

MANUAL DE SEGURANÇA DIGITAL



ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SANTA CATARINA

NÚCLEO INSTITUCIONAL DE SEGURANÇA



ÍNDICE

ESTAMOS CONECTADOS, E ISSO EXIGE ATENÇÃO!	3
1. GOLPES DIGITAIS: O CENÁRIO NO BRASIL	4
2. QUAIS OS CANAIS MAIS USADOS PELOS GOLPISTAS?	4
2.1. Aplicativo de conversa (whatsapp)	4
2.2. Redes sociais (facebook e instagram)	5
2.3. SMS (mensagens de texto)	6
2.4. Emails	7
2.5. Sites de e-commerce (OLX e Marketplace)	7
2.6. Extorsão virtual	8
2.7. Falso aluguel	9
2.8. Falso precatório/falso advogado	9
2.9. Falso boleto ou guia de pagamento	10
2.10. Golpe da selfie	11
3. MANTENHA SEU APARELHO SEGURO	12
4. FURTO, ROUBO OU EXTRAVIO DE CELULAR	13
5. COMO RECUPERAR A SUA CONTA DE WHATSAPP	14
6. DENUNCIANDO UMA CONTA FAKE DE WHATSAPP	14
7. RECUPERANDO CONTA DO INSTAGRAM	15
8. PROTEGENDO MENORES NO AMBIENTE DIGITAL	15
9. CONTESTANDO UM PIX	16
10. CAIU NO GOLPE? COMUNIQUE A POLÍCIA!	17
11. SOUBE DE ALGUMA AÇÃO CRIMINOSA? DENUNCIE!	17
12. CONCLUSÃO	18
13. LINKS ÚTEIS	19
14. ANEXOS	20

ESTAMOS CONECTADOS, E ISSO EXIGE ATENÇÃO!

Vivemos em uma era de conectividade sem precedentes. Desde simples trocas de mensagens até acessos a contas e transações bancárias, praticamente todos os aspectos de nossa rotina passam pelos meios digitais. Essas novas dinâmicas tornam a vida mais prática, entretanto também têm seus riscos, por deixar todos mais expostos.

Os meios digitais nos conectam e facilitam a nossa vida, mas também são palco de golpes diversos, como criação de falsos perfis de redes sociais, emails fraudulentos e links maliciosos. Em diversos casos, os criminosos não precisam sequer invadir sistemas ou terem maiores habilidades nos meios digitais, bastando que as vítimas forneçam ou proporcionem acesso a informações sensíveis ou ainda que cliquem em links suspeitos, para que tenham seus dados acessados e utilizados em práticas criminosas, o que pode gerar grandes prejuízos.

Ninguém está isento das ameaças existentes na internet e nos meios digitais. Até mesmo grandes empresas multinacionais, que contam com sofisticados recursos de segurança, já chegaram a ficar com suas plataformas fora do ar por vários dias, após ataques hackers que comprometeram servidores digitais e expuseram vulnerabilidades, colocando milhares de usuários em risco.

O Núcleo Institucional de Segurança da Assembleia Legislativa de Santa Catarina (NIS – ALESC) desenvolveu esse manual com um único objetivo: proteger você. Parlamentares, servidores e cidadãos em geral fazem uso das redes e meios digitais permanentemente, portanto estão igualmente sujeitos aos riscos neles existentes. Aqui você saberá mais detalhes sobre os golpes mais comuns, encontrará orientações, exemplos, e, sobretudo dicas confiáveis para não cair nas armadilhas digitais.



1 - GOLPES DIGITAIS: O CENÁRIO NO BRASIL

No ano de 2024, mais de 281 mil casos de estelionato digital foram registrados no Brasil, o que representa um aumento de 17% com relação ao ano anterior. Aproximadamente 25% da população brasileira já foi vítima de algum tipo de golpe virtual.

Esses criminosos geralmente se utilizam de engenharia social, descobrindo informações pessoais do alvo, onde as abordagens geralmente manipulam psicologicamente as vítimas, envolvendo sempre urgência, medo ou vantagens, sempre no intuito de induzi-las a atos impulsivos, cliques, compartilhamentos ou transferências.

Por essas e outras razões, é importante estar atento, sabendo identificar, evitar e também contornar essas situações que se fazem cada vez mais freqüentes.

2 - QUAIS OS CANAIS MAIS USADOS PELOS GOLPISTAS?

Os meios digitais com maior incidência de atuação dos golpistas são:

2.1. Aplicativos de conversa (whatsapp);

Como funciona?

Golpes com falsificação de identidade: é comum que pessoas que tentam aplicar golpes finjam ser um amigo ou familiar para levar a vítima a compartilhar informações pessoais, fazer depósitos, transferências ou pagar boletos. Esses criminosos também podem se passar por figuras públicas, autoridades, celebridades ou empresas conhecidas.

O que fazer?

Se uma mensagem parecer suspeita ou boa demais para ser verdade, não toque ou clique nela, não a compartilhe nem encaminhe. Caso alguém envie mensagens com foto de alguma pessoa conhecida, mas com número diferente, tente fazer contato com o verdadeiro número pra falar com ela e confirmar.

2.2. Redes sociais (facebook e instagram);

Nas redes sociais são comuns tentativas de enganar as vítimas para obter vantagem financeira, dados ou mesmo o acesso à conta. O golpista se disfarça de amigo, marcas famosas ou influenciadores para parecer confiável, na intenção de convencer a vítima a clicar em links, enviar informações ou fazer pagamentos.

O golpista faz uso de mensagens bem redigidas, histórias emocionantes ou promoções atraentes para manipular quem está do outro lado da tela. Essa tática se chama engenharia social, e o objetivo é sempre o mesmo: fazer a pessoa agir rápido, sem pensar.

Por isso é importante manter a atenção e desconfiar de qualquer coisa fora do comum, tipo uma vantagem fora do normal ou uma suposta “oportunidade única”.

O que fazer?

Desconfie de qualquer perfil que desativa os comentários. Esse é um dos maiores indicativos de possível golpe; se os comentários estão desativados, possivelmente o golpista esteja tentando evitar que outras pessoas alertem novas vítimas. As grandes marcas e perfis confiáveis em geral, mantêm os comentários abertos como forma de transparência.

Links curtos, sem contexto, enviados por contas desconhecidas ou até por amigos agindo de forma "estranha" — podem levar a páginas falsas que roubam suas senhas ou instalam vírus ou programas espões no seu dispositivo. Sempre confirme a origem antes de clicar.

Desconfie de pedidos de dinheiro ou promoções milagrosas.

Se alguém pedir pix, depósito, ou transferência urgente (geralmente para contas de terceiros), oferecer algum investimento com lucro garantido ou prometer prêmios ou vantagens exageradas, desconfie. Golpistas usam essas “iscas” para gerar pressão e fazer a vítima agir sem pensar, com pressa ou urgência. Se essa oferta vier de um conhecido no instagram ou facebook, antes de tomar qualquer atitude, entre em contato pessoalmente ou por telefone e pergunte se a conta dele foi invadida.

Use senhas fortes e diferentes para cada rede.

Evite usar a mesma senha para redes sociais, e-mail e outros serviços. Dê preferência para senhas fortes, com combinações longas, com letras maiúsculas, minúsculas, números e símbolos. Essa medida reduz as chances de sua conta ser invadida caso aconteça um vazamento.

Denuncie perfis suspeitos no próprio instagram: ao identificar uma conta que pode estar aplicando golpes, denuncie diretamente na plataforma, isso ajuda a alertar outros usuários e aumenta a chance do perfil ser removido.

2.3. SMS (mensagens de texto);

Como funciona?

Nesta modalidade, a vítima recebe um SMS onde o golpista reporta situações como milhas prestes a expirar, compras em análise, etc. Normalmente o SMS traz um link para a vítima clicar e ter seu dispositivo invadido, ou ainda um telefone de contato de uma falsa central telefônica, onde também serão solicitados dados sensíveis da vítima para a prática de crimes.

O que fazer?

Ao receber mensagens desta natureza, evite clicar nos links recebidos, assim como não ligue para os telefones ali indicados. Na dúvida entre no site oficial da empresa ou banco para conferir os canais oficiais de contato dos mesmos.

2.4. Emails;

Como funciona?

A vítima recebe um falso email, onde é induzida a clicar em um link/botão que dará acesso aos dados do seu celular ou computador. Nesta modalidade algumas práticas comuns são: falso email do DETRAN relatando problemas na CNH da vítima, falsa intimação do Poder Judiciário informando decisão judicial ou intimação, falso email da Receita Federal onde reportam problemas de IR ou com o CPF, falsa intimação policial, etc.

O que fazer?

Ao receber emails suspeitos, procure verificar se o remetente se trata mesmo do órgão oficial. Se persistirem dúvidas, você pode consultar seus dados no site do órgão. Na dúvida, evite clicar em links ou redirecionamentos que estão no email suspeito. Tente de outra maneira entrar em contato com o órgão oficial para realizar consultas.

2.5. Sites de e-commerce (OLX e Marketplace);

Como funciona?

A vítima anuncia um produto em sites de compra e venda, onde insere o seu número de contato. O golpista, se fazendo passar por funcionário do site, entra em contato com a vítima e pede um código enviado a ela pra “validar” o anúncio.

O código informado se trata do código de autenticação do whatsapp da vítima, o qual foi previamente solicitado pelo golpista.

O que fazer?

Evite colocar o seu contato no anúncio. Os aplicativos/sites de compra e venda possuem chats para comunicação segura entre usuários. Quando for efetuar a negociação, se certifique de estar realmente tratando com a pessoa interessada, e não com intermediários. Ao marcar um encontro, procure combinar em local público e seguro.

2.6. Extorsão virtual;

Como funciona?

Esse golpe geralmente tem início através de redes sociais, sites de relacionamento ou jogos on-line, onde criminosos se utilizam de perfis falsos e técnicas de engenharia social para se aproximarem das vítimas. Usando fotos atraentes e com conversas sedutoras, criam um ambiente de intimidade com a vítima, convencendo-a a trocar imagens íntimas. Ao estarem de posse do material enviado, os criminosos passam a chantageá-la, exigindo valores para não divulgar as imagens enviadas e o conteúdo das conversas a familiares ou nas redes sociais.

Neste golpe também é comum que outro perfil entre em contato se passando por policial e afirmando que a vítima estava trocando material pornográfico com uma menor de idade, e propõe fazer um “acordo” pra não dar início a uma investigação.

O que fazer?

Evite compartilhar conteúdo íntimo, e se vier a cair no golpe, não deixe de registrar o boletim de ocorrência e de procurar ajuda. Bloqueie o perfil criminoso, denuncie e não faça qualquer tipo de pagamento.

2.7. Falso aluguel;

Como funciona?

Criminosos anunciam a locação de um imóvel, geralmente com valores abaixo do mercado, utilizando os dados e imagens de outro anúncio verdadeiro. As vítimas fazem contato e realizam a negociação, onde os golpistas pedem pagamento adiantado e fora das plataformas oficiais, alegando geralmente a existência de outros interessados, o que desperta o sentimento de urgência na vítima, que não toma as devidas cautelas. Os criminosos geralmente indicam a conta de um “laranja” para pix ou depósito. Após receberem os valores, os golpistas retiram o anúncio e bloqueiam as vítimas, impedindo qualquer novo tipo de contato.

O que fazer?

O ideal é procurar agentes imobiliários confiáveis e estabelecidos no mercado, ou optar por plataformas que oferecem mecanismos de segurança para evitar prejuízos tanto ao locador como ao locatário. Importante estar atento e desconfiar de anúncios com valores abaixo dos praticados no mercado, e de anunciantes que queiram realizar a negociação de forma muito rápida.

Caso venha a cair no golpe, procure uma delegacia de polícia para registrar o boletim de ocorrência, levando todas as informações, como onde viu o anúncio, algum eventual telefone utilizado pelo golpista, conta onde foi efetuado o depósito, etc.

2.8. Falso precatório/falso advogado;

Como funciona?

A vítima é procurada pelos criminosos, os quais se fazem passar por advogados ou serventuários do Poder Judiciário, informando o suposto resultado de um processo judicial (que realmente existe) onde esta teria valores a receber.



Para receber o montante, informam a necessidade de pagamento de custas pra liberação desses valores. Os golpistas indicam contas de “laranjas” para depósitos, e após estes serem realizados, desaparecem deixando a vítima no prejuízo.

O que fazer?

Procure falar pessoalmente ou ligar no telefone do escritório do seu advogado, para se certificar da veracidade da informação, ou ainda consultar o processo em questão no site do Poder Judiciário.

Caso venha a cair no golpe, procure uma delegacia de polícia para registrar o boletim de ocorrência, levando todas as informações, como o telefone utilizado pelo golpista, conta onde foi efetuado o depósito, etc.

2.9. Falso boleto ou guia de pagamento;

Como funciona?

Geralmente os criminosos enviam por email, por SMS ou pelo whatsapp um boleto falso, muito similar aos verdadeiros, inclusive contendo dados da vítima.

Julgando estar recebendo um boleto legítimo, a vítima efetua o pagamento e o valor é encaminhado aos criminosos. Esse golpe ocorre porque de alguma forma os golpistas tiveram acesso a dados financeiros da vítima, e encaminham o boleto semelhante aos que ela está acostumada a pagar.

O que fazer?

Ao receber boletos em canais atípicos, sempre procurar conferir os dados do mesmo. Ao receber por email, procure verificar se o remetente realmente é o seu banco ou a instituição emitente.

Se vier a cair no golpe, faça o boletim de ocorrência on-line ou procure uma delegacia de polícia para registrar, levando todas as informações que tiver sobre o caso. Procure o seu gerente do banco com urgência pra tentar estornar a transação.

2.10. Golpe da selfie;

Como funciona?

Criminosos se fazem passar por bancos ou empresas e solicitam às vítimas o envio de uma selfie para atualização cadastral ou confirmação de identidade. A finalidade dos golpistas é posteriormente se fazer passar pela vítima em sistemas de reconhecimento facial e acessar contas. Com a simples imagem enviada, os golpistas podem acessar contas bancárias da vítima, fazer transações como pix ou transferências, solicitar empréstimos ou até mesmo abrir novas contas com os seus dados. A imagem pode ainda ser utilizada para criação de perfis falsos nas redes sociais.

O que fazer?

Desconfie de contatos solicitando fotos para desbloqueio de contas, não encaminhe fotos, documentos ou informações sensíveis pelo whatsapp, SMS ou redes sociais, tenha habilitada a verificação em duas etapas nos aplicativos que envolvam transações financeiras.

Se for vítima desta modalidade, bloqueie suas contas e cartões, comunique o banco solicitando o cancelamento das operações e registre o boletim de ocorrência.



3 - MANTENHA SEU APARELHO SEGURO

O telefone celular representa hoje, além de um meio de comunicação, uma importante ferramenta para a resolução de várias demandas. Porém, caso esse aparelho seja perdido, furtado ou roubado, pode gerar transtornos e prejuízos diversos ao seu proprietário. É importante que você mantenha em local seguro as informações identificadoras do seu aparelho, a fim de facilitar registros e cancelamentos caso isso seja necessário.

Guarde em local seguro e acessível os dados gerais como marca, modelo, numero de série e IMEI (encontrados geralmente na nota fiscal ou na caixa do produto).

Tenha senhas personalizadas e não genéricas, para que outra pessoa não consiga desbloquear seu aparelho facilmente.

Mantenha a verificação em 2 etapas habilitada na sua conta de whatsapp.

Procure utilizar recursos de segurança como leitor de impressões digitais e reconhecimento facial para desbloqueio do aparelho.

Deixe ativado o código pin do chip, isso impedirá que seu chip possa ser utilizado em outro aparelho em caso de perda, furto ou roubo.



4 - FURTO, ROUBO OU EXTRAVIO DE CELULAR

Quais providências tomar?

Caso você tenha o celular perdido ou subtraído de alguma forma, siga as dicas abaixo a fim de evitar que terceiros possam ter acesso aos seus dados, contas, ou mesmo efetuar transações ou contatos se passando por você:

Comunique a sua operadora acerca do fato e solicite o bloqueio do chip para impedir o uso da linha por terceiros;

Providencie o cancelamento dos métodos de pagamento associados ao aparelho, como cartões de crédito, contas bancárias, Apple Pay, Google Pay, Paypal;

Faça o registro da ocorrência pela internet ou na Delegacia de Polícia mais próxima, informando os dados do aparelho, como IMEI, número de série, marca e modelo;

Desvincule o aparelho de suas contas pessoais como e-mail, redes sociais e demais aplicativos;

Acesse o site ou aplicativo Celular Seguro, <https://www.gov.br/ptbr/apps/celular-seguro-br> ou <https://celularseguro.mj.gov.br/> e faça o bloqueio total do seu aparelho.

5 – COMO RECUPERAR A SUA CONTA DE WHATSAPP

- Registrar o boletim de ocorrência (pode ser on line);
- Avisar aos contatos e familiares sobre o ocorrido;
- Fazer contato com a operadora para bloquear o chip/sim card;
- Mandar email para support@whatsapp.com para pedir a desativação da conta;
- Reinstalar o aplicativo, já com um novo chip, para receber um novo código de verificação via SMS;

6 – DENUNCIANDO UMA CONTA FAKE DE WHATSAPP

Caso uma conta fake (se fazendo passar por alguém) venha a fazer contato com você, é possível fazer a denúncia no próprio aplicativo para excluí-la. Na própria conversa clique no número e ao abrir a tela de opções deslize até a opção DENUNCIAR.

Se for uma conta falsa usando seus dados pessoais, faça o boletim de ocorrência e encaminhe email para support@whatsapp.com com o assunto “remover/excluir conta” adicionado do número fake, e no corpo do email explique que a conta está usando sua imagem e seus dados sem permissão, solicitando a remoção do perfil.

7 – RECUPERANDO CONTA DO INSTAGRAM

Saia do aplicativo instagram em todos os dispositivos;

Entre novamente no aplicativo, coloque o nome de usuário e em seguida clique na opção “esqueceu a senha?”;

Clique na opção “precisa de mais ajuda?”;

O aplicativo apresentará o email ou telefone vinculado à sua conta e, a partir de então, dará as instruções de recuperação;

Se você não reconhecer o email ou telefone apresentado, clique em “não consigo acessar este email ou número de telefone”, em seguida, marque a opção “minha conta foi invadida”, selecionando na tela seguinte “sim, eu tenho uma foto na minha conta”;

Digite seu email no espaço indicado, e ao clicar em “enviar”, você receberá um código de confirmação no respectivo email;

Na sequência, você receberá um comando para tirar uma selfie para confirmação da sua identidade e recuperação da conta;

Após a selfie, siga as indicações e você receberá um link no email para a recuperação da conta invadida.

8 - PROTEGENDO MENORES NO AMBIENTE DIGITAL

A internet proporciona muitas oportunidades de ensino e diversão para crianças e adolescentes, mas é importante que os responsáveis adotem medidas preventivas a fim de evitar que os menores sejam expostos a riscos nas redes. Confira dicas básicas e de suma importância:

Eduque e oriente os menores sobre o que é apropriado na internet. Ressalte a importância de evitar excesso de exposição da imagem e informações pessoais, contatos com pessoas desconhecidas e sempre verifique a confiabilidade dos sites acessados;

Use controles parentais, que são mecanismos de monitoramento das atividades dos dispositivos, que permitem filtrar os conteúdos acessados, bloquear sites perigosos ou inadequados, bem como determinar o tempo de acesso às redes pelos menores;

Oriente sobre a necessidade da privacidade no ambiente virtual, alertando sobre os riscos de compartilhamento de dados pessoais e sensíveis, como nome, endereço, escola e telefone, e procure manter um diálogo aberto para que as crianças se sintam seguras ao relatar qualquer situação incômoda, falar sobre o conteúdo que acessam, e questionar acerca de eventuais dúvidas;

Procure observar possíveis sinais de cyberbullying, incentive os menores a falarem sobre situações inadequadas e sempre denunciarem qualquer tipo de assédio online.

9 - CONTESTANDO UM PIX

Em casos de fraudes, golpes ou coerção, o usuário tem a possibilidade de acionar o Mecanismo Especial de Devolução (MED), disponível no aplicativo de bancos e instituições financeiras.

No ato da contestação da transação, o banco do golpista bloqueará os valores da conta até a resolução da demanda.

Através do aplicativo, o usuário poderá, no ato da contestação, adicionar provas da ação criminosa.

Após o valor ser bloqueado, os bancos envolvidos terão um prazo de sete dias para analisar o pedido.

O serviço não se aplica a desacordos comerciais, arrependimentos em compras ou digitações equivocadas, servindo apenas para vítimas das ações criminosas acima citadas.

10 - CAIU NO GOLPE? COMUNIQUE A POLÍCIA!

Se você foi vítima de qualquer tipo de golpe, estando ele ou não descrito neste manual, procure imediatamente comunicar a Polícia. Isso pode ser feito pessoalmente em uma Delegacia, ou ainda através do site www.delegaciavirtual.sc.gov.br.

11- SOUBE DE ALGUMA AÇÃO CRIMINOSA? DENUNCIE!

Caso você tome conhecimento de alguma ação criminosa, ou ainda do paradeiro de algum criminoso foragido, denuncie! A sua identidade será mantida em total sigilo, e você estará colaborando com o trabalho das forças de segurança.

Há três maneiras de se realizar as denúncias à Polícia Civil, através do site www.delegaciavirtual.sc.gov.br clicando em “comunicar central de denúncias”, pelo disque-denúncia no número 181 ou ainda através do whatsapp (48) 98844-0011, lembrando que em todos os canais as informações são confidenciais e a identidade do denunciante será preservada.

12 - CONCLUSÃO

Diversos são os artifícios utilizados pelos criminosos para acessar dados e obter vantagens financeiras através dos canais digitais.

Cabe aos usuários ficarem cada vez mais atentos, uma vez que os golpistas estão sempre desenvolvendo novas técnicas de crimes a serem perpetrados pelas redes e meios virtuais.

Sendo assim, é recomendável proceder sempre com cautela ao se deparar com publicações, emails ou links duvidosos.

A segurança nos meios digitais não depende apenas da tecnologia, mas principalmente das atitudes do usuário. Vários são os tipos de golpes existentes, e cada vez eles tomam novas roupagens. Por isso a atenção e o cuidado em operações financeiras e no uso das redes são imprescindíveis.

Este material foi elaborado com o objetivo de alertar acerca dos golpes e fraudes virtuais mais usados atualmente e, também, fornecer orientações para uso seguro da internet e alguns mecanismos de reversão para eventuais vítimas.

O Núcleo Institucional de Segurança da Assembleia Legislativa (NIS – ALESC) reitera que está à disposição para ações preventivas e reativas no que diz respeito a essas práticas criminosas, estando os contatos para acionamento abaixo elencados.

NÚCLEO INSTITUCIONAL DE SEGURANÇA – NIS

Fone (48) 3221-2780 - Email nis@alesc.sc.gov.br

Unidade Administrativa – Av. Mauro Ramos, 300, Sala 305



13 – LINKS ÚTEIS

O GOLPE ESTÁ AÍ - POLÍCIA CIVIL -SC

https://pc.sc.gov.br/?page_id=71

CARTILHA DE SEGURANÇA CIBERNÉTICA - TJ-SC

[https://www.tjsc.jus.br/documents/66294/2623449/cartilha+seguran %C3%A7a+cibern%C3%A9tica/c0f12308-4fff-f3df-2684-aa-51c5df0d33](https://www.tjsc.jus.br/documents/66294/2623449/cartilha+seguran+%C3%A7a+cibern%C3%A9tica/c0f12308-4fff-f3df-2684-aa-51c5df0d33)

CARTILHA FUNDAÇÃO ABRINQ – MENORES NA INTERNET

<https://www.fadc.org.br/noticias/proteger-criancas-internet>

PHISHING E OUTROS GOLPES

<https://cartilha.cert.br/fasciculos/phishing-golpes/fasciculo-phishinggolpes.pdf>

14. ANEXOS

MODELO DE GOLPE VIA E-MAIL Phishing - Proposta imperdível



ATENÇÃO: Seu processo está a reta final! Ação necessária 3:49:25 AM

De ALERTA_IMEDIATO <protocolo@protocolo.dealhonoseuprcss.site>

Data Sab, 26/07/2025 11:05

Para voceusuario@gmail.com <voceusuario@gmail.com>

Assunto: Olá, <voceusuario>! Você foi selecionado para solicitar um American Express Business Black ! Identificação: 12804273.

Convite Exclusivo: American Express® Black

Experiência premium com benefícios globais

...**você recebeu um convite especial.**

Com base no seu perfil, você pode solicitar o **American Express Black** e acessar um conjunto de **benefícios exclusivos** no Brasil e no exterior.

- ✓ Acesso a Salas VIP (programas parceiros e convites exclusivos)
- ✚ Acúmulo de pontos para viagens, upgrades e experiências
- ✚ Vantagens em hotéis selecionados (early check-in, late check-out, upgrades conforme disponibilidade)
- ✚ Concierge 24h para reservas, roteiros e assistência internacional
- ✚ Seguros e proteção em viagens e compras qualificadas

Solicitar Convite

Convite nº: 53620717 — válido por tempo limitado

Sujeito à análise e elegibilidade. Benefícios podem exigir ativações em programas parceiros e variar conforme condições vigentes.

Esta mensagem foi gerada automaticamente.
Em caso de dúvidas, acesse os canais oficiais do Bradesco e American Express.



MODELO DE GOLPE VIA E-MAIL

Phishing - Falsa urgência e ameaça



ATENÇÃO: Seu processo está a reta final! Ação necessária 3:49:25 AM

De ALERTA_IMEDIATO <protocolo@protocolo.deolhonoseuprccss.site>

Data Sab, 26/07/2025 11:05

Para voceusuario@gmail.com <voceusuario@gmail.com>

ÚLTIMA INSTÂNCIA - SEU PROCESSO TRABALHISTA

Prezado(a) cliente, informamos que seu processo trabalhista está na **última instância** e requer uma verificação de sua parte. Além disso, a audiência está marcada para uma data próxima, sendo crucial que você verifique suas informações o quanto antes.

ATENÇÃO! A audiência acontecerá em breve. Por favor, não deixe para última hora.

Data da Audiência: 7 de agosto de 2025

Hora da Audiência: 14:00 (horário de Brasília)



MODELO DE GOLPE VIA E-MAIL

Fraudes envolvendo seu CPF



Olá, voceusuario! gov.br: Governo Federal: Iniciado processo de cancelamento de CPF!
Autenticação: 70942587. - Verifique Agora> Seu CPF possui restrição grave! - Cancelamento do
CPF em andamento: Consulte os problemas relacionados agora! - Receita...

De Receita Federal - Tributos <situacao@receitafederal.gov.br>

Data Qua, 23/07/2025 15:06

Para voceusuario@gmail.com <voceusuario@gmail.com>



MINISTERIO DA FAZENDA
RECEITA FEDERAL

NOTIFICAÇÃO OFICIAL

Sistema de Administração Tributária Nacional

IRREGULARIDADE DETECTADA NO CPF

Informação de Irregularidade

Prezado(a) voceusuario@gmail.com,

Informamos que foi detectada uma **irregularidade fiscal** relacionada ao seu Cadastro de Pessoa Física (CPF) junto à Receita Federal do Brasil.

Status atual: Restrição Ativa

Protocolo: RFB-9257001

Data de detecção: 28/04/2025

Natureza: Pendência de Declaração e Inconsistência Cadastral

Situação: Em processo de suspensão

Consequências da não regulamentação:

- Bloqueio completo do CPF
- Suspensão de benefícios governamentais
- Restrições em operações bancárias e financeiras
- Inclusão em cadastros de inadimplência (SPC/SERASA)

Atenção: A atual legislação determina que cadastros com irregularidades não sanadas serão automaticamente suspensos e poderão ser cancelados definitivamente.



MODELO DE GOLPE VIA E-MAIL DETRAN - CNH SUSPENSA/INFRAÇÃO



DETRAN: URGENTE! CNH esta temporariamente suspensa. ID: 57476036

De Consulta Detran <processo969983@detran>

Data Seg, 23/06/2025 18:45

Para voceusuario@gmail.com <voceusuario@gmail.com>



Aviso de infração de Trânsito

Identificação vinculada à sua CNH (Carteira Nacional de Habilitação)

Detalhes da infração:

Prezado(a) voceusuario@gmail.com

ATENÇÃO: Foi identificada uma infração grave vinculada à sua CNH que não foi regularizada dentro do prazo estipulado pelo DETRAN. Se não for resolvida até a data indicada abaixo, sua CNH poderá ser suspensa permanente

Status da infração: VENCIDA

Para evitar a suspensão da sua CNH, regularize a pendência o mais rápido possível. O processo é rápido e simples

[Clique aqui para regularizar agora](#)

Este e-mail foi enviado pelo sistema integrado de multas do DETRAN
2025 Carteira Digital de Trânsito (CDT)



Aponte para o QR Code abaixo e acompanhe o site da Alesc para conhecer iniciativas, campanhas e leis que contribuem para a proteção dos cidadãos.



Nos siga também nas redes sociais:

/assembleiasc

