Estudo: Caça aos Golpes Digitais (Página 1)

Objetivo: ensinar a identificar golpes comuns em contexto bancário brasileiro.
Sinais de alerta:
 - Urgência artificial ("sua conta será bloqueada em 1h").
 - Links encurtados ou domínios parecidos (ex.: itau-secure.com).
 - Pedidos de código de verificação por WhatsApp.
 - Anexos inesperados (.pdf/.zip) e erros de ortografia.
Boas práticas:
 - Verifique o domínio (ex.: *.itau.com.br, *.bradesco.com.br, bb.com.br, santander.com.br, caixa.gov.br, nubank.com.br, inter.co).
 - Nunca informe senhas ou códigos por mensagem.
 - Acesse o app/banco digitando o endereço oficial.
Consentimento informado: este estudo não coleta PII; métricas são agregadas localmente no seu navegador.

Estudo: Caça aos Golpes Digitais (Página 2)

Procedimento do experimento (resumo):
1) Pré-teste com 10 itens (sem feedback).
2) Exposição: Grupo A joga o mini-jogo; Grupo B lê este PDF.
3) Pós-teste com 10 itens diferentes (sem feedback).
4) Questionários SUS (usabilidade) e NASA-TLX (carga).
Métricas primárias: Δ acurácia (pós−pré), tempo médio por item, falsos (+/−).
Ética: participação voluntária, sem dados pessoais. Feche o navegador para limpar dados locais.