



OPINIÃO

Caso do Louvre: o alerta global sobre segurança que vai além das senhas

Mirella Kurata (*)

Ao ser alvo de um assalto milionário em outubro de 2025, no qual ladrões levaram joias da coroa francesa avaliadas em cerca de 100 milhões de dólares, o Louvre levantou novos debates sobre segurança digital, principalmente tratando-se de escolhas de senhas.

O Museu mais visitado do mundo, com orçamento milionário e status de patrimônio cultural global, teve divulgado que o seu sistema de videovigilância utilizava “Louvre” como senha, expondo falhas graves de segurança digital e infraestrutura obsoleta, o que reforça que não há tecnologia capaz de proteger uma organização que não enxerga a segurança como parte da sua estratégia e cultura.

A tentação de delegar à tecnologia toda a responsabilidade pela cibersegurança é um erro comum. No entanto, o caso do Louvre mostra o contrário ao contrapor a proteção mais avançada do mundo com uma senha previsível e uma equipe sem treinamento contínuo sobre boas práticas. Entre piadas e incredulidade, esse episódio rendeu questionamentos dos internautas sobre os padrões de senhas complexas adotados por muitos sites e aplicativos, já que nem o Louvre faz isso.

No entanto, a resposta é simples: a negligência digital independe de tamanho, prestígio ou poder econômico, no dia a dia, o impacto de uma senha fraca pode ser a perda de dados pessoais, de uma conta bancária ou até da própria identidade digital. A cibersegurança é, antes de tudo, comportamental e depende da conscientização, disciplina e responsabilidade compartilhada. Criar uma cultura de segurança é tão importante quanto investir em firewalls, sistemas de detecção ou inteligência artificial.

Outro ponto exposto pelo episódio do Louvre é o impacto da infraestrutura obsoleta, já que o museu mantinha parte de sua operação em servidores de 2003, uma prática ainda comum de muitas instituições públicas e privadas ao redor do mundo. Sistemas legados não são, por si só, o problema, mas sim eles permanecerem conectados a ambientes críticos sem as devidas camadas de proteção, atualização ou segmentação. O desafio é

encontrar o equilíbrio entre continuidade operacional e modernização segura, e isso exige planejamento técnico e visão de longo prazo.

Apesar de muitos ainda separarem o âmbito físico do digital, no Louvre foi a falha cibernética que facilitou o roubo dos objetos, reforçando o quanto essa fronteira de espaços está cada vez mais tênue. Hoje, câmeras, sensores, catracas e sistemas de alarme estão todos conectados às redes digitais e basta uma brecha de senha ou configuração mal feita para comprometer toda uma operação de segurança. Essa integração, porém, exige que as equipes de tecnologia e de segurança patrimonial atuem de forma conjunta, compartilhando responsabilidades e informações em tempo real.

No Brasil, o caso do Louvre serve de alerta especialmente para o setor público. Prefeituras, órgãos governamentais, escolas e hospitais ainda operam, em muitos casos, com sistemas antigos, acessos compartilhados e ausência de protocolos de cibersegurança. Por lidarem com dados sensíveis, de cidadãos, servidores e serviços essenciais, essas instituições são alvos frequentes de ataques, muito também porque costumam subestimar os riscos. Proteger o setor público envolve muito mais que só senhas fortes, inclui também planejamento orçamentário, capacitação de equipes e políticas de cibersegurança que não se limitem à área de TI, mas que envolvam gestores, comunicadores e servidores em todos os níveis.

Mais do que evitar incidentes, investir em segurança é agregar valor à instituição e seus serviços e produtos. Cada medida de proteção adotada, seja uma senha forte, um sistema atualizado ou uma equipe bem treinada, é um ativo intangível que preserva reputação, credibilidade e continuidade de negócios. No Louvre, as jóias roubadas foram avaliadas em milhões, mas o verdadeiro prejuízo foi institucional com a perda da confiança pública e o abalo à imagem de um dos ícones culturais global. Em um ambiente corporativo e governamental o princípio é o mesmo, com a segurança digital sendo uma questão de cultura, um dos ativos mais valiosos que uma organização pode ter.

(*) CEO da DMK3.

Um terço das pessoas evita obter informações sobre sua própria saúde

Annals of Behavioral Medicine é uma revista médica mensal publicada pela Oxford University Press.

Vivaldo José Breternitz (*)

Um estudo por ela publicado recentemente mostra que cerca de um terço das pessoas evita ou tende a evitar obter informações sobre sua saúde, mesmo quando o acesso a elas é cada vez mais amplo.

A pesquisa analisou 92 estudos anteriores, envolvendo 564.497 participantes de 25 países. Os resultados revelam que embora o diagnóstico precoce seja muito importante para o sucesso de tratamentos, muitas pessoas resistem a exames preventivos e consultas de rotina. Trata-se da primeira estimativa global sobre o fenômeno, com implicações relevantes para o estabelecimento de políticas de saúde.

Segundo os autores do estudo, a tendência é mais forte diante de doenças incuráveis: 41% evitam informações relacionadas ao Alzheimer e 40% ao Huntington, um mal degenerativo. Em casos de doenças graves, mas tratáveis, como HIV (32%) e câncer (29%), os índices caem um pouco. Já em doenças crônicas e controláveis, como diabetes, a evasão foi menor, ficando em 24%.

Os pesquisadores definem “evitação de informações médicas” como qualquer comportamento voltado a atrasar ou impedir o acesso a dados disponíveis, mas considerados indesejados, desde adiar consultas até recusar exames.

Embora custo e falta de informação sejam fatores frequentemente lembrados, o estudo aponta que o fenômeno não se explica apenas por isso. A Alemanha, por exemplo, onde planos de saúde cobrem consultas e informam pacientes sobre serviços disponíveis, também registrou altos índices de evasão.

“Uma possibilidade é que a decisão de não querer saber seja deliberada”, afirmou Ralph Hertwig, coautor do estudo e diretor do Centro de Racionalidade Adaptativa do Instituto Max Planck, em Berlim. Hertwig lembra que o grupo já identificou esse tipo de “ignorância deliberada” em outras áreas da vida, motivada por razões diversas.

Foram identificados 16 principais fatores que influenciam a evitação, entre eles sentir-se sobrecarregado, baixa confiança na própria capacidade de cuidar da saúde, medo de julgamento, desconfiança e falta de confiança no sistema médico. Questões como gênero, raça ou etnia não tiveram peso relevante.

As variações regionais observadas sugerem que os diferentes sistemas de saúde podem influenciar o comportamento das pes-



Yazid_Nasuha_CANVA

soas, ressaltando que a prática não deve ser automaticamente classificada como irracional: pode ser uma forma de lidar com a ansiedade diante de más notícias.

“Observamos que menor confiança no sistema médico está associada à maior evasão de informações”, destacou Konstantin Offer, principal autor do estudo e pesquisador do Instituto Max Planck. “Restaurar a confiança poderia levar a maior engajamento das pessoas.”

Em resumo, evitar check-ups ou não querer saber o resultado de exames é mais comum do que parece. A dúvida que permanece é como essa tendência, cada vez mais evidenciada, pode impactar os sistemas de saúde e as pessoas, no longo prazo.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnit@gmail.com.



News @TI

ricardosouza@netjen.com.br

Software.com.br inicia comercialização no Brasil da ferramenta de IA Brian

@A Software.com.br, especialista em tecnologia líder na América Latina, anuncia parceria estratégica com a AskBrian, empresa do grupo think-cell, para comercialização no Brasil do assistente digital com Inteligência Artificial Brian. Projetado para atender às demandas de profissionais que atuam com dados, relatórios e apresentações, como executivos, consultores, analistas financeiros e equipes de estratégia, o Brian oferece uma experiência de automação inteligente que transforma a rotina empresarial, integrando diversas ferramentas, fontes de dados e plataformas que otimizam processos operacionais, liberam tempo para atividades de maior valor e aumentam a produtividade no ambiente de trabalho (www.software.com.br).

Solução de conforto térmico que reduz gasto de energia em até 40%

@A Daikin irá expor na COP30 aparelhos de ar condicionado para uso em edifícios que reduzem o gasto de energia elétrica em até 40%. Testes realizados em prédios da própria companhia comprovaram a redução no consumo, em comparação com métodos convencionais de ventilação e climatização. A solução tem potencial de contribuir para a descarbonização de edifícios. Os visitantes do estande, que estará montado no Pavilhão Japonês, poderão vivenciar uma demonstração interativa que simula diferentes níveis de umidade, permitindo perceber diretamente como o conforto pode variar mesmo quando a temperatura é a mesma (https://www.daikin.com.br/).

Programa de estágio apostando na formação da geração Z em Inteligência Artificial

@OiFood anuncia o lançamento do GEN AI, programa de estágio da empresa para identificar, contratar e desenvolver a próxima geração de criadores de IA — ou seja, jovens talentos que unem curiosidade, habilidades técnicas e propósito para moldar o futuro da Inteligência Artificial. As inscrições estão abertas a jovens de todo o Brasil, podendo ser realizadas até 23 de novembro através do site (https://carreiras.ifofood.com.br/job/8243837002/).

Teste com AccuCore HCF™ (Hollow Core Fiber)

@A Scala Data Centres uniu-se à Lightera e a Nokia para realizar a primeira prova de conceito (PoC) com AccuCore HCF™ (Hollow Core Fiber) na América Latina. O teste, realizado no campus Tamboré da Scala em São Paulo, o maior complexo de data centers da América


Latina, demonstrou redução de aproximadamente 32% na latência em comparação com fibras ópticas convencionais. Esse avanço representa um marco em infraestrutura digital, aproximando as velocidades de transmissão dos limites físicos da luz. Após o sucesso da prova de conceito, as três empresas estudam implantações em escala de produção, com foco inicial em aplicações de ultrabaixa latência e alto volume de dados — alinhadas à visão da Scala de construir infraestrutura digital de próxima geração, otimizada para IA Fabric e workloads de alta performance.

Solução evita chamadas indesejadas

@Milhões de brasileiros enfrentam diariamente o incômodo das ligações indesejadas. Muitas vezes, ocorrem em horários inconvenientes e os destinatários nem conhecem as pessoas procuradas. Além disso, essas chamadas podem ser golpes ou cobranças indevidas. Para minimizar o transtorno, é recomendado cadastrar-se na plataforma "Não Me Perturbe", solução criada pela ABR Telecom (Associação Brasileira de Recursos em Telecomunicações) para a Anatel. Uma vez cadastrado um telefone fixo ou móvel pelo consumidor na plataforma “Não Me Perturbe”, os bancos e as prestadoras de serviços de telecomunicações participantes do serviço não poderão realizar qualquer oferta de operações de empréstimo e cartões de créditos consignado, assim como ofertas de telefone móvel, telefone fixo, TV e Internet para esse telefone. Para se cadastrar, acesse o site Link (https://www.naomeperturbe.com.br/) e siga as instruções.

Tecnologia de identificação única (IA) ajuda a barrar falsificações e proteger consumidores

@A solução ID Secure, desenvolvida pela SecureTrace e reconhecida internacionalmente com 99,9% de eficácia anticópia, fortalece a segurança de cadeias produtivas sensíveis, como a de bebidas e medicamentos, oferecendo meios confiáveis de identificação e controle de origem. De forma simples, o sistema permite que produtos sejam verificados ao longo de toda a cadeia, do fabricante ao ponto de venda, garantindo transparência, rastreabilidade e proteção tanto para o consumidor quanto para as marcas. Além de proteger o consumidor, o ID Secure também oferece segurança jurídica e reputacional a bares, restaurantes e estabelecimentos comerciais, que passam a comprovar a procedência de seus estoques. As informações geradas pelo sistema podem ser acessadas por órgãos de fiscalização e pelas forças de segurança, facilitando o trabalho de investigação e combate ao mercado ilegal (https://www.securetrace.com.br/).

 José Hamilton Mancuso (1936/2017)	Laurinda Machado Lobato (1941-2021)	Responsável: Lilian Mancuso
Editórias <i>Economia/Política:</i> J. L. Lobato (lobato@netjen.com.br); <i>Ciência/Tecnologia:</i> Ricardo Souza (ricardosouza@netjen.com.br); <i>Livros:</i> Ralph Peter (ralphpeter@agenteliterariopalh.com.br); <i>Comercial:</i> comercial@netjen.com.br <i>Publicidade Legal:</i> lilian@netjen.com.br	<i>Webmaster/TI:</i> Fabio Nader; <i>Editoração Eletrônica:</i> Ricardo Souza. <i>Revisão:</i> Maria Cecília Camargo; <i>Serviço informativo:</i> Agências Brasil, Senado, Câmara, EBC, ANSA. Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.	Jornal Empresas & Negócios Ltda Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080 Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br) Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90 JUCESP, Nire 35218211731 (6/6/2003) Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.
Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.		ISSN 2595-8410