KnowBe4

Relatório de benchmark de phishing

AMÉRICA DO SUL, 2025

Explicando o risco humano e reduzindo as taxas de cliques de phishing

Reduzir os riscos de phishing é fundamental para o gerenciamento eficaz de riscos humanos (HRM).

Todo ataque de phishing bem-sucedido depende de uma pessoa confiável para realizar uma ação específica, como clicar em um hiperlink. Mesmo que um e-mail de phishing consiga passar pelas defesas técnicas, ele ainda será ineficaz se o destinatário o denunciar, excluir ou não interagir com ele.

Além de aprimorar suas defesas técnicas com um produto antiphishing que usa tecnologia de IA, as organizações também podem reduzir significativamente o risco de phishing por meio de treinamento de conscientização em segurança (SAT) com melhores práticas.

O primeiro passo para qualquer estratégia eficaz de mitigação de riscos é entender o perfil de risco de sua organização e como ela se compara a outras do mesmo setor, porte organizacional e região geográfica. Em seguida, é necessário identificar a suscetibilidade real da sua organização ao risco de phishing e, em particular, quem poderia interagir com um e-mail de phishing. Esses insights permitirão que você ofereça segurança oportuna e personalizada, como programas de treinamento sob medida e coaching em tempo real.

O relatório de benchmark de phishing por setor da KnowBe4 constitui a etapa inicial dessa estratégia. No relatório deste ano, analisamos um total de 67.718.305 simulações de phishing entre 14.508.441 usuários em 62.460 organizações durante um período de três anos para mostrar a Phish-prone™ Percentage (porcentagem de propensão ao phishing, PPP) de organizações em 19 setores e sete regiões geográficas.

Este guia oferece uma visão geral das principais descobertas relacionadas à América do Sul.

Como calculamos a Phish-prone Percentage

A PPP é a porcentagem de funcionários de uma organização que provavelmente será vítima de ataques de engenharia social ou phishing. Em outros lugares, você talvez veja isso descrito como “taxa de cliques de simulação de phishing”.

Fase um

Resultados de base do teste de phishing

Antes de qualquer treinamento da KnowBe4, enviamos uma simulação inicial de phishing. Essa simulação é usada para identificar os riscos e calcular a PPP de base de uma organização.

Fase dois

Resultados do teste de phishing em 90 dias de treinamento

Os funcionários recebem o treinamento de conscientização em segurança da KnowBe4. Outra simulação é enviada para recalcular a PPP da organização e medir a eficácia do programa de treinamento.

Fase três

Resultados do teste de phishing depois de um ano ou mais de treinamento contínuo

Depois de 12 meses de treinamento de conscientização em segurança da KnowBe4, a PPP é calculada novamente para quantificar com mais precisão a eficácia do programa de treinamento.

Benchmarks internacionais de phishing em 2025

Nas diferentes regiões, as PPPs de base mais altas foram encontradas na América do Sul (39,1%), na América do Norte (37,1%) e na Austrália e Nova Zelândia (36,8%).

As organizações com mais de 1.000 funcionários sediadas na Austrália e na Nova Zelândia foram as mais propensas a phishing globalmente, com 44,6% de cliques em hiperlinks de phishing simulados. O nível de risco mais baixo foi encontrado em pequenas organizações (de 1 a 249 funcionários) na Ásia e no Reino Unido e Irlanda, com um quarto (24,3%) dos funcionários clicando nos links.

Todas as regiões alcançaram taxas médias de melhoria acima de 80%, sendo a América do Norte a mais alta (89,5%) e a América do Sul em segundo lugar (88,9%).

		Fase um – Resultados de base			Fase dois – 90 dias			Fase três – 1 ano ou mais		
	Porte da organização	**1–249 funcionários**	**250–999 funcionários**	**1.000 ou mais funcionários**	**1–249 funcionários**	**250–999 funcionários**	**1.000 ou mais funcionários**	**1–249 funcionários**	**250–999 funcionários**	**1.000 ou mais funcionários**
Região	**América do Norte**	26%	31,1%	42%	21,1%	21,2%	18,5%	3,7%	3,9%	4,1%
		TOTAL: 37,1%			**TOTAL: 19,6%**			**TOTAL: 3,9%**		
	África	27,9%	30,1%	35,8%	24,9%	28%	20%	2,2%	9,2%	5,1%
		TOTAL: 34,9%			**TOTAL: 21,1%**			**TOTAL: 5,3%**		
	Ásia	24,3%	27,6%	29%	18,9%	19,1%	17,6%	5,1%	4,5%	5,4%
		TOTAL: 28,6%			**TOTAL: 17,9%**			**TOTAL: 5,2%**		
	Austrália e Nova Zelândia	25%	29,2%	44,6%	23,2%	23%	16,6%	3,9%	6,1%	4,7%
		TOTAL: 36,8%			**TOTAL: 19,9%**			**TOTAL: 4,9%**		
	Europa	24,9%	26,7%	34,9%	20,7%	21,6%	20,5%	3,9%	4,4%	5,3%
		TOTAL: 32,5%			**TOTAL: 20,7%**			**TOTAL: 5%**		
	América do Sul	30,2%	26,3%	42,8%	23,3%	23,1%	16,9%	3,4%	5,1%	4,5%
		TOTAL: 39,1%			**TOTAL: 18,2%**			**TOTAL: 4,5%**		
	Reino Unido e Irlanda	24,3%	28,5%	36%	22,1%	22,1%	17,1%	4%	4,1%	5,3%
		TOTAL: 32,9%			**TOTAL: 19%**			**TOTAL: 4,8%**		

América do Sul | *Por Rafael da Silva e Bex Bailey*

Com 39,1%, a PPP inicial em nossa base de clientes na América do Sul foi maior do que em qualquer outra região. Sem participar do treinamento de melhores práticas em segurança cibernética, quase dois em cada cinco funcionários clicarão automaticamente em links de phishing.

A boa notícia é que, depois da implementação do treinamento e das simulações de phishing, essa taxa de cliques fica bem alinhada com a média global, caindo para 18,2% após 90 dias e para 4,5% após um ano.

As PPPs iniciais foram extremamente altas nas organizações de serviços ao consumidor, com 59,9%, seguidas por seguros (48,6%), energia e serviços públicos (48,3%), serviços financeiros (47,9%) e atacado e varejo (42,7%). Todos esses setores tiveram uma redução drástica do risco após um ano de treinamento e simulações, especialmente no caso dos serviços ao consumidor, em que a PPP média diminuiu para 1,9%. Em outros setores, as PPPs caíram para 5,2% em seguros, 4,4% em energia e serviços públicos, 3,6% em serviços financeiros e 4,1% em atacado e varejo.

Quando analisamos os dados por porte organizacional, vemos que as organizações maiores, com mais de 1.000 funcionários, correm o maior risco no início do programa de SAT, o que é semelhante à tendência global. Isso faz muito sentido: mais pessoas equivalem a uma superfície de risco humano maior a ser protegida. Portanto, é mais provável que um funcionário desavisado clique em um link de phishing.

No entanto, ao contrário da tendência global, as organizações menores, com 1 a 249 funcionários, na América do Sul, apresentaram um nível de risco mais alto do que as organizações do mesmo porte em outras regiões. A PPP média global dessas empresas foi de 24,6%, enquanto a média sul-americana foi de 30,2%. Mais uma vez, há boas notícias a esse respeito. Essas organizações obtiveram a menor taxa de cliques regional após um ano de treinamento e simulações em melhores práticas, com a PPP caindo para apenas 3,4%, um pouco abaixo da média global de 3,6%.

América do Sul	Phish-prone Percentage		
Porte da organização	**Fase um – Resultados de base**	**Fase dois – 90 dias**	**Fase três – 1 ano ou mais**
1–249	30,2%	23,3%	3,4%
250–999	26,3%	23,1%	5,1%
1.000 ou mais	42,8%	16,9%	4,5%
PPP média em organizações de todos os portes	**39,1%**	**18,2%**	**4,5%**

Fatores que aumentam o risco humano na América do Sul

No documento Risco em Foco 2025: Apresentação para Conselho da América Latina, a Global Foundation for Internal Audit destaca a segurança cibernética como o principal risco em 2025 e prevê que ela permanecerá nessa posição por pelo menos os próximos três anos. Diversos fatores estão impulsionando esse risco em toda a região, principalmente à medida que as pessoas interagem com novas tecnologias e são alvo de novas ameaças.

Agora, os funcionários estão sendo reconhecidos como uma linha crucial de defesa contra ameaças cibernéticas

Transformação e revolução digital

A América do Sul tem registrado uma adoção rápida, porém desigual, de novas tecnologias, impactando todas as áreas da vida, desde o setor bancário até a educação e a saúde. Embora a inclusão digital traga uma série de benefícios, ela também cria novos riscos que devem ser tratados. No relatório Cybersecurity Economics for Emerging Markets, o Banco Mundial destaca como a transformação digital da América Latina e do Caribe ultrapassou a capacidade de segurança cibernética da região.

Além disso, o ritmo desigual de adoção criou uma "divisão digital" entre regiões e grupos socioeconômicos. Essa situação impõe desafios únicos a serem superados, como a complexidade de aumentar a conscientização em segurança cibernética em vários segmentos da população.

Essa combinação entre a transformação digital que cria novos meios de ataque e os diferentes níveis de maturidade da segurança cibernética torna as organizações sul-americanas alvos atraentes para os criminosos cibernéticos.

Especificamente, a "desigualdade da segurança cibernética" parece ter aberto a porta para o aumento dos ataques de ransomware. No LatAm Cyber Summit 2024 Annual Report, a Cyber Series destaca que as empresas latino-americanas têm a maior porcentagem de uso de ransomware em ataques a organizações (79% contra a média global de 53%).

Não vamos nos esquecer da IA!

As tecnologias que usam IA desempenham um papel importante na revolução digital mundial e na América do Sul. Conforme divulgado pelo PNUD para a América Latina e o Caribe, a previsão é que a IA contribua com até 5,4% do PIB da América Latina até 2030, o equivalente a US$ 0,5 trilhão.

Novamente, isso é uma faca de dois gumes. Embora as pessoas possam colher os benefícios da IA tanto em casa quanto no trabalho, a segurança da IA é uma preocupação global, com os invasores encontrando novos pontos de entrada nos sistemas e até mesmo manipulando os modelos de dados por conta própria. Assim como em outras regiões, a América do Sul também é vulnerável ao aumento da escala e da sofisticação dos ataques cibernéticos que podem ser criados com a IA, como campanhas avançadas de phishing e cargas de malware, incluindo ransomware.

As pessoas sempre criarão riscos, especialmente ao interagir com tecnologias modernas

O risco humano é um fator com o qual todas as organizações precisam lidar. As pessoas são o nosso maior ativo, mas erros serão cometidos, e riscos serão assumidos. A disparidade e, talvez, a imaturidade dos níveis de conscientização em segurança entre os funcionários da América do Sul podem ser observadas nesse estudo, com a região apresentando a PPP inicial mais alta do mundo.

Infelizmente, essa falta de conscientização geral é reforçada por uma escassez de habilidades em segurança cibernética. No relatório Building a Skilled Cyber Security Workforce in Latin America, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) destaca que a segurança cibernética é a categoria que mais cresce em termos de ofertas de emprego na região, mas o alto nível de exigência em termos de habilidades significa que muitas organizações podem ter dificuldades para encontrar o talento que procuram entre os grupos de candidatos.

Após um ano de treinamento contínuo, a maioria dos setores e empresas de todos os portes alcançou taxas de PPP de um dígito, com uma redução média de 78% em relação aos níveis iniciais

Pontos principais

Na América do Sul, as organizações enfrentam desafios específicos de segurança cibernética, incluindo riscos elevados de phishing na linha de base e rápida inclusão digital.

- **A PPP inicial global mais alta (39,1%) cai para 4,5% com o treinamento de segurança contínuo**
- **Os serviços ao consumidor lideram a PPP de base (59,9%), mas melhoram drasticamente, atingindo 1,9%**
- **As organizações maiores enfrentam inicialmente um risco humano maior; as empresas menores também superam as médias globais**
- **A rápida adoção da IA e a escassez de habilidades ampliam as ameaças e vulnerabilidades**
- **O treinamento contínuo de conscientização permanece fundamental para reduzir o risco humano em todos os setores**

A alta PPP inicial da América do Sul destaca uma necessidade urgente de programas robustos de conscientização em segurança. O treinamento contínuo e o gerenciamento proativo de riscos podem diminuir significativamente as ameaças de phishing. Ao promover uma cultura de segurança cibernética, as organizações permanecem resilientes em um cenário digital que evolui rapidamente.

Para saber mais, acesse **KnowBe4.com**

Precisamos de abordagens de treinamento mais personalizadas, relevantes e adaptáveis para nos mantermos à frente das ameaças crescentes

Sobre a KnowBe4

A KnowBe4 capacita seus funcionários a tomar decisões de segurança mais inteligentes todos os dias. Usada por mais de 70 mil organizações em todo o mundo, a KnowBe4 ajuda a fortalecer sua cultura de segurança e gerenciar os riscos humanos. Ela oferece uma abrangente plataforma assistida por IA para o gerenciamento de riscos humanos, criando uma camada de defesa adaptativa que fortalece o comportamento dos usuários contra as mais recentes ameaças em segurança cibernética. A plataforma HRM+ inclui módulos com treinamentos em conscientização e conformidade, segurança de e-mail na nuvem, coaching em tempo real, antiphishing por crowdsourcing, AI Defense Agents e muito mais. Como única plataforma global de segurança em sua categoria, a KnowBe4 usa ferramentas, técnicas e conteúdos personalizados e relevantes para oferecer proteção em segurança cibernética, mobilizando os funcionários a transformar a maior superfície de ataque no maior ativo de uma organização.

Para obter mais informações, acesse **www.KnowBe4.com**

KnowBe4

KnowBe4 Brazil | Av. Ibirapuera, 2315, Indianópolis, CEP 04029-200, São Paulo-SP
Tel: +55 (0800) 761 2668 | www.KnowBe4.com | Sales@KnowBe4.com