# Golpes financeiros contra pessoas idosas por meio de engenharia social no ambiente digital

*Flávio Morgado*

## Introdução

Na pandemia de Covid-19, as pessoas idosas aumentaram a utilização do WhatsApp para a comunicação social, principalmente na época de quarentena (Lopes *et al.,* 2020). "Os idosos são considerados imigrantes digitais pois tiveram de aprender a lidar com as tecnologias digitais durante o seu surgimento e por isso são mais vulneráveis frente aos ataques digitais" (Fortes Luce, Brasil Estabel, 2020; Araujo e Lima, 2023; CERT.br, 2023). As fraudes financeiras podem também gerar consequências para a saúde física e mental, conforme o conceito de saúde da Organização Mundial da Saúde como situação de perfeito bem-estar físico, mental e social.

Engenharia social é uma técnica para enganar pessoas, de modo a obter informações confidenciais, como senhas e dados pessoais, mediante o abuso da confiança, da falta de cuidado com senhas, da curiosidade e do medo das pessoas **(**Mitnick e Simon**,** 2003).

O objetivo deste artigo é identificar os principais tipos de golpes financeiros contra pessoas idosas por meio de engenharia social no ambiente digital e propor algumas ações para evitá-los.

## Materiais e métodos

O contexto do artigo é o da superexposição dos idosos às mais variadas formas de comunicação e conteúdo, e a dificuldade destes de identificar, classificar e avaliar os conteúdos com os quais se deparam.

Para lidar com essa multiplicidade de estímulos, o ser humano conta com duas formas de pensar, chamados por Kahneman (2012) de Sistema 1 e Sistema 2. O Sistema 1 é rápido, intuitivo, e odeia ambiguidades, que lhe causam desconforto. O Sistema 2 é lento, racional, preguiçoso, requer atenção, está sempre funcionando, adora casos, é mais concreto.

Essas formas de compreensão do fenômeno são objeto de estudo da chamada Economia Comportamental (Kahneman, 2012; Thaler, 2015; Ávila e Bianchi, 2019), na qual este artigo se fundamenta.

A comunicação para um determinado público serve para que este saiba ou faça algo, como aderir a uma medida sanitária (distanciamento físico, máscara, lavar as mãos, usar álcool em gel etc.), tomar vacina, contrair um empréstimo, comprar um produto, votar em um candidato etc. (Knaflic, 2017). Se a comunicação é uma engenharia social, ela fará com que o destinatário cometa um engano, ou faça algo que poderá trazer prejuízos para si mesmo ou pessoas próximas.

Conforme Araujo e Lima (2023) e CERT.br (2023), os idosos, por desconhecer ferramentas de segurança, como a autenticação em duas etapas ou os antivírus, estão mais sujeitos a fraudes financeiras, utilizando os seguintes meios:

- *Phishing*: obtenção, ou "pesca", de informações confidenciais fingindo ser uma instituição confiável, convencendo a vítima a clicar em links maliciosos, abrir anexos infectados por códigos maliciosos (*malware*) etc.;
- Espionagem pela *webcam* sem consentimento;
- Uso da localização sem consentimento;
- Furtos de identidade;
- Roubo dos contatos;
- Interfaces mais simples, voltadas para idosos, mas vulneráveis;
- Uso da engenharia social.

Outras mensagens financeiras, embora não envolvam furto de informações, podem incentivar o consumo inconsciente, o endividamento ou investimentos sem a rentabilidade adequada ao momento de vida do idoso (Tonin e Hoffmann, 2015).

O método para o levantamento dos principais golpes foi a busca de notícias, relatos de pessoas próximas e alunos (aproximadamente 100 a cada semestre), além das mensagens recebidas pelo autor com tentativas de golpe, que, por ser uma pessoa idosa, deve estar no radar de golpistas tratados neste artigo.

## Resultados e discussão

***Tentativas de golpes -*** Serão descritos alguns tipos de golpes muito frequentes envolvendo a engenharia social:

a) *Alerta de banco sobre compras efetuadas, solicitando confirmação.*
   A pessoa recebe uma mensagem no WhatsApp ou SMS do tipo:
   - "Eu sou do Banco XYZ e estou ligando sobre um PIX para você no valor de 3.500 reais. Se você confirma, digite 1. Senão, digite 2 para falar com um de nossos atendentes";

   - Compra aprovada no valor de 5.999,00 nas lojas CASAS BAHIA pelo app do Banco XYZ. CASO nao reconheca ligue imediatamente na central de atendimento pelo 4003 7984". Esta mensagem veio assim mesmo, sem R$ no valor, sem acento no não, sem cedilha no reconheça, e usando telefone 4003 7984, com prefixo parecido com o dos bancos.

Supondo que a pessoa tenha conta no Banco XYZ, e digite 2, ou ligue para o número indicado, um atendente tentará obter dados da conta, senhas etc.
Nesses casos, o melhor é ignorar a mensagem, ou entrar em contato com a central de atendimento do banco para confirmar a transação.

b) *Clonagem de celular com acesso ao arquivo de contatos.*
Trata-se de um golpe tecnológico, seguido de engenharia social para obter vantagens da lista de contatos.

Após a clonagem, os golpistas mandam mensagens para as pessoas da lista de contatos do dono do celular clonado. As mensagens visam obter valores ou o que for possível dos contatos, como por exemplo, nesta troca de mensagens entre o suposto filho e o pai, conforme o quadro 1.
Quadro 1 – Sequência de mensagens de suposto filho (com foto verdadeira) e o pai.

| Hoje |
|---|
| Boa tarde pai (13:49) |
| Meu celular deu um problema no visor eu deixei na assistência, se precisar falar comigo estou usando este número até arrumar o outro (13:49) |
| Ligação de voz perdida (14:01) |
| Ligação de voz perdida (14:05) |
| Já ligo de volta (14:08) |
| Ligação de voz (14:12) |
| (Completou, mas não conseguia falar) |
| Ligação de voz (14:13) |
| (Completou, mas não conseguia falar) |
| Pai, o sinal está péssimo, não completou a ligação (14:14) |
| Está ocupado? (14:14) |
| Estou na minha mãe (14:15) |
| E porque estou precisando de um favor (14:15) |
| O que é? (14:15) |
| Pai eu estou precisando fazer um pagamento de urgência e a senha do aplicativo do banco está no outro celular. Consegue fazer esse pagamento para mim? (14:16) |
| Segunda-feira eu pegando meu celular devolvo o valor (14:16) |

Depois da última mensagem o pai não respondeu e ligou para o número verdadeiro, supostamente inoperante. Quando o filho atendeu, foi confirmada a fraude e foram alertados os contatos.

Logo em seguida, eles apagaram todas as mensagens, mas já tinha sido feito um print.

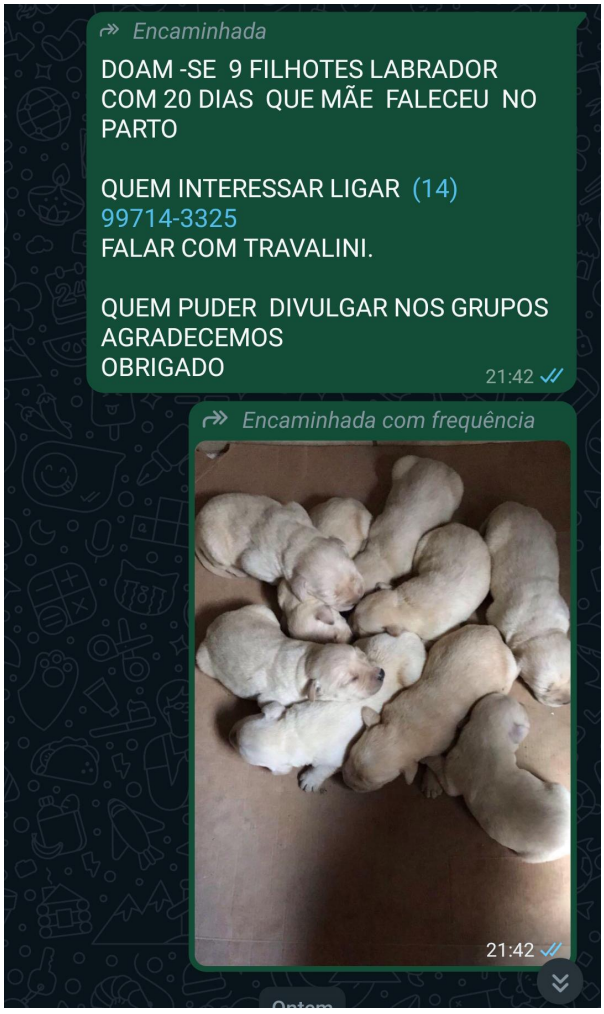
Uma sugestão é nunca colocar a identificação da relação com a pessoa do contato. Use o nome ou apelido do pai ou da mãe, ou algo que lembre o nome da rua, em vez da palavra ‘casa’. Isso dificulta a vida dos golpistas, pois é provável que antes que alguém faça o pagamento solicitado, alguém

entre em contato com a pessoa do celular clonado, e esta dispare mensagens de alerta para os seus contatos.

Outra sugestão é a confirmação em duas etapas, para evitar a clonagem.

c) *Doação de filhotes ou ganho de processo judicial*
Mensagem recebida por várias pessoas, e pior, compartilhada, conforme figura 1:

Figura 1 – Mensagem encaminhada sobre doação de filhotes




Se a conversa tiver sequência, provavelmente o doador pedirá um valor para cobrir o custo do rateio do parto, das vacinas e do frete da entrega, algo como R$ 500 (valor “pequeno”, perto do custo de um filhote de labrador, em média R$ 3.000). A mensagem foi detectada como falsa por meio de contatos entre as pessoas que desconfiaram.

Não se trata de culpar a vítima pela ingenuidade ou ganância, mas muitos golpes, como no caso dos filhotes de labrador, são bem-sucedidos não só pela fofura dos filhotes, mas por acreditar-se que alguém vai entregar por R$ 500

reais algo que poderia ser vendido por R$ 3.000 em média. O que o tutor da mãe dos filhotes faria caso ela não morresse no parto?

Uma variação desse golpe é a notificação de ganho de algum processo judicial, solicitando algum valor para pagamento de custas, documentação etc.

*d) Outros golpes*

- Presente no dia do aniversário: enviado por uma suposta empresa de envio de presentes, como a Giuliana Flores, com opções para retirar na loja ou para receber por motoboy, a um custo de R$ 4,99. Se a pessoa não responde, eles entram em contato e tentam "empurrar" a entrega, talvez para clonar o cartão ou coisa pior. Se a pessoa pergunta quem enviou, eles dizem que foi uma pessoa de um lugar que você trabalha ou trabalhou. Se você fizer mais perguntas, eles desligam.

- Golpe da confirmação de pagamento em vendas pelo Mercado Livre, OLX etc.: Os golpistas veem que a pessoa está vendendo algo e mandam mensagens pedindo para fazer negócio sem o intermediário, ou mandam comprovante (falso) de pagamento do produto, para que a pessoa entregue o produto;

- Oferta de vitaminas, remédios e procedimentos para desacelerar o envelhecimento, aumentar a vitalidade, a libido etc.;

- Convênios e soluções fora do SUS por preços abaixo do mercado;

- Ofertas de empréstimos consignados, principalmente logo após a aposentadoria (nem sempre com juros baixos, que seriam possíveis em função da garantia oferecida), que podem levar ao crédito irresponsável e ao endividamento;

- Comunicações sobre a necessidade de provas de vida, feitas online ou por telefone;

## *Educação contra a desinformação*

O processo educacional deve levar em conta as questões de segurança de uma determinada época. Os golpes vão se modificando à medida que são criados antídotos contra os existentes. Por exemplo, vários golpes coletados no livro Golpes & Fraudes (Maldaner, 2000), já não são praticados, pois os bancos mudaram o processo da transação para torná-las seguras.

Grande parte dos golpes dependem do comportamento das pessoas, não estando relacionados a fraudes contra a tecnologia, roubos e furtos. A prevenção a estes golpes depende da mudança de comportamento, que pode ser potencializada pela educação financeira:

a) *Observar falhas nos elementos do processo de comunicação:*
   - Erros de ortografia nas mensagens;
   - Mensagens frequentemente encaminhadas (correntes);
   - Nunca “clicar aqui”;
   - Contatos telefônicos solicitando dados que as instituições deveriam ter, ou com pedidos de senhas;
   - Tentativas de gerar endividamento devido ao crédito irresponsável (oferta de empréstimo consignado logo depois da aposentadoria, banco que não é o da pessoa, bens ou serviços desnecessários etc.)
   - Desconfiar de ofertas muito vantajosas (sorteios, recebimento de pix, dicas exclusivas, doações de filhotes etc.)

b) *Pedir ajuda para alguém confiável;*

c) *Instalar antivírus e manter softwares atualizados;*

d) *Evitar senhas fracas e efetuar a troca regularmente;*

e) *Ligar na central de atendimento do banco ou digitar o link do banco na barra de endereços do navegador.*

## Considerações finais

A educação financeira é para a ativação do Sistema 2 de Kahneman (2012), racional, analítico, mas dispendioso e preguiçoso, que fará as análises necessárias para identificar padrões de golpes. Usando como metáfora a Inteligência Artificial, o aprendizado de máquinas é feito à base de treino, validação, testes. Quando os bancos fazem repetidas propagandas alertando sobre fraudes, mandam SMS a cada transação avisando sobre “atenção a golpes!” ou “Nunca ligamos solicitando transações para cancelamento de operações não reconhecidas” etc., eles estão treinando nosso Sistema 2 nos padrões de fraude.

## Referências

Araujo, Gabriely; Lima, Galeno. Idoso é alvo fácil de invasores na Internet. Disponível em https://infograficos.estadao.com.br/focas/planeje-sua-vida/idoso-e-alvo-facil-de-invasores-na-internet, Acesso em 22/12/2023.

Ávila, Flávia; Bianchi, Ana Maria. **Guia de Economia Comportamental e Experimental**. 2. ed. São Paulo: EconomiaComportamental.org, 2019.

CERT.br. Internet segura. 2.ed. Disponível em https://internetsegura.br/pdf/guia-internet-segura.pdf, Acesso em 22/12/2023.

Fortes Luce, B.; Brasil Estabel, L. Letramento informacional e mídias sociais: uma experiência com idosos para a competência informacional na identificação de *fake news*. **Revista Brasileira de Pós-Graduação**, *[S. l.]*, v. 16, n. 35, p. 1–

14, 2020. DOI: 10.21713/rbpg.v16i35.1661. Disponível em: https://rbpg.capes.gov.br/rbpg/article/view/1661. Acesso em: 22 dez. 2023.

Kahneman, Daniel. **Rápido e devagar**: duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

Lopes, R. G. C.; Côrte, B.; Morgado, Flávio; Brandao, V.; Manso, M. E. G.; Lodovici, F. M.M. Pandemia COVID-19: Perfil de um grupo de pessoas idosas brasileiras participantes de uma pesquisa abrangendo América Latina e Caribe. **Revista Kairós**, v.23, p.309 - 332, 2020.

Maldaner, Senador Casildo. Golpes & Fraudes: saiba como evitar. Brasília: Senado Federal, 2000.

Mitnick, Kevin D., Simon, William L. **A arte de enganar**: Ataques de *hackers*: Controlando o fator humano na segurança da informação. São Paulo: Pearson Universidades, 2003.

Tonin, Carla Maria Schroeder; Hoffmann, Eduardo. A vulnerabilidade do consumidor idoso frente às instituições financeiras. **Anais do 13º Encontro Científico Cultural Interinstitucional**, 2015.

Thaler, Richard H. **Misbehaving**: the making of Behavioral Economics. New York: W.W. Norton & Company, 2015.

*Data de recebimento: 30/08/2024; Data de aceite: 30/08/2024.*

**Nota**
O presente trabalho é produto do projeto de pesquisa “Reações de idosos a mensagens que podem afetar sua saúde financeira e geral: uma proposta educacional”*,* aprovado no 3° Edital Acadêmico Envelhecer com Futuro do Itaú Viver Mais em parceria com o Portal do Envelhecimento.

_____

**Flávio Morgado** - Bacharel em Matemática, Mestre em Administração de Empresas e Doutor em Comunicação e Semiótica. Professor e pesquisador da PUC São Paulo. Experiência em Sistemas de Informação. Pesquisa envelhecimento, inteligência artificial, gestão em saúde e impactos sociais da Tecnologia da Informação. É membro do Núcleo de Estudo e Pesquisa do Envelhecimento da PUC-SP. E-mail: fmorgado.sp@gmail.com