



Cartilha de Apoio À Terceira Idade

**Enfrentamento de Golpes
e Fraudes financeiras**

Apresentação

Nós, estudantes do curso de Engenharia da Computação da Universidade Estadual de Ponta Grossa, desenvolvemos esta cartilha com o objetivo de ajudar os idosos a se protegerem contra golpes e fraudes no ambiente digital.

Vivemos em um mundo cada vez mais conectado, onde celulares, redes sociais e aplicativos fazem parte do nosso dia a dia.

No entanto, junto com os avanços da tecnologia, surgem também pessoas mal-intencionadas que tentam enganar os usuários, especialmente os mais vulneráveis. Os idosos, por muitas vezes não estarem familiarizados com os perigos da internet, acabam sendo alvo frequente de golpes digitais.

A cartilha de enfrentamento a golpes e fraudes tem como principal missão informar, orientar e conscientizar.

Ela foi pensada em uma linguagem simples, com exemplos reais e dicas práticas, para que todos possam entender e se sentir mais seguros ao usar a tecnologia.



Acreditamos que a informação é uma das formas mais eficazes de proteção. Por isso, este material, aborda os golpes mais comuns e ensina, passo a passo, como evitá-los.

Nossa intenção é contribuir para que a tecnologia seja usada com mais segurança, promovendo autonomia, confiança e proteção digital para os idosos e suas famílias.



CONHEÇA OS PRINCIPAIS GOLPES E FRAUDES FINANCEIRAS

Golpe da Falsa Central Telefônica ou Falso Funcionário de Banco

1

O golpista liga se passando por um funcionário do banco ou de uma empresa conhecida. Ele informa sobre uma compra suspeita no cartão ou a necessidade de uma "atualização de segurança".

O golpista solicita dados pessoais e financeiros, como senhas, números de cartão e códigos de segurança.

Em alguns casos, pode até pedir para que a vítima realize uma transferência bancária/pix ou instale um aplicativo no celular, que na verdade pode permitir o que o golpista acesse o celular a distância.



► Como identificar esse tipo de golpe?

Senso de urgência: O falso funcionário cria um cenário de pânico, dizendo que sua conta está em risco e que uma ação imediata é necessária. Eles fazem isso para que você aja por impulso, sem pensar.

Solicitação de dados sigilosos: Um funcionário de banco ou de qualquer empresa séria **NUNCA** vai pedir por telefone ou mensagem:

- Sua senha do cartão ou do aplicativo.
- Código de segurança de 3 ou 4 dígitos (CVV) do seu cartão.
- Que você tire uma foto do seu cartão.

Pedido de pagamentos: Nenhuma instituição pedirá que você faça uma transferência para cancelar uma transação ou proteger seu dinheiro, muito menos ir a um caixa eletrônico e seguir instruções por telefone.

REGRA DE OURO:

Se a ligação parece ser do seu banco, **desligue**.

Procure o número de telefone oficial no verso do seu cartão e você mesmo **ligue para o banco** para verificar se há algum problema.





CONHEÇA OS PRINCIPAIS GOLPES E FRAUDES FINANCEIRAS

Golpe do Empréstimo Consignado Falso

2

Golpistas entram em contato oferecendo empréstimos consignados com condições muito vantajosas, como juros baixos e liberação rápida, mesmo para negativados.

Para "liberar" o crédito, exigem um depósito antecipado para cobrir supostas "taxas administrativas" ou "seguros". Após o pagamento, o golpista desaparece.

► Como identificar esse tipo de golpe?

Ofertas boas demais pra ser verdade: Prometem juros muito baixos, liberação de dinheiro para negativados e sem consulta. Se a vantagem é muito grande, desconfie.



Pedido de depósito antecipado: Este é o sinal definitivo do golpe. Eles pedem um pagamento adiantado para "liberar o empréstimo", alegando ser uma "taxa de cartório", "seguro" ou "taxa administrativa".

Instituições financeiras sérias **NUNCA** cobram taxas adiantadas. O custo do empréstimo já vem incluído nas parcelas.

REGRA DE OURO:

Empréstimo de verdade não pede dinheiro adiantado. O custo total do empréstimo (juros e taxas) é sempre incluído no valor das parcelas que você pagará depois de receber o dinheiro, e nunca deve ser pago antes.



CONHEÇA OS PRINCIPAIS GOLPES E FRAUDES FINANCEIRAS

Golpe do Parente em Apuros (WhatsApp Clonado)

3

O criminoso consegue clonar a conta de WhatsApp de um familiar ou amigo. Ele então envia mensagens se passando por ela e pedindo uma transferência de dinheiro urgente para resolver uma emergência inventada, como um problema com o carro ou uma despesa médica inesperada.

► Como identificar esse tipo de golpe?

Contato incomum: Um filho, neto ou amigo que não costuma pedir dinheiro, de repente, manda uma mensagem pedindo uma transferência urgente.



O Golpista se recusa a falar: Se você ligar, ele não atenderá. Dará uma desculpa como "o microfone do celular quebrou" ou "estou em um lugar com muito barulho". Ele insiste em se comunicar apenas por texto.

A conta é de um estranho: A conta bancária (PIX, TED, DOC) informada para a transferência nunca está no nome do seu parente, mas sim no de uma terceira pessoa desconhecida. A desculpa é sempre que ele está "usando a conta de um amigo".



REGRA DE OURO:

Recebeu um pedido de dinheiro por mensagem? Ligue para a pessoa (uma chamada de voz ou vídeo) para confirmar a história. Use o número que você já tem salvo na sua agenda, não o número que enviou a mensagem.



CONHEÇA OS PRINCIPAIS GOLPES E FRAUDES FINANCEIRAS

Golpe do Link e E-mail Falsos

4

Você recebe um e-mail, SMS ou mensagem em redes sociais com um link. A mensagem pode falar sobre:

- Uma promoção imperdível ou desconto incrível.
- A necessidade de atualizar um cadastro.
- Um prêmio ou sorteio ganho.
- Uma dívida pendente ou multas de trânsito não pagas.

Ao clicar no link, você é direcionado para uma página falsa, muito parecida com a de uma empresa legítima, onde é incentivado a digitar seus dados pessoais e bancários.

► Como identificar esse tipo de golpe?

Remetente suspeito: Olhe com atenção o endereço de e-mail. Golpistas usam endereços que parecem oficiais, mas têm pequenas diferenças, por exemplo:

A caixa, como uma instituição governamental utiliza o domínio: **caixa.gov.br**, um exemplo é o e-mail:

naoresponda@caixa.gov.br, possuem o <caixa.gov.br>, são verdadeiros.

Agora, e-mails assim: **atendimento.caixa@*outlook.com***, são **FALSOS**.

Links estranhos: Passe o mouse por cima do link (sem clicar) e veja o endereço que aparece. Se não for o site oficial da empresa, não clique, por exemplo:

O endereço oficial é: **magazineluiza.com.br**, sites com o endereço dessa forma: **magalu-promo.net** ou **magazine.luiza.com**, são **FALSOS**.



REGRA DE OURO:

Sempre verifique o endereço de e-mail completo. Se a parte que vem depois do @ não for exatamente o site oficial da empresa que você conhece, delete o e-mail imediatamente.



CONHEÇA OS PRINCIPAIS GOLPES E FRAUDES FINANCEIRAS

Golpe da Prova de Vida ou Recadastramento do INSS

5

O golpista entra em contato por telefone ou WhatsApp, fingindo ser um funcionário do INSS ou do banco onde a vítima recebe o benefício.

Ele informa que, devido a novas regras, a "prova de vida" agora pode ser feita online para evitar o bloqueio do pagamento.

Para isso, pede que a vítima envie uma foto do rosto, uma foto dos documentos (RG e CPF) e, em alguns casos, que clique em um link para "validar os dados".

Com essas informações e fotos, os criminosos abrem contas e fazem empréstimos em nome da vítima.

► Como identificar esse tipo de golpe? _____

Contato Ativo do "INSS": O INSS não entra em contato por telefone ou WhatsApp para agendar ou realizar a prova de vida. A iniciativa deve ser sempre do cidadão.

Pedido de Fotos com Documentos: Nenhum órgão oficial solicita fotos suas segurando documentos por meio de aplicativos de mensagem.

Links enviados por mensagem: Não clique em links enviados por mensagem para este fim. A prova de vida é feita diretamente no aplicativo Meu INSS, no caixa eletrônico ou na agência bancária.



REGRA DE OURO:

A prova de vida é feita por você nos canais oficiais (aplicativo do Meu INSS, banco ou agência), nunca através de alguém que te liga, manda mensagem ou e-mails para ajudar, e muito menos pedem seus dados.



CONHEÇA OS PRINCIPAIS GOLPES E FRAUDES FINANCEIRAS

Golpe do Romance Virtual (Estelionato Sentimental)

6

O criminoso cria um perfil falso em redes sociais ou aplicativos de relacionamento, geralmente com fotos de outra pessoa, aparentando ser muito atraente e bem-sucedido.

Ele inicia um contato, é extremamente carinhoso e atencioso, e constrói uma relação de confiança e dependência emocional com a vítima.

Quando sente que a vítima está apaixonada, ele inventa uma grande emergência (um problema de saúde, uma dificuldade para vir ao Brasil, uma dívida urgente) e começa a pedir dinheiro.

Os pedidos são sempre acompanhados da promessa de que ele virá ao encontro da vítima assim que o problema for resolvido.

► Como identificar esse tipo de golpe?

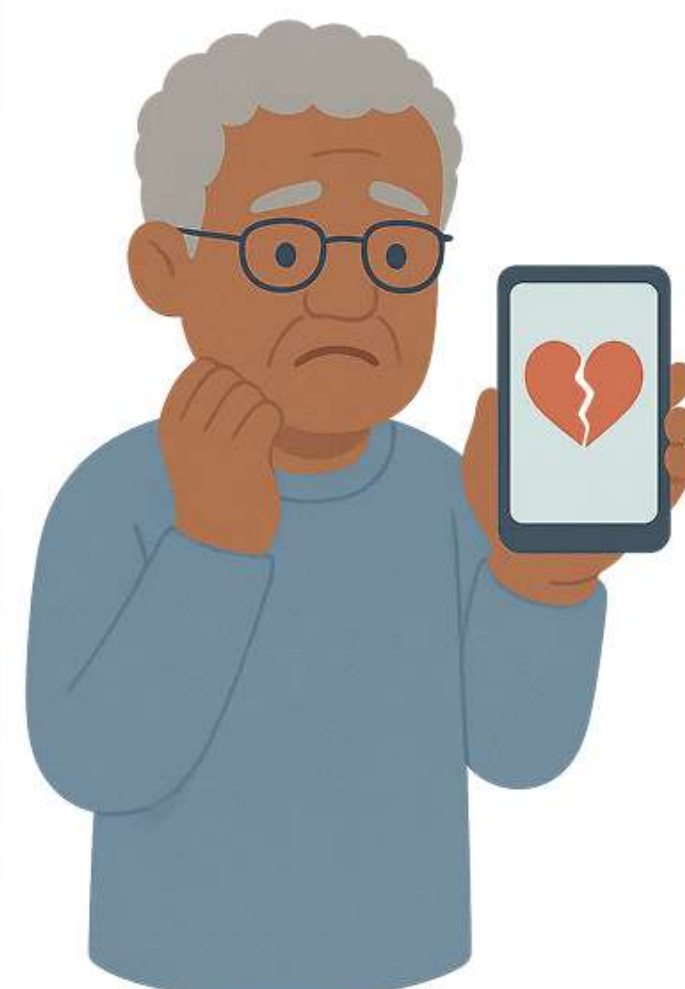
Várias desculpas: Ela sempre tem uma desculpa para não poder fazer uma chamada de vídeo ou para cancelar encontros marcados.

História mirabolante: A história de vida é mirabolante (mora no exterior, é militar em uma missão, médico em um campo de refugiados, etc.).

Sempre pedem dinheiro: Depois de um tempo, inevitavelmente, surge um pedido de dinheiro para resolver uma crise.

REGRA DE OURO:

Desconfie de romances que acontecem apenas no mundo virtual. Se a pessoa que você nunca viu pessoalmente começar a pedir dinheiro, por mais comovente que seja a história, é um golpe.





COMO EVITAR CAIR EM GOLPES?

A prevenção é a sua maior aliada.

● **DESCONFIE SEMPRE:**

Mantenha um pé atrás com contatos inesperados, seja por telefone, e-mail ou mensagem. Na dúvida, não clique, não informe e não pague.

● **PROTEJA SUAS SENHAS:**

Crie senhas fortes, misturando letras maiúsculas, minúsculas, números e símbolos. Não use a mesma senha para todos os serviços e nunca as compartilhe com ninguém. Se precisar anote as senhas em agendas ou cadernos pessoais.

● **NÃO COMPARTILHE DADOS PESSOAIS:**

Suas informações são valiosas. Não forneça senhas, códigos de segurança, número do cartão ou dados de documentos por telefone ou mensagem.



● **CONTATE AS EMPRESAS POR CANAIS OFICIAIS:**

Se receber um contato suspeito de um banco ou empresa, desligue o telefone e entre em contato com a instituição através dos números ou site oficial que você já conhece e utiliza.

● **VERIFIQUE ANTES DE FAZER TRANSFÊRENCIAS:**

Antes de fazer qualquer PIX ou transferência, especialmente se solicitada por mensagem, ligue para a pessoa (em uma chamada de voz ou vídeo) para confirmar a história e os dados bancários.

● **CUIDADO COM REDES DE INTERNET PÚBLICAS:**

Evite acessar aplicativos de banco e fazer transações financeiras em redes de internet abertas, como as de shoppings e rodoviárias.



FUI VÍTIMA DE UM GOLPE, E AGORA?

- ▶ Se você identificar que caiu em um golpe ou que seus dados foram roubados, agir rapidamente pode diminuir os prejuízos.
- ▶ **REGISTRE UM BOLETIM DE OCORRÊNCIA:**
Vá até a delegacia de polícia mais próxima ou registre o B.O. online no site da polícia civil.

O boletim de ocorrência é fundamental para formalizar a denúncia e iniciar uma investigação.

Se possível guarde todas as provas, isso pode auxiliar na investigação

- ▶ **CONTATE SEU BANCO SE FOR O CASO:**
Se caso o golpe envolver agências bancárias e cartões, ligue para o seu gerente ou para a central de atendimento do seu banco. Informe o ocorrido, peça o bloqueio do cartão e da conta, e verifique a possibilidade de contestar a transação.
- ▶ **AVISE FAMILIARES E AMIGOS:**
Caso seu WhatsApp tenha sido clonado, avise seus contatos por outros meios para que não se tornem novas vítimas.
- ▶ **DENUNCIE AOS ÓRGÃOS DE PROTEÇÃO:**
Disque 100: É o canal de denúncias de violações de direitos humanos, que inclui a violência financeira contra a pessoa idosa. A ligação é gratuita e sigilosa.

Disque Idoso (0800 141 00 01): Está à disposição da população orientações sobre os direitos da pessoa idosa, presta informações, encaminha denúncias.

LEMBRE-SE: Não se sinta constrangido por ter sido enganado. Denunciar é a melhor forma de se proteger, ajudar outras pessoas e contribuir para que os criminosos sejam punidos. Converse com sua família, peça ajuda e navegue com confiança!





PROTEJA A TERCEIRA IDADE

NÚMEROS E CONTATOS IMPORTANTES!

► BOLETIM DE OCORRÊNCIA:

Pode comparecer a delegacia de polícia mais próxima na sua cidade, ou pode registrar o **Boletim de Ocorrência** pelo **site** da Polícia Civil do Paraná.

LINK PARA REGISTRO DE BO:

[“https://www.policiacivil.pr.gov.br/BO”](https://www.policiacivil.pr.gov.br/BO)

► DENÚNCIA AOS ORGÃOS COMPETENTES:

DISQUE 100: Canal de denúncias de violação de direitos humanos em todo território nacional.

DISQUE IDOSO 0800 141 00 01: Está a disposição da população idosa para informações e denúncias.

Atendimento de segunda-feira a sexta feira,
das 8h30 às 12hs - 13h30 às 17h30

E-MAIL: disqueidoso@sejuf.pr.gov.br



CARTILHA DE APOIO À TERCEIRA IDADE



Universidade Estadual
de Ponta Grossa