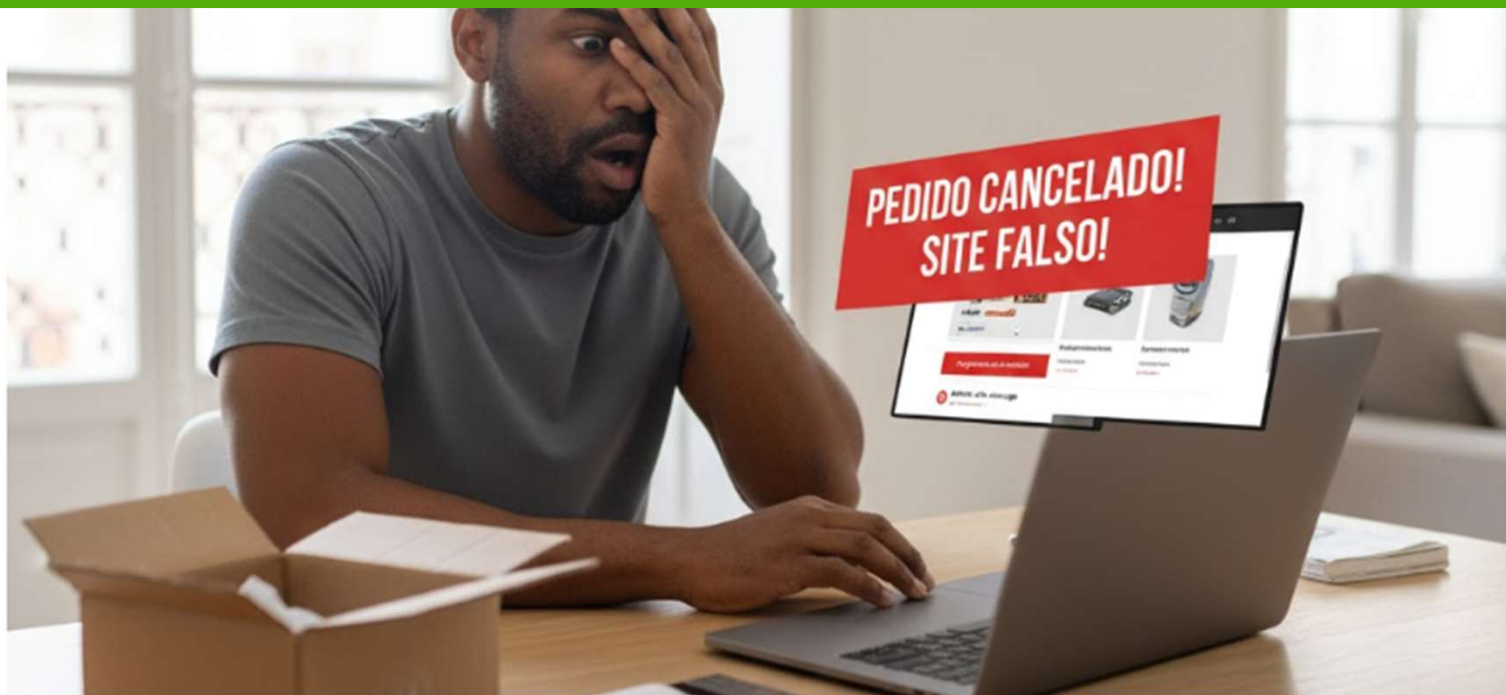
Faça

- **Procure vagas em lugares confiáveis:** Use sites conhecidos de emprego, agências reconhecidas ou os canais oficiais das empresas.
- **Desconfie de promessas boas demais:**
- **Pesquise sobre a empresa:** Veja se ela realmente existe, procure o CNPJ e olhe o site ou redes sociais oficiais.
- **Verifique o e-mail do recrutador:** Empresas usam e-mails com o nome da própria empresa (ex: nome@empresa.com.br), e não endereços genéricos como Gmail, Outlook ou Yahoo.
- **Pergunte e confirme:** Em entrevistas online, faça perguntas sobre a vaga e a empresa, recrutadores responderão com facilidade e clareza todas as suas dúvidas.

Não Faça

- **Não pague taxas:** Não pague taxa alguma! Empresas não cobram nada dos candidatos.
- **Seja cético:** Não confie cegamente em resultados patrocinados de pesquisa em buscadores na Internet ou e-mails de emprego não solicitados.
- **Verifique anúncios:** Nunca se candidate a vagas sem verificar a autenticidade dos anúncios, especialmente em plataformas ou grupos de redes sociais.

Golpe na Compra Online



Esse golpe acontece quando criminosos **criam sites falsos ou usam lojas conhecidas de forma enganosa**, oferecendo produtos muito baratos para enganar quem compra online. **A vítima paga**, perde o dinheiro e muitas vezes tem os dados pessoais e informações do cartão indevidamente coletados e fraudados.

Faça

- **Pesquise a reputação da loja:** Antes de finalizar a compra, procure pelo nome do site no Google, **Reclame Aqui** e redes sociais. Verifique se há reclamações de produtos não entregues ou fraude.
- **Use canais de pagamento oficiais:** Prefira usar métodos de pagamento conhecidos e seguros, como cartões de crédito virtuais ou intermediadores de pagamento (Mercado Pago, PagSeguro), **que oferecem proteção ao comprador.**
- **Desconfie de preços inacreditáveis:** Se o preço estiver muito abaixo do que é praticado no mercado, desconfie.
- **Confira os dados do boleto/Pix:** Ao pagar via boleto, confira o nome da empresa no beneficiário, o CNPJ e o código do banco. Se for Pix, verifique se o nome do destinatário corresponde à loja onde você está comprando.

Não Faça

- **Não clique em links de promoção inesperada:** Evite clicar em links de ofertas recebidos por e-mail, SMS ou WhatsApp, mesmo que sejam muito tentadores. O melhor é sempre digitar o endereço do site oficial no navegador.
- **Evite comprar em sites desconhecidos no primeiro acesso:** Dê preferência a sites conhecidos e com boa reputação para suas compras.
- **Não use computadores públicos / compartilhados:** Evite fazer compras online usando computadores compartilhados.
- **Não forneça dados pessoais em excesso:** lojas virtuais confiáveis não pedem informações como o número completo do seu RG ou CPF apenas para fazer um orçamento. Informe apenas o que for realmente necessário e desconfie de pedidos exagerados.

Golpe do Falso Colaborador



As **ligações desconhecidas** podem ser golpes em que criminosos fingem representar **bancos, advogados, empresas ou órgãos do governo** para te enganar. Eles usam **truques para parecer confiáveis** e fazer com que a vítima revele dados pessoais, senhas ou informações do cartão de crédito ou débito. Às vezes, até falsificam o número que aparece na tela do seu celular para parecer uma chamada verdadeira.

Faça

- **Use bloqueadores de chamadas:** Instale aplicativos de bloqueio de chamadas e denuncie ligações de spam.
- **Seja cauteloso:** Tenha cuidado ao atender chamadas de números desconhecidos.
- **Espalhe a conscientização:** Eduque outras pessoas sobre golpes telefônicos comuns.
- **Ative medidas de segurança:** Use senhas no correio de voz para maior proteção.

Não Faça

- **Não compartilhe informações pessoais:** Nunca forneça dados pessoais ou financeiros.
- **Não confie no identificador de chamadas:** O identificador pode ser falsificado. Portanto, não confie nele.
- **Evite números desconhecidos:** Não retorne chamadas de números desconhecidos ou internacionais.
- **Proteja seus dados:** Instituições legítimas nunca pedem informações sensíveis como nomes de usuário, senhas ou códigos OTP. Nunca compartilhe essas informações.

Golpes e Crimes em Jogos Online



No universo dos jogos, **os cibercriminosos não querem só ganhar**, eles usam **links falsos, vírus, conversas manipuladoras e a falsa identidade de outros jogadores** para se apropriar de sua conta, seus itens, seus dados financeiros e, em casos gravíssimos, atuam como predadores buscando **explorar e manipular vítimas vulneráveis**.

Faça

- **Monitore os jogos dos seus filhos:** Se for pai/mãe, supervisione o acesso e saiba com quem a criança está falando online.
- **Use senhas fortes e únicas:** Crie senhas diferentes e complexas para cada jogo e conta.
- **Habilite a autenticação de Dois Fatores (2FA):** Sempre ative esta proteção extra em todas as suas contas de jogos.
- **Mantenha dados pessoais em segredo:** **NUNCA** compartilhe seu nome completo, endereço, telefone ou fotos com desconhecidos nos jogos.
- **Verifique antes de pagar:** Seja muito cauteloso com jogos que pedem dinheiro real ou prometem lucros fáceis. Confie apenas em lojas oficiais.

Não Faça

- **Não aceite presentes de estranhos:** Recuse amizades, convites de grupos ou links de qualquer pessoa que você não conheça na vida real.
- **Não baixe aplicativos por fora:** Evite baixar jogos ou *cheats* de sites ou fontes que não sejam as lojas oficiais (Google Play, App Store, loja do console, etc.).
- **Não conceda permissões exageradas:** Não permita que o jogo acesse sua localização, seus contatos ou suas fotos se isso não for essencial para jogar.
- **Não confie em lucros fáceis:** Ignore qualquer jogo ou anúncio que garanta dinheiro ou itens de volta (retornos garantidos) — é quase sempre um golpe.
- **Não fale sobre a sua vida pessoal.**

Golpes na Black Friday



BLACK FRIDAY

Desconto 99%

Compartilhe, Click!

Aproveite agora!!

Durante a **Black Friday**, aumentam muito as tentativas de golpes pelo celular, WhatsApp, SMS e redes sociais. Os golpistas sabem que as pessoas estão buscando ofertas e aproveitam esse momento para enganar com links falsos, mensagens irresistíveis e promoções “boas demais para ser verdade”.

Faça

- **Verifique o site antes de comprar:** Sempre digite o endereço da loja direto no navegador (Ex: www.magazineluiza.com.br, www.amazon.com.br).
- **Pesquise a reputação da loja:** Se não conhece a loja, pesquise no Google, **Reclame Aqui** ou **Procon**. Verifique avaliações recentes. Sites falsos costumam ter preços muito abaixo do normal.
- **Habilite autenticação em duas etapas (2FA):** Isso impede que golpistas acessem suas contas mesmo que descubram sua senha.
- **Desconfie de promoções urgentes demais:** Mensagens como “só hoje”, “últimas unidades” e “corra antes que acabe” são usadas para te fazer agir sem pensar.
- **Fique Atento!**

Não Faça

- **Não clique em links enviados por WhatsApp, SMS, Instagram ou e-mail desconhecido:** Essa é a principal forma de golpes na Black Friday.
- **Não forneça seus dados pessoais em páginas suspeitas:** Golpistas pedem CPF, endereço, número de cartão, código de segurança e até senha sob o pretexto de “confirmar compra”.
- **Não pague PIX para lojas desconhecidas:** PIX é praticamente irreversível e é o método preferido dos golpistas.
- **Não baixe aplicativos por links:** Aplicativos falsos podem roubar suas senhas e dados bancários.
- **Não compartilhe promoções antes de verificar:** Muitas correntes pedem para enviar a amigos para “liberar o cupom”. Pode ser golpe para espalhar páginas falsas.

Golpe do Amor



É um tipo de golpe em que o criminoso **cria uma identidade falsa** nas redes sociais ou em **aplicativos de namoro**, com o **único objetivo de manipular emocionalmente a vítima para conseguir dinheiro**.

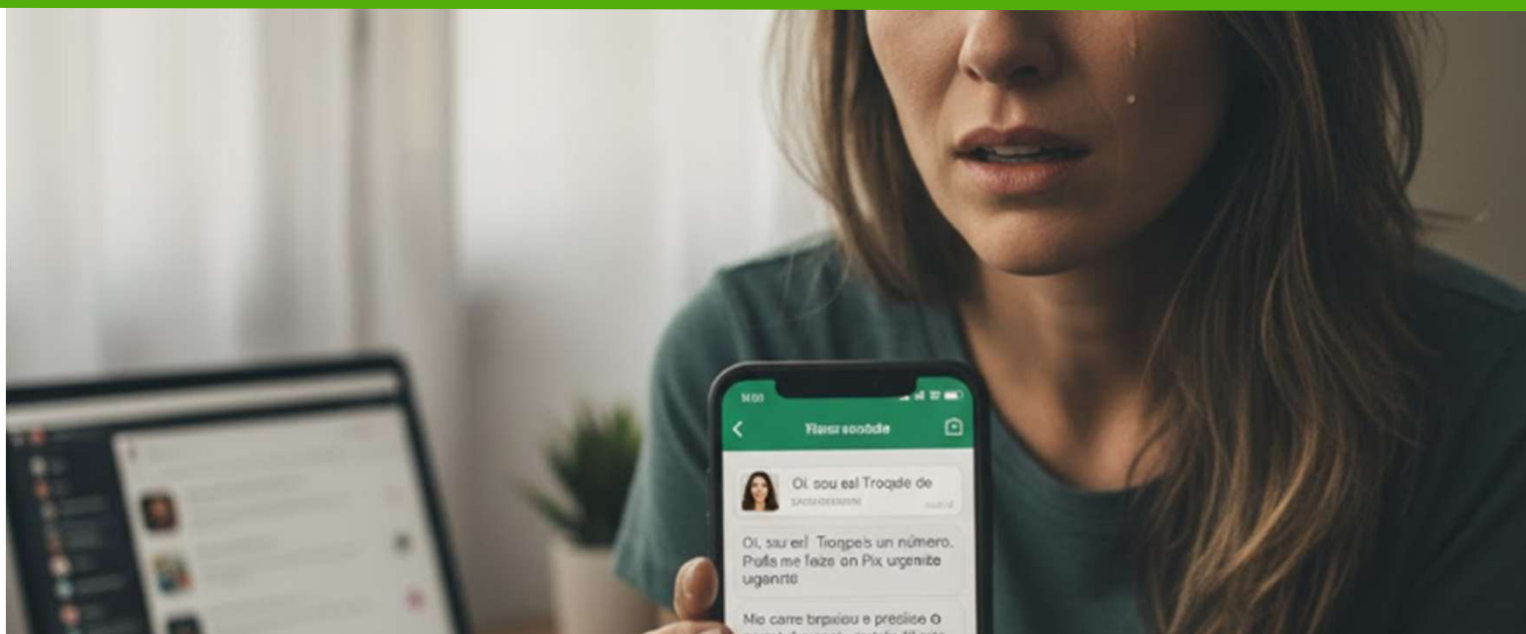
Faça

- **Pesquise as fotos do perfil** usando a pesquisa reversa de imagens (Google Imagens, TinEye).
- **Use chamadas de vídeo** (porém, com cautela).
- **Verifique a coerência da história e do português:** Preste atenção em furos na história, mudanças repentinas de detalhes da vida, etc.
- **Converse com um amigo ou familiar de confiança sobre o relacionamento.**
- **Mantenha-se cético** se a pessoa declarar amor rapidamente (o famoso "love bombing").
- **Verifique se as imagens não foram geradas por Inteligência Artificial:** Procure por inconsistências e artefatos que a IA ainda tem dificuldade em replicar perfeitamente como mãos, dedos, joias e acessórios, textos ilegíveis, iluminação, etc.

Não Faça

- **NUNCA envie dinheiro ou cartões-presente**, nem faça transferências (Pix, TED) para alguém que você nunca conheceu pessoalmente.
- **Não compartilhe seus dados** bancários, senhas, ou informações de documentos (RG, CPF, CNH).
- **Não aceite fotos ou vídeos íntimos** da pessoa, nem envie os seus.
- **Não baixe qualquer aplicativo ou clique em links suspeitos** que a pessoa enviar.
- **Não esconda o relacionamento** de amigos ou familiares.
- **Nunca pagar o resgate aos cibercriminosos**, uma vez que eles certamente manterão os dados e irão extorquir a pessoa novamente depois. O certo é **procurar um advogado** especializado e **fazer a denúncia**.

Furto do Perfil em Redes Sociais



A Invasão ou Apropriação de Perfil é um crime cibernético onde golpistas se **apropriam das suas contas** de redes sociais, como WhatsApp e Instagram. Ao se passarem por você, **eles exploram a confiança de seus amigos e familiares**, inventando histórias de urgência para pedir dinheiro ou outros golpes.

Faça

- **Ative a verificação em duas etapas (MFA):** Este é o passo mais importante. Crie um PIN ou senha exclusivo nos seus aplicativos (WhatsApp, Instagram, etc.). Se alguém tentar invadir sua conta, precisará desse código secreto, mesmo que tenha seu código de acesso inicial.
- **Crie senhas fortes e exclusivas:** Use uma senha diferente para cada rede social e aplicativo
- **Desconfie de links e mensagens estranhas:** Se receber um link, código de acesso ou pedido de informações pessoais por SMS, e-mail ou chat, NUNCA clique ou forneça dados.
- **Configure alertas de login**
- **Fique Atento!**

Não Faça

- **Não compartilhe códigos de verificação:** NUNCA compartilhe o código de 6 dígitos que chega por SMS (para WhatsApp, Instagram, etc.), mesmo que a pessoa diga que "enviou por engano".
- **Não clique em links de promoções suspeitas:** Links recebidos por mensagens diretas (Direct) ou WhatsApp prometendo prêmios, cupons ou sorteios são iscas para se apropriar de suas credenciais.
- **Não aceite pedidos de dinheiro urgentes de contatos online:** Não confie apenas em mensagens de texto, antes de fazer qualquer transferência (Pix), ligue para o seu contato pelo **número antigo** ou se possível encontre pessoalmente para confirmar.

Fui vítima o que fazer agora?



Um golpe virtual é uma armadilha digital, um esquema fraudulento planejado para **manipular e enganar usuários da internet**, visando coletar seus dados pessoais ou acesso a contas, muitas vezes disfarçado de oportunidade, urgência ou assistência, ou até mesmo pedir ou desviar dinheiro.

Faça

- **Faça um Boletim de Ocorrência (B.O.) Online ou Presencial.**
- **Reúna e preserve todas as provas:** Salve capturas de tela (prints), e-mails, mensagens (WhatsApp, Telegram, SMS), extratos bancários, comprovantes de pagamento, links de sites falsos, perfis de redes sociais dos golpistas, tudo que possa comprovar o golpe e a identidade dos criminosos.
- **Contate imediatamente seu Banco/Instituição Financeira:** Se houver perda financeira ou uso indevido de seu cartão/conta, informe seu banco sobre o golpe. Solicite o bloqueio de cartões e a contestação de transações não autorizadas.
- **Altere todas as senhas.**
- **Avise seus contatos.**
- **Procure apoio jurídico:** Consulte um advogado especializado em direito digital

Não Faça

- **Não apague nenhuma prova.**
- **Não sinta vergonha de denunciar:** Lembre-se que você não é culpado(a) e denunciar é a melhor forma de proteger a si mesmo e a outras pessoas.
- **Não tente resolver o problema sozinho com o golpista:** Evite qualquer contato direto com o golpista após descobrir a fraude.
- **Não compartilhe suas informações com mais ninguém:** Apenas com as autoridades legítimas envolvidas no caso.
- **Não desista da denúncia:** O processo de investigação e recuperação pode ser demorado, mas a persistência é fundamental.
- **Nunca pagar o resgate aos cibercriminosos**, uma vez que eles certamente manterão os dados e **irão extorquir você novamente**. O certo é procurar um advogado especializado.