INVESTINDO NO AZUL

PROGRAMA DE EDUCAÇÃO FINANCEIRA DO COMANDO DA AERONÁUTICA

CUIDADOS COM AS FRAUDES ONLINE

FIQUE ATENTO!

Mais de

7 milhões

de brasileiros

foram vítimas de golpes financeiros no último ano.

Mais de

R$ 551 milhões

em prejuízos

Mais de

R$ 5 bilhões

valor das tentativas de fraudes

GOLPE DA FALSA CENTRAL DE ATENDIMENTO

Neste golpe, um indivíduo que se apresenta como um funcionário da central de atendimento entra em contato com você. Eles podem alegar ser da sua instituição financeira, da loja onde você realiza compras ou de qualquer outra empresa com a qual você tenha vínculo.

O contato geralmente é feito de maneira alarmante, alegando que há um problema sério com sua conta ou que foi detectada uma transação suspeita, e que é necessário agir imediatamente para resolver a questão. Em seguida, eles podem utilizar suas informações para esvaziar sua conta ou fazer compras com seu cartão.

No caso do SMS, ele pode simular uma tentativa de compra recusada e fornecer um número de telefone para você ligar. No entanto, esse número é falso e redireciona sua ligação diretamente para os golpistas.

SAIBA COMO SE PROTEGER:

•Nunca forneça dados pessoais.
•Desconfie de chamadas que exigem ações urgentes.
•Fique atento a links suspeitos que parecem atualizações.
•Lembre-se de que nenhum banco solicita informações pessoais por telefone.
•Se algo parecer suspeito, desligue imediatamente.

GOLPE DO LINK FALSO

O phishing, também conhecido como "pescaria digital," é uma fraude eletrônica que tem como objetivo obter senhas e dados pessoais dos usuários. Os ataques de phishing frequentemente ocorrem por meio de mensagens enviadas por e-mail, SMS, aplicativos de mensagens como WhatsApp, ou redes sociais, que tentam induzir o usuário a clicar em links maliciosos. Além disso, existem sites falsos que enganam as pessoas para que revelem suas senhas e informações pessoais.

Os casos mais comuns de phishing incluem e-mails que parecem ser de bancos, alegando que há um problema com a conta do cliente, que o cartão excedeu o limite, que é necessário atualizar o token, ou que há um novo software de segurança do banco que precisa ser instalado imediatamente.

O Brasil é um dos países com maior incidência desse tipo de crime.

SAIBA COMO SE PROTEGER:

•Fique atento a erros de ortografia e gramática, ou a ofertas que parecem boas demais para ser verdade.
•Desconfie de mensagens que criam um senso de urgência ou que fazem ameaças caso você não siga as instruções.
•Verifique o endereço da URL, que pode ser semelhante ao de sites legítimos, mas com pequenas diferenças.
•Copie o texto e faça uma pesquisa em um mecanismo de busca confiável.

GOLPE VIA WHATSAPP

Em um dos golpes mais comuns, o criminoso se faz passar por funcionário de um banco, loja ou empresa e oferece alguma vantagem ou serviço. Ele avisa que enviará um código para confirmação, mas, na realidade, esse código é o de verificação do seu WhatsApp. Se você compartilhar esse código, sua conta pode ser clonada, permitindo que o golpista acesse seus contatos e peça dinheiro em seu nome.

Outro golpe frequente envolve a criação de um perfil falso, onde o criminoso usa fotos e informações de redes sociais para se passar por um amigo ou familiar seu, alegando ser o novo número dessa pessoa. Em seguida, ele inventa uma situação de emergência, como uma doença, uma necessidade financeira ou um acidente, para persuadi-lo a transferir dinheiro.

SAIBA COMO SE PROTEGER:

- Ative a “verificação em duas etapas” no WhatsApp.
- Nunca compartilhe o código de verificação recebido por SMS.
- Evite clicar em links suspeitos ou desconhecidos.
- Verifique a informação entrando em contato através dos canais oficiais.
- Mantenha um antivírus confiável instalado no seu dispositivo móvel

GOLPES APÓS ROUBO OU FURTO DE CELULAR

Antigamente, o furto de celular geralmente tinha como objetivo apenas o aparelho em si. Atualmente, o interesse dos criminosos está no que você armazena no dispositivo, como aplicativos bancários, que podem ser usados para realizar transações indevidas, causando prejuízos e muita preocupação.

SAIBA COMO SE PROTEGER:

•Utilize uma senha robusta ou um código de bloqueio para proteger seu celular.
•Não acesse o aplicativo do seu banco em dispositivos de terceiros.
•Mantenha-se atento quando estiver na rua.
•Evite se distrair ao digitar ou tirar fotos em público.
•Não deixe sua conta de e-mail conectada.
•Anote o número IMEI do seu aparelho para registro em caso de perda ou roubo.

GOLPES COM CARTÕES

Apesar dos vários mecanismos de segurança e das novas tecnologias, os métodos de pagamento ainda estão sujeitos a fraudes. Indivíduos mal-intencionados tentam enganar os clientes das instituições financeiras, fazendo com que eles revelem seus dados sem perceber.

Se a maquininha de cartão estiver com o visor quebrado, fique atento! O golpista pode alegar que a tela está com defeito e sugerir que você verifique o valor da compra pelo aplicativo do celular dele. Na realidade, o valor registrado na maquininha pode ser muito maior do que o mostrado no celular.

Além disso, golpistas que atuam como vendedores podem observar quando você digita sua senha na máquina e, ao devolver seu cartão, trocá-lo por outro. Com o seu cartão e senha, eles realizam compras à sua custa.

SAIBA COMO SE PROTEGER:

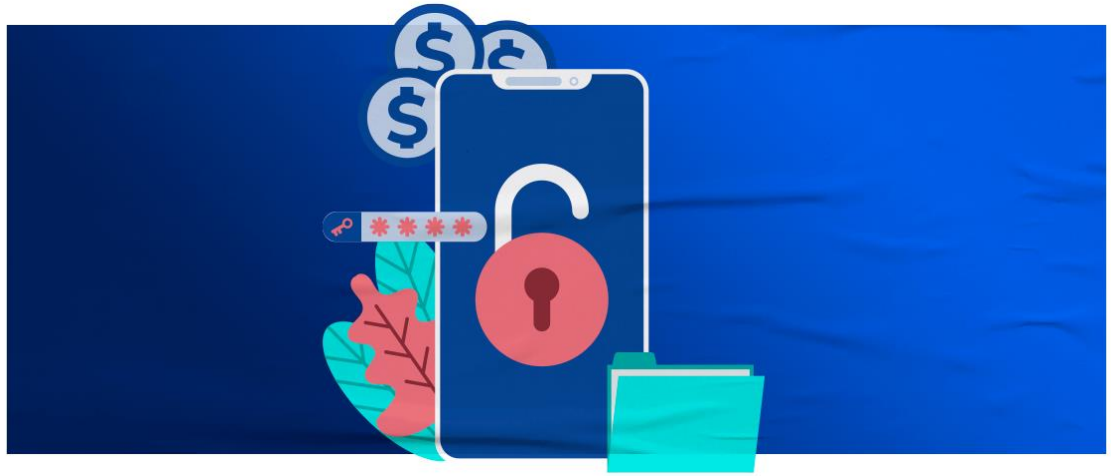
- Utilize cartões virtuais para compras online.
- Se o visor da maquininha estiver quebrado ou com defeito, recuse-se a realizar o pagamento.
- Fique atento se os números da sua senha ficarem visíveis na tela, o que pode ser um sinal de clonagem.
- Nunca compartilhe informações do seu cartão de crédito.
- Evite realizar transações bancárias em redes Wi-Fi públicas.
- Ao descartar seu cartão, corte o chip em pedaços.

GOLPE DA PORTABILIDADE

Imagine a situação: no dia em que o salário é depositado, todos recebem o pagamento, menos você. Ao consultar o RH, você descobre que o valor foi transferido para uma conta com seu nome, mas não é a conta que você usa habitualmente.

Isso é um caso de estelionato.

Nesse tipo de golpe, os criminosos utilizam dados e documentos da vítima para abrir uma conta em outro banco e solicitar a portabilidade do salário. Esse processo pode ser feito diretamente através do aplicativo do banco.



SAIBA COMO SE PROTEGER:

•Proteja suas informações pessoais online: não permita que estranhos acessem seu celular ou computador, sempre encerre a sessão ao sair de e-mails e redes sociais, limpe seu histórico de navegação e mantenha seu dispositivo seguro contra ataques virtuais.
•Evite clicar em links suspeitos e não forneça seus dados pessoais.
•Desconfie de mensagens que solicitem confirmação de suas informações pessoais.
•Utilize o site Registrato, do Banco Central, para acompanhar as movimentações bancárias realizadas em seu nome.
•Tenha cuidado com as informações que compartilha nas redes sociais, como detalhes sobre sua rotina, endereço, CPF e senhas.

GOLPE DO FALSO EMPRÉSTIMO

As quadrilhas criam sites falsos que se passam por instituições financeiras e fazem anúncios oferecendo crédito com condições muito vantajosas na internet. Quando alguém interessado preenche o cadastro nesses sites, os criminosos entram em contato e enviam um contrato fictício, repleto de multas para desencorajar desistências. Para liberar o falso empréstimo, eles exigem o pagamento de taxas e impostos.

SAIBA COMO SE PROTEGER:

•Se você não solicitou uma proposta de empréstimo, pergunte por que o contato foi feito.
•Desconfie de ofertas com juros significativamente abaixo da média do mercado.
•Procure empresas de crédito com uma boa reputação.
•Entenda que nenhuma instituição financeira séria solicita pagamento de taxas ou depósitos antecipados como garantia.
•Fique atento a anúncios suspeitos e nunca forneça informações pessoais, como documentos, comprovantes de renda, endereço, dados bancários ou selfies com RG e CPF.
•Utilize o site Registrato, do Banco Central, para monitorar as movimentações bancárias em seu nome.

GOLPE DO BOLETO FALSO

O fraudador por trás do boleto falso pode ter acesso a diversas informações pessoais da vítima, tornando a situação bastante convincente. O boleto pode ser enviado como uma falsa correspondência bancária ou de uma loja, ou ainda em formato eletrônico, por meio de mensagens de SMS, WhatsApp ou e-mail que direcionam para páginas falsas onde o documento falso pode ser baixado. Os boletos falsificados são muito semelhantes aos originais que a vítima costuma receber. Quando a vítima paga um boleto adulterado, o dinheiro vai para a conta do golpista em vez de para o verdadeiro credor, que pode continuar fazendo cobranças ou não entregar o produto.

SAIBA COMO SE PROTEGER:

•Verifique os detalhes do boleto e avalie se a cobrança é realmente válida antes de efetuar o pagamento.
•Confirme se a sequência numérica do código de barras corresponde àquela na parte superior do boleto.
•Certifique-se de que os três primeiros dígitos representam o código do seu banco.
•Compare o valor total do código de barras com o valor especificado no documento.
•Confira se o boleto está em seu nome e se está escrito corretamente.
•Desconfie de e-mails de remetentes desconhecidos, com erros de português ou de digitação; empresas legítimas geralmente utilizam domínios próprios e personalizados.
•Emita o boleto diretamente pelo site ou aplicativo oficial da instituição.