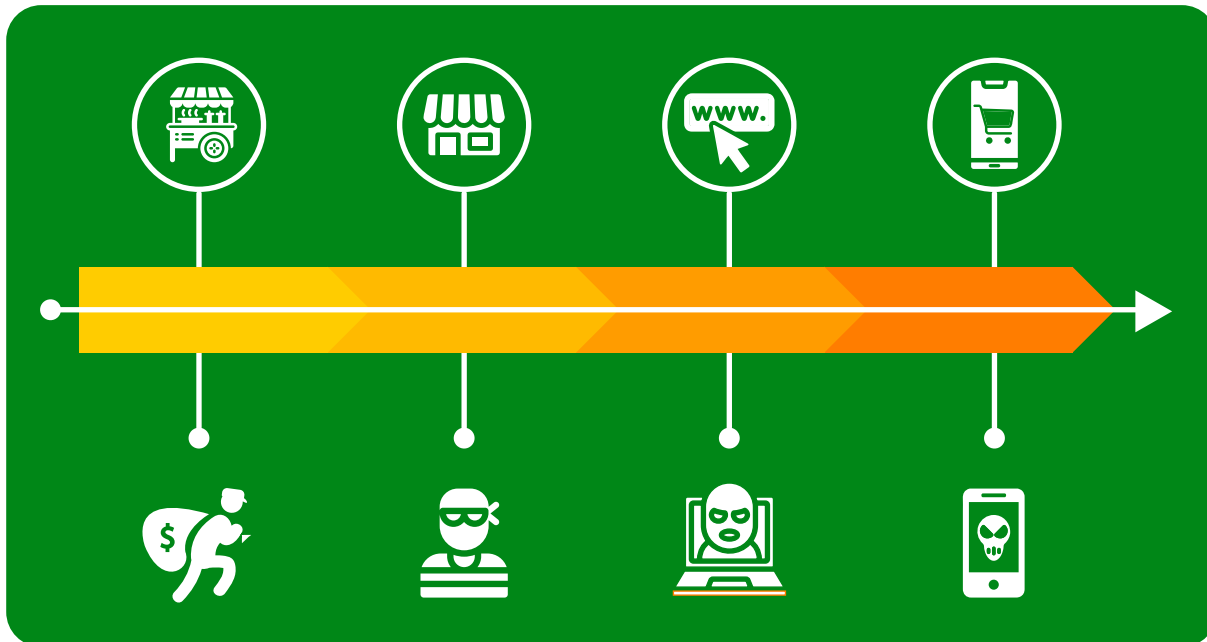


E-BOOK

Me Protegendo Contra **Golpes e Fraudes**



Boas-vindas



Você já parou para pensar como a arte de enganar sempre esteve presente?

Desde os mercados da antiguidade até as tecnologias de hoje, os métodos de golpe e fraude mudaram, mas o jogo de manipulação continua o mesmo.

E ainda assim, muitas vezes pensamos que não vamos cair nessa. Porém, é importante dizer que **NÃO** existe perfil de vítima, e sim **COMPORTAMENTO DE RISCO**.

Todo mundo tem um golpe para chamar de seu.

Junte-se a nós nesta jornada para descobrir estratégias práticas de defesa e aprender a reconhecer os sinais de alerta de golpes e fraudes antes que seja tarde!

Golpes e Fraudes: Qual a diferença?

GOLPE

Situação em que o golpista **conta com a colaboração/participação do próprio cliente**, que está sendo enganado, para realizar a transação financeira



FRAUDE

Situação em que o fraudador **NÃO necessita da participação direta do cliente** para realizar a transação financeira



A Segurança Começa com Pequenos Passos

O conhecimento, a atenção redobrada e a desconfiança podem ser suas maiores aliadas na hora de se prevenir de um possível golpe ou tentativa de fraude.

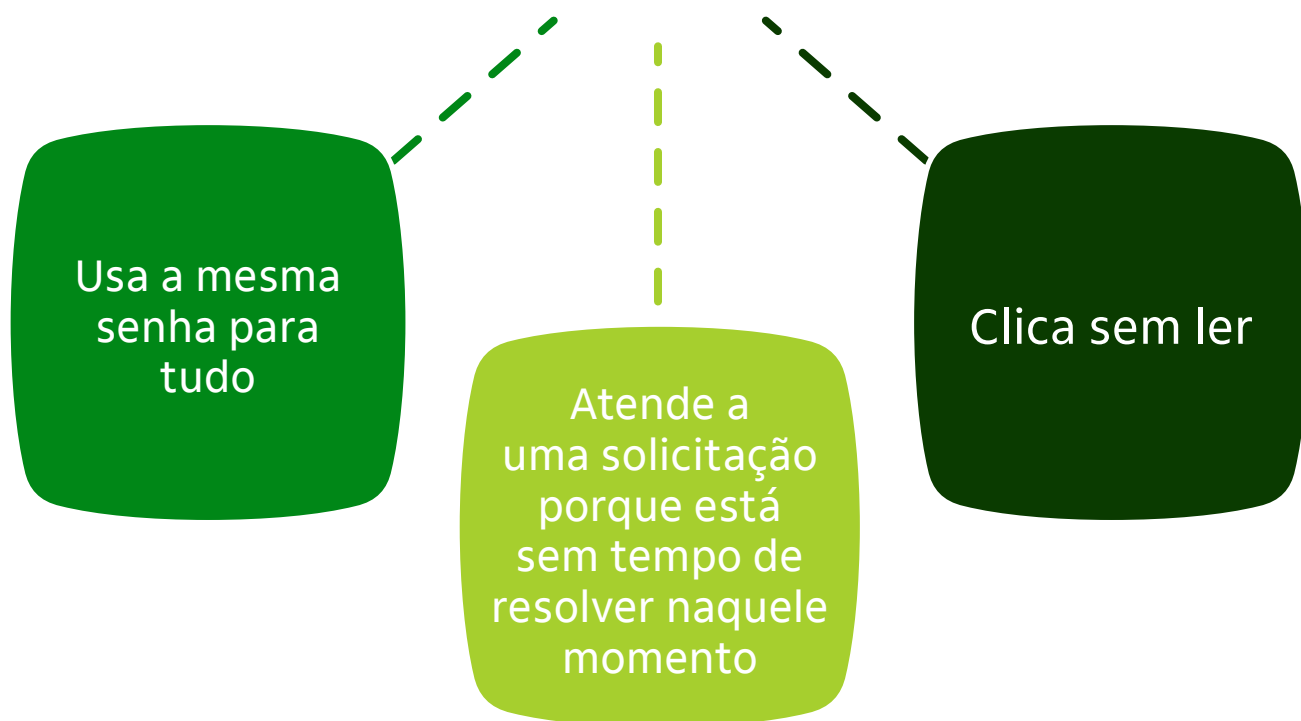


A falta de tempo é nossa inimiga!

Na correria do nosso dia-a-dia, muitas vezes acabamos tomando atitudes precipitadas ou que comprometem nossa segurança.

A falta de **TEMPO**

faz com que a gente NÃO adote comportamentos seguros:



POR ISSO SEMPRE:

Faça uma pausa!

Avalie e Desconfie

se sua postura
é segura

dos pedidos e
solicitações que receber

Realidade

+70%

dos golpes e fraudes bancários são decorrentes de **engenharia social**.

Mas o que é isso?

Engenharia Social é o
uso das nossas emoções!

Golpistas cada vez mais especializados:

- estudam os processos do banco
- usam a tecnologia a seu favor
- usam a criatividade e o jogo de cintura para manipular

Os golpistas se passam por:

- funcionários de banco
- empresas de vendas de produtos
- familiares ou amigos em situação de urgência ou emergência
- entre outros (a criatividade é infinita)



Os golpistas criam cenários que despertam sentimentos de urgência, medo, ganância, compaixão, entre outros.



Ciclo da engenharia social

1 - Preparo

Coleta de informações

Dados

Dados são facilmente compartilháveis de diversas fontes: internet, redes sociais, e até conseguidos durante a abordagem do golpista.

2 - Contato

Estabelece a comunicação

Credibilidade

Entra em contato com você e cria uma situação.

Ligação do número da central do banco
"Sou da área de segurança do banco tal"

E-mail ou mensagem em nome da bandeira de cartão de crédito
"Você tem 250.543 pontos a expirar em 24h"

3 - Exploração

Prepara o alvo

Emoção

É aqui que a manipulação psicológica acontece...

Medo
"Seu nome está negativado, conta está bloqueada"

Ganância
"Descontos ou ganhos fáceis"

Solidariedade
"Por favor preciso de ajuda"

Curiosidade
"Veja as fotos"
"Faça o teste!"

Senso de Urgência

4 - Conclusão

Finaliza a abordagem

Solicitação

E é aqui que a pessoa abordada pode interromper o golpe de acontecer....

O golpista não tem algo que precisa e está nas suas mãos entregar **(ou não)** a ele.

Normalmente são solicitações fora da rotina.

Identifique uma tentativa de golpe!

1

Desconfie da Confiança Excessiva:

Se alguém te ligar sabendo seu nome ou onde você mora, não quer dizer que seja de um canal oficial. Dados são facilmente compartilháveis de diversas fontes: internet, redes sociais, e até conseguidos durante a abordagem do golpista.

2

Não Corra com Decisões:

Se alguém te pedir para fazer algo rápido, como realizar operações na sua conta bancária, um pagamento, fornecer uma senha ou código iToken, tome cuidado. Golpistas fazem parecer urgente para você não pensar muito.

3

Verifique Emergências:

Se receber um pedido de ajuda, pare e pense. Ligue para a pessoa por outro meio para confirmar se é ela mesmo. Desconfie de todo pedido urgente ou que peça para realizar transações ou compartilhar senhas.

4

Cuidado Imediato com Pedidos de Informações:

Seja muito cauteloso se alguém pedir seus dados bancários, senhas ou códigos iToken. Não compartilhe seus dados e desconfie se for solicitado que você faça operações bancárias não planejadas, mesmo que pareça ter uma boa razão.

5

Cuidado com Links Suspeitos:

Não clique em links que chegam por e-mails ou mensagens, especialmente se eles prometem prêmios ou alertam sobre algo assustador. Confira de onde vem o link antes de clicar.



09



Golpe do aniversário ou brinde - O golpista diz que alguém mandou uma lembrança de aniversário. Para realizar a entrega, pedem o pagamento de uma taxa no cartão, ou então pedem uma selfie para confirmar a entrega, que é utilizada para contratação de financiamento.



Boleto falso - O golpista captura um boleto legítimo, muda o beneficiário e o coloca de volta no processo de envio, seja digital ou impresso. A vítima realiza o pagamento sem conferir os dados do beneficiário.



Falso motoboy - O golpista liga para a vítima em nome do banco ou de alguma bandeira de cartão de crédito. Pergunta se a pessoa fez uma compra, normalmente de alto valor. E para fazer o estorno, pede para digitar a senha e entregar o cartão a um portador para realizar suposta perícia.



Maquininha - O golpista se apresenta como vendedor de um produto ou serviço. Na hora que a vítima efetua a compra, o golpista coloca um valor maior na maquininha, distraindo a vítima para que ela não perceba.



Troca de cartão - O golpista se apresenta como vendedor de algum produto ou serviço, e na hora da compra, observa a senha da pessoa. Devolve um outro cartão parecido, ficando com o cartão e a senha da vítima.



Delivery - O golpista identifica que a vítima fez um pedido por aplicativo e entra em contato se passando por entregador da loja. Ao realizar a entrega, o entregador coloca um valor maior que o combinado.



Falsa venda - O golpista posta anúncio de vendas utilizando o perfil da rede social de outra pessoa. Os valores são muito atrativos e quando algum amigo entra em contato, o golpista solicita a transferência ou pix do valor imediato.



Links falsos - Também chamado de phishing, é o golpe mais frequente na internet, onde e-mails, mensagens de texto ou posts em redes sociais parecem vir de fontes confiáveis, como seu banco ou um amigo. Eles solicitam que você clique em um link ou forneça informações pessoais.

Senhas Seguras

Suas senhas são como as chaves dos seus tesouros digitais — elas protegem suas contas de e-mail, redes sociais, dados bancários e muito mais.



Como Criar uma Senha Forte?

Misture e Combine:

Use uma combinação de letras maiúsculas e minúsculas, números e símbolos para criar uma senha complexa que seja difícil de adivinhar.

Exemplo:



#a1b3c5678

Evite o Óbvio:

Nomes de animais de estimação, datas de aniversário, ou sequências como "12345" são exemplos de senhas fracas. Pense fora da caixa!

Exemplo:



23031990

Frase de Senha:

Considere usar uma frase inteira, como um verso de uma música, ou uma fala de um filme, com algumas alterações para adicionar complexidade, como trocar letras por números ou incluir símbolos.

Exemplo:



#F3itoD3futur0

Dicas Para Gerenciar Suas Senhas

Altere Regularmente: Mude suas senhas de tempos em tempos, idealmente a cada seis meses, para reduzir o risco de invasões.

Cuidado em Redes Públicas: Evite acessar contas pessoais em redes públicas de Wi-Fi, pois essas redes podem ser facilmente comprometidas.

Compartilhamento com Atenção: Se precisar compartilhar suas senhas por algum motivo emergencial, nunca compartilhe todas com a mesma pessoa, anote-as em lugares distintos, e use diferentes senhas para facilitar a identificação de qualquer acesso não autorizado.



Ligaram dizendo que tem uma
suspeita de fraude na sua conta?

Seu filho pedindo dinheiro
pelo WhatsApp?

Promoção imperdível
da Black Friday?

**Desconfie e
confirme por
algum canal
de confiança!**



Prevenção!

Defina e anote o contato das pessoas de confiança que
você pode pedir ajuda caso precise.

Tenha sempre acessível o telefone da sua agência/geren-
te e da delegacia mais próxima.

Caí num Golpe, e Agora?

**Contate o canal
OFICIAL** do seu
banco
imediatamente



**Comunique-se com a
sua rede de apoio,**
amigos ou familiares
que possam auxiliar
neste momento



**Troque senhas
e revise sua
segurança online**



**Informe plataformas e
autoridades,** e sempre
registre um Boletim de
Ocorrência que, em
muitos casos, pode ser
feito pela internet



Itaú 
viver mais

 LYS