Estamos evoluindo a Inteligência Artificial. Mas estamos deixando o fator humano para trás?

ClearFi
INSTITUTE

ClearFi Institute | Financial Innovation & Trust
Bento Silva
https://www.linkedin.com/company/clearfi-institute-financial-innovation-trust/
https://www.linkedin.com/in/bento-silva/

Os ataques estão cada vez mais sofisticados.

Mas continuam explorando exatamente a mesma vulnerabilidade:

nossas decisões.

A Inteligência Artificial nunca evoluiu tão rápido.

A cada semana surgem modelos mais sofisticados, agentes autônomos, automações inteligentes e ferramentas capazes de executar tarefas que, até pouco tempo atrás, eram exclusivas do ser humano.

Ao mesmo tempo, uma pergunta começa a se tornar inevitável:

> **“estamos evoluindo nossa tecnologia na mesma velocidade em que preservamos nossa capacidade de pensar, questionar e decidir?”**

Talvez o maior desafio da era da IA não seja construir máquinas mais inteligentes, mas garantir que as pessoas continuem exercendo aquilo que nenhuma tecnologia consegue substituir: o discernimento humano.

Eu tenho como prática revisar semanalmente os principais incidentes ocorridos no mundo, utilizando alguns canais que tenho acesso e portais para profissionais de segurança cibernética. Nessa útima semana, ao revisar esses incidentes percebi que a maioria deles não começaram com uma falha técnica, mas com uma pessoa cansada, pressionada ou distraída do outro lado da tela.

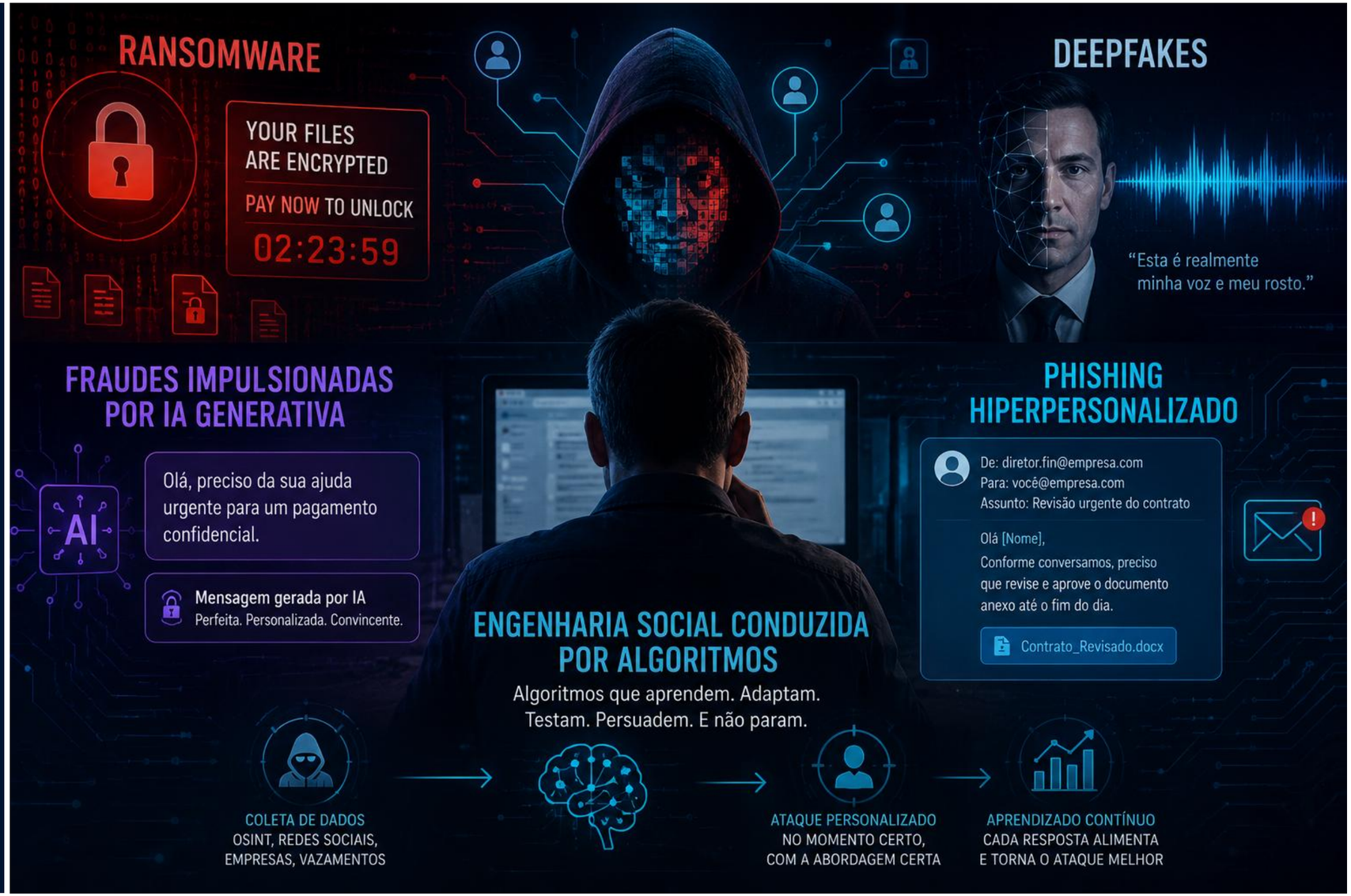
Em um dos casos, se eu tivesse que resumir em uma frase, seria basicamente isso: **alguém sob um prazo apertado recebeu uma mensagem aparentemente legítima e aprovou uma solicitação sem validar por um segundo canal.** Nenhuma vulnerabilidade explorada, nenhum exploit sofisticado, apenas uma decisão tomada rápido demais.

Percebi que isso não é coincidência, é um padrão.

Um padrão que venho observando há anos, mas que se tornou impossível ignorar nos últimos meses: a tecnologia de ataque evoluiu mais rápido do que nossa capacidade de proteger o elo mais frágil da cadeia, o ser humano.

- Ransomware
- Deepfakes
- Fraudes impulsionadas por IA generativa
- Phishing hiperpersonalizado
- engenharia social conduzida por algoritmos capazes de aprender a cada tentativa.

A lista cresce mês após mês, e as manchetes começam a parecer menos incidentes isolados e mais sintomas de algo muito maior.





Durante muito tempo, causar um impacto relevante exigia um atacante altamente sofisticado, com muita expertise técnica.

Hoje, isso já não é mais verdade.

Um criminoso não precisa necessariamente de conhecimento técnico avançado para **gerar danos em escala global**. Em muitos casos, basta acesso a uma ferramenta de IA, alguns prompts bem construídos e alguém cansado do outro lado da tela.

Ao mesmo tempo, o que esses ataques exploram não mudou tanto assim, apenas ficou mais fácil de explorar.

O alvo continua sendo o **comportamento humano**: o colaborador sobrecarregado que clica sem validar, o executivo pressionado que aprova sem confirmar, a confiança depositada em uma voz, uma mensagem ou um vídeo que parecem legítimos.

Depois de mais de duas décadas trabalhando com risco operacional, infraestrutura crítica e segurança no setor financeiro, aprendi uma lição que nunca deixou de se confirmar: **os maiores incidentes raramente começam em uma vulnerabilidade técnica. Eles começam em uma decisão humana.**

O que mudou foi a escala, e a precisão com que máquinas agora conseguem simular, manipular e explorar comportamento humano.

Estamos automatizando processos

Estamos automatizando relações

Produzimos cada vez mais dados

Exercitamos cada vez menos pensamento crítico

Tomamos decisões cada vez mais rápidas

> **Quanto mais automatizamos decisões, mais importante se torna preservar nossa capacidade de pensar criticamente.**



Individualmente, cada um desses movimentos parece apenas uma consequência natural da transformação digital. Juntos, porém, criam um ambiente onde velocidade passou a valer mais do que validação.

E é exatamente nessa lacuna que o cybercrime moderno está prosperando.

O mercado corre para implementar IA em tudo: atendimento, análise, operações, vendas, segurança, governança e produtividade.

Em muitos casos, isso é necessário. Mas poucas organizações estão discutindo, com a profundidade necessária, uma pergunta simples: **qual é o impacto humano de tudo isso?**

Isso não é resistência à inovação. É maturidade na adoção.



A tríade já não é suficiente!

Durante décadas aprendemos que segurança depende do equilíbrio entre **Pessoas, Processos e Tecnologia.**

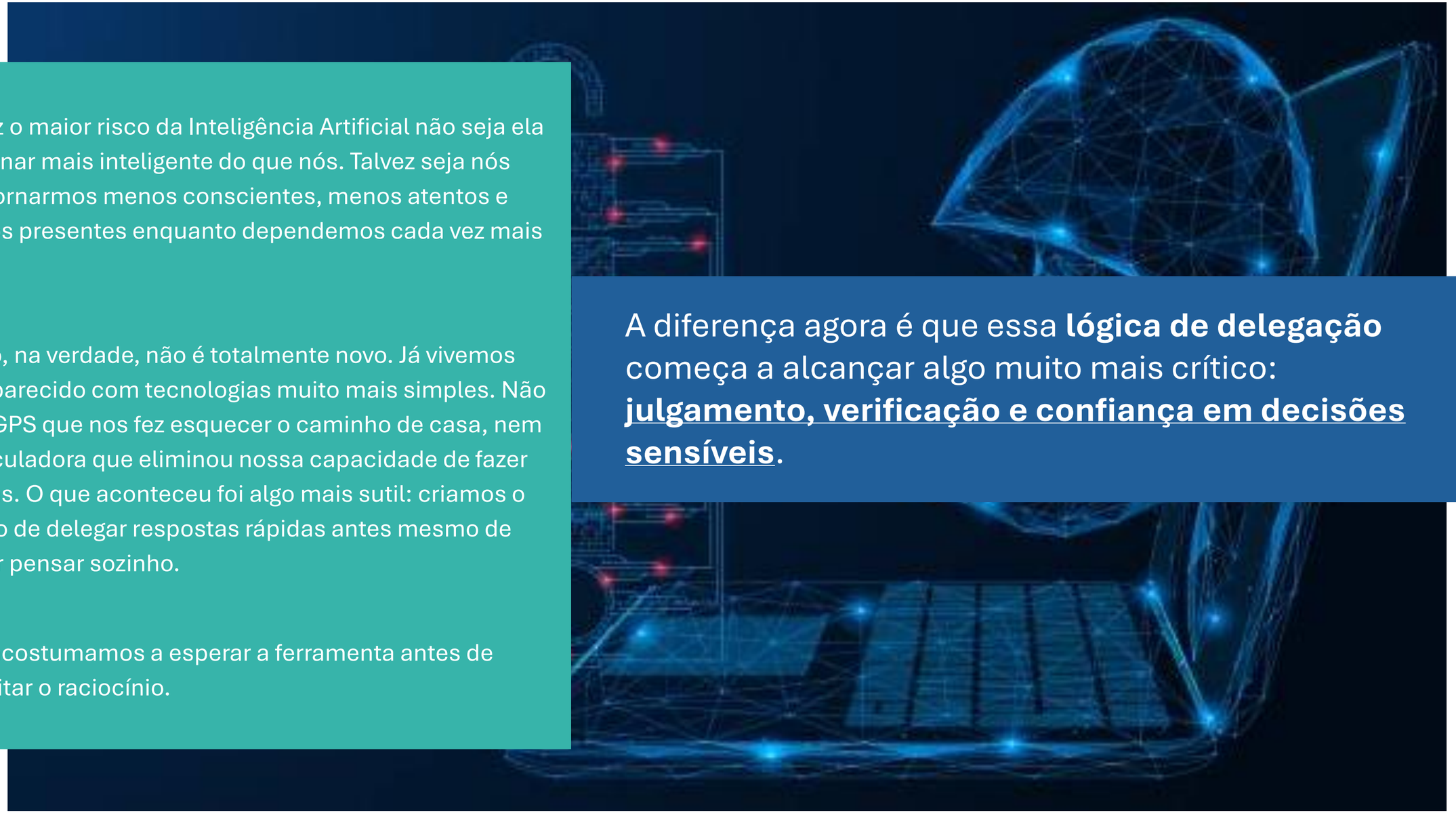
Na era da **Inteligência Artificial**, talvez seja necessário explicitar um quarto componente.

“CONSCIÊNCIA”

Talvez o maior risco da Inteligência Artificial não seja ela se tornar mais inteligente do que nós. Talvez seja nós nos tornarmos menos conscientes, menos atentos e menos presentes enquanto dependemos cada vez mais dela.

E isso, na verdade, não é totalmente novo. Já vivemos algo parecido com tecnologias muito mais simples. Não foi o GPS que nos fez esquecer o caminho de casa, nem a calculadora que eliminou nossa capacidade de fazer contas. O que aconteceu foi algo mais sutil: criamos o hábito de delegar respostas rápidas antes mesmo de tentar pensar sozinho.

Nos acostumamos a esperar a ferramenta antes de exercitar o raciocínio.



A diferença agora é que essa **lógica de delegação** começa a alcançar algo muito mais crítico: **julgamento, verificação e confiança em decisões sensíveis**.

E quando deixamos de exercitar isso, o custo já não é apenas errar uma conta. O custo pode ser abrir a porta para um ataque.

A próxima grande discussão da tecnologia provavelmente não será apenas sobre inovação, será sobre equilíbrio.

Sobre recuperar aquilo que nunca deveria ter sido deixado para trás: **pensamento crítico, responsabilidade, validação, empatia e conexão humana.**

Volto aos incidentes que mencionei no início. Se eu tivesse que apontar uma causa raiz comum entre eles, não seria uma falha de sistema. Seria um instante quase invisível em que alguém deixou de parar e validar.

É exatamente nesse segundo que a defesa mais sofisticada do mundo perde para uma pausa que não aconteceu.

Porque o futuro da segurança talvez não dependa da inteligência das máquinas. Mas da capacidade humana de continuar dizendo:
"Espere.
Vou validar antes."



Sobre o autor



Bento Silva
https://www.linkedin.com/in/bento-silva/

- **Responsável pela criação do Cyber Lab da FEBRABAN**
  Liderei a concepção, estruturação e operação do Laboratório de Segurança Cibernética da FEBRABAN, promovendo pesquisas, desenvolvimento de frameworks, inteligência de ameaças e iniciativas que fortalecem a cibersegurança do setor financeiro brasileiro.

- **Banking & Cybersecurity**
  Mais de duas décadas de atuação no setor financeiro, com forte foco em cibersegurança, gestão de riscos, proteção de dados, resposta a incidentes e desenvolvimento de estratégias de segurança da informação.

- **Infraestrutura e Governança**
  Especialista em infraestrutura de TI, governança de tecnologia, continuidade de negócios e compliance regulatório (NIST, ISO 27001, SOC 2, LGPD, PCI), garantindo ambientes seguros, resilientes e alinhados aos objetivos de negócio.

- **Experiência internacional nos EUA**
  Atualmente reside nos Estados Unidos, acompanhando de perto as tendências globais de tecnologia, transformação digital e cibersegurança. Ao longo dessa trajetória internacional, atuou na Apple, HP e Kotman Technology, com foco em excelência no atendimento, soluções tecnológicas e relacionamento estratégico com clientes, liderando iniciativas de alinhamento técnico, infraestrutura, segurança da informação e transformação digital para empresas de diferentes segmentos.

Sobre o ClearFi Institute
O ClearFi Institute é uma iniciativa independente dedicada à produção de pesquisas, white papers e análises sobre pagamentos, inovação financeira, governança, cibersegurança e transformação digital, contribuindo para o debate técnico e estratégico sobre a evolução do sistema financeiro.
https://www.linkedin.com/company/clearfi-institute-financial-innovation-trust/