FORTINET
Training Institute

Conscientização e treinamento em segurança em 2024

Relatório de pesquisa global

Metodologia

As descobertas neste relatório são baseadas em respostas obtidas de entrevistas on-line com 1.850 profissionais de nível executivo e de nível gerencial em organizações que têm conscientização e treinamento em segurança em vigor. As entrevistas foram realizadas pela Sapio Research em maio e junho de 2024. As respostas foram obtidas de indivíduos nos seguintes 29 países locais:

- Argentina
- Austrália
- Brasil
- Canadá
- Colômbia
- França
- Alemanha
- Hong Kong
- Índia
- Indonésia
- Israel
- Itália
- Japão
- China continental
- Malásia
- México
- Holanda
- Nova Zelândia
- Filipinas
- Singapura
- África do Sul
- Coreia do Sul
- Espanha
- Suécia
- Taiwan
- Tailândia
- Emirados Árabes Unidos
- Reino Unido
- Estados Unidos da América

Os resultados gerais são precisos para ± 2,3% a um limite de confiança de 95%.

Tamanho da empresa

100–499 funcionários **22%**
500–999 funcionários **21%**
1.000–2.499 funcionários **21%**
2.500–4.999 funcionários **18%**
Mais de 5.000 funcionários **18%**

Sexo

67% dos entrevistados eram do sexo masculino
33% dos entrevistados eram do sexo feminino

Total de entrevistados: 1.850

AÁsia-Pacífico **30%**
Europa, Oriente Médio e África **27%**
América do Norte **22%**
América Latina **22%**

Tipo de função

7% ocuparam cargos de proprietário
26% ocuparam cargos executivos de nível C
7% ocuparam cargos de vice-presidente
18% ocuparam cargos de chefe de departamento
17% ocuparam cargos de diretor
25% ocuparam cargos de gerente

Três principais setores de negócios:

Manufatura **17%**
Serviços financeiros **13%**
Serviços profissionais e tecnologia **11%**

Resumo executivo

Os líderes reconhecem que as pessoas são uma primeira linha de defesa crucial contra-ataques cibernéticos. É por isso que muitos executivos estão preocupados com o nível de conscientização sobre riscos cibernéticos de seus funcionários e ainda mais preocupados com novas ameaças geradas por IA, que já estão provando serem mais difíceis de detectar e bloquear do que ataques cibernéticos "tradicionais".

As organizações estão se preparando para ataques de IA

- **62%** dos líderes esperam que os funcionários sejam vítimas de ataques nos quais os cibercriminosos usam IA.
- **95%** estão usando, implementando ou pesquisando soluções de IA para evitar ataques cibernéticos.
- **80%** relatam que as atitudes em relação ao treinamento de conscientização de segurança melhoraram devido ao uso de IA por criminosos.
- Apesar das preocupações com os riscos da IA, **31%** das organizações não gerenciam ou monitoram como os funcionários usam aplicativos de IA.

Os líderes precisam de funcionários com reconhecimento cibernético

- **67%** com a falta de conscientização geral sobre segurança de seus funcionários, contra **56** em 2023.
- Principais determinantes para adotar um programa de conscientização e treinamento em segurança:
  - Violação de segurança anterior ou ameaça de uma violação de segurança **(52%)**
  - Patrocínio corporativo **(21%)**
  - Requisitos regulatórios e de conformidade **(13%)**
- **94%** estão interessados em implementar políticas de segurança cibernética mais rigorosas para usuários de alto risco.

O treinamento é fundamental para aumentar a conscientização sobre segurança

- **97%** dos tomadores de decisão dizem que mais treinamento e conscientização ajudariam a reduzir os ataques cibernéticos, um pouco mais do que **93%** em 2023.
- **89%** relatam melhorias na postura de segurança de sua organização após implementar conscientização e treinamento em segurança.
- Os tópicos mais importantes de conscientização e treinamento em segurança são:
  - Segurança de dados **(48%)**
  - Privacidade de dados **(41%)** que é consistente com conclusões de 2023.

O treinamento precisa ser envolvente e intencional

- Em média, **81%** das organizações sentiram que três horas de treinamento por ano eram necessárias para aumentar a conscientização cibernética.
- **75%** das campanhas de conscientização de segurança são planejadas com antecedência e entregues mensalmente **(34%)** ou trimestralmente **(47%).**
- **86%** dos líderes estão satisfeitos com suas soluções atuais de conscientização e treinamento em segurança. Daqueles que relataram estar insatisfeitos, **41%** disseram que seus programas não tinham um conteúdo envolvente.

Uma visão nova e expandida da conscientização e do treinamento

O tópico de conscientização e treinamento em segurança fazia parte anteriormente do Relatório de pesquisa global sobre lacunas de habilidades em segurança cibernética da Fortinet.. A crescente importância dos fatores humanos de segurança cibernética nos levou a emitir uma pesquisa independente em 2024, aprofundando-se no tópico.

Embora muitas perguntas tenham sido feitas pela primeira vez este ano e não tenham base para comparação, incluímos comparações selecionadas ano após ano em relação aos dados do nosso Resumo de pesquisa global de conscientização e treinamento em segurança de 2023

INTRODUÇÃO

Não são permitidos links fracos

A conscientização e o treinamento em segurança dos funcionários se tornaram preocupações de alto nível para líderes que desejam reforçar as defesas cibernéticas de suas organizações de todas as maneiras possíveis.

Este relatório apresenta as descobertas da pesquisa relacionadas ao estado da conscientização e treinamento cibernéticos em todo o mundo:

- Onde os líderes estão se concentrando;
- Como as organizações estão lidando com a urgência;
- O que mantém os tomadores de decisão acordados à noite;

À medida que a IA continua a permear todos os aspectos de nossas vidas, os líderes de negócios estão cada vez mais à frente das ameaças relacionadas à IA, desde esquemas falsos profundos e ataques de phishing de próximo nível, bem como o uso de modelos de linguagem grandes, companheiros de codificação, geradores de imagem e outras ferramentas de IA pelos funcionários. Apesar dessas ansiedades, quase um terço das organizações não ou o uso de aplicativos de IA pelos funcionários, sugerindo uma lacuna nas políticas corporativas para alguns.

Hoje, os cibercriminosos estão usando a IA para dificultar a detecção de esquemas de phishing. Como o phishing tem como alvo usuários individuais diretamente, as organizações estão esmagadoramente focadas em ensinar funcionários como não ser vítima desses ataques. Quase todos os entrevistados dizem que a prevenção de phishing é um componente de seus programas e planos de treinamento. Outras prioridades principais para conscientização e treinamento incluem segurança e privacidade de dados.

A pesquisa deste ano também esclarece como as organizações tendem a abordar a conscientização e o treinamento em segurança. Ele mostra que a maioria é altamente intencional, pré-planejando tópicos de treinamento e oferecendo parcelas de conteúdo em intervalos regulares ao longo do ano. A maioria dos líderes apoia esses esforços e acredita que mais treinamento e conscientização são necessários.

Conforme observado em nosso Relatório de Pesquisa Global sobre Lacuna de Habilidades de Segurança Cibernética de 2024, as organizações veem a conscientização e o treinamento como parte de uma abordagem de três vertentes para mitigar o risco cibernético, que também inclui contratar e reter pessoal de segurança de TI qualificado e implementar soluções de segurança cibernética eficazes.

Em 2024, estamos vendo o papel elevado que a apólice está desempenhando, ou pode desempenhar, na segurança cibernética, seja relacionado ao gerenciamento do comportamento dos funcionários on-line ou à crescente popularidade do seguro cibernético. Essas descobertas sugerem que os líderes entendem que a segurança cibernética está enraizada na cultura organizacional, e que política, conscientização e treinamento contribuem para isso.

62% das organizações esperam que os funcionários sejam vítimas de mais ataques cibernéticosno futuro devido ao uso malicioso da IA pelos invasores.

As organizações estão se preparando para ataques orientados por IA

Os usuários corporativos e cibercriminosos adotaram a IA para acelerar, dimensionar e simplificar seu trabalho. Os líderes de negócios estão cientes das ameaças representadas pelo uso indevido interno de ferramentas de IA e ataques externos habilitados para IA, e estão ansiosos para fazer algo sobre eles.

A maioria (62%) dos entrevistados da pesquisa relatam que esperam que os funcionários sejam vítimas de mais ataques à medida que os criminosos aumentam seu uso da IA. Quase todos (96%) estão pesquisando, implementando ou já têm planos de resposta a incidentes relacionados ao combate a ameaças externas relacionadas à IA, que hoje incluem deepfakes de áudio e vídeo difíceis de detectar projetados para acionar transações fraudulentas, bem como esquemas de phishing altamente direcionados. Novos tipos de ataques habilitados para IA continuam a surgir.

A maioria dos entrevistados (80%) afirmam que o conhecimento de toda a empresa sobre ataques de IA tornou suas organizações mais abertas à conscientização e treinamento em segurança. A maioria (95%) também relata ter ou desenvolver políticas de segurança para gerenciar riscos internos relacionados ao uso de ferramentas de IA.

Essas políticas tendem a girar em torno do vazamento de informações, incluindo dados privados ou proprietários que aparecem em saídas de IA voltadas para o público, divulgação inadvertida de segredos ou anonimização de informações de identificação pessoal.

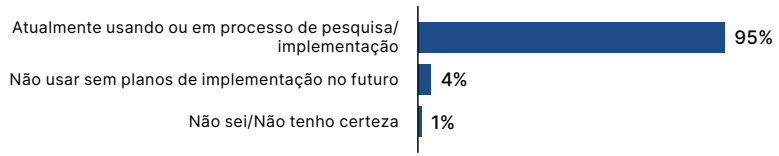
Os vazamentos podem acontecer muito facilmente, por exemplo, quando um funcionário copia conteúdo corporativo em um modelo de linguagem grande (LLM) para edição ou compõe um prompt detalhado para responder a uma pergunta. Essas entradas podem ser usadas para treinar modelos de IA ou serem consultadas por partes externas, fazendo com que informações privadas sejam tornadas públicas.

Embora a criação de políticas para controlar o uso da IA corporativa seja importante, em quase um terço (31%) das organizações, essas políticas não são complementadas com gerenciamento ou monitoramento ativo do uso da IA pelos funcionários, deixando possíveis vulnerabilidades desmarcadas.

As organizações estão usando IA para segurança cibernética

Quase todos os entrevistados da pesquisa (95%) dizem que sua organização está atualmente usando soluções de segurança orientadas por IA para evitar ataques de segurança cibernética ou está no processo de pesquisar ou implementar essas ferramentas.

Porcentagem de organizações que usam ou adotam IA para segurança cibernética



PROFUNDIDADE

Treinamento, conscientização e confiança andam de mãos dadas

O suporte mais forte para conscientização e treinamento aumenta a confiança da IA

As organizações com mais suporte interno para conscientização e treinamento tendem a ter mais confiança sobre a capacidade dos funcionários de lidar com ameaças relacionadas à IA:

- 60% dos entrevistados com forte suporte para treinamento disseram que achavam que os funcionários cairiam para mais ataques devido à IA.
- 66% das organizações com suporte moderado para treinamento estão preocupadas com o risco de mais funcionários.
- 70% das organizações com pouco ou nenhum suporte para treinamento preocupam-se que mais funcionários se enquadrarão em ataques baseados em IA.

A maioria das organizações ainda não gerenciam o uso de IA pelos funcionários

A maioria (53%) dos entrevistados dizem que sua organização ainda está implementando ou não tem processos para gerenciar e monitorar o uso de ferramentas de IA pelos funcionários:

- 31% não têm medidas em vigor e outras

10% não sabem ou não têm certeza.

- 22% dizem que estão trabalhando nisso, mas não terminaram de implementar processos de monitoramento e gerenciamento.

Daqueles com medidas em vigor, 21% sancionam aplicações de IA específicas para uso interno e 16% impõem controles técnicos.

As preocupações sobre as ameaças de IA variam de acordo com o setor

Os entrevistados em determinados setores estão muito mais preocupados com a IA fazendo com que os funcionários caiam em busca de ameaças:

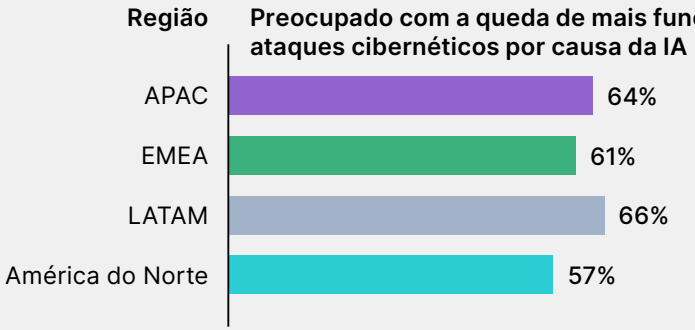
- 70% das empresas de mídia e entretenimento esperam que os funcionários caiam em mais ataques devido ao uso da IA pelos invasores.
- Os governos estaduais e locais em segundo lugar, com 68%.
- Empresas de energia e serviços públicos (59%), saúde (57%) e varejo (56%)

Menos de um quarto das organizações **(21%)** sancionar aplicativos de IA específicos para uso do funcionário.

Destaques regionais

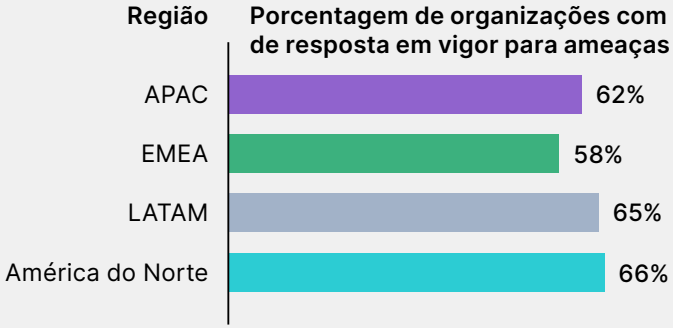
As preocupações com IA são maiores na América Latina

As organizações na América Latina (LATAM) são mais propensas a pensar nos funcionários cairão cada vez mais em ataques cibernéticos devido ao uso de IA pelos invasores.



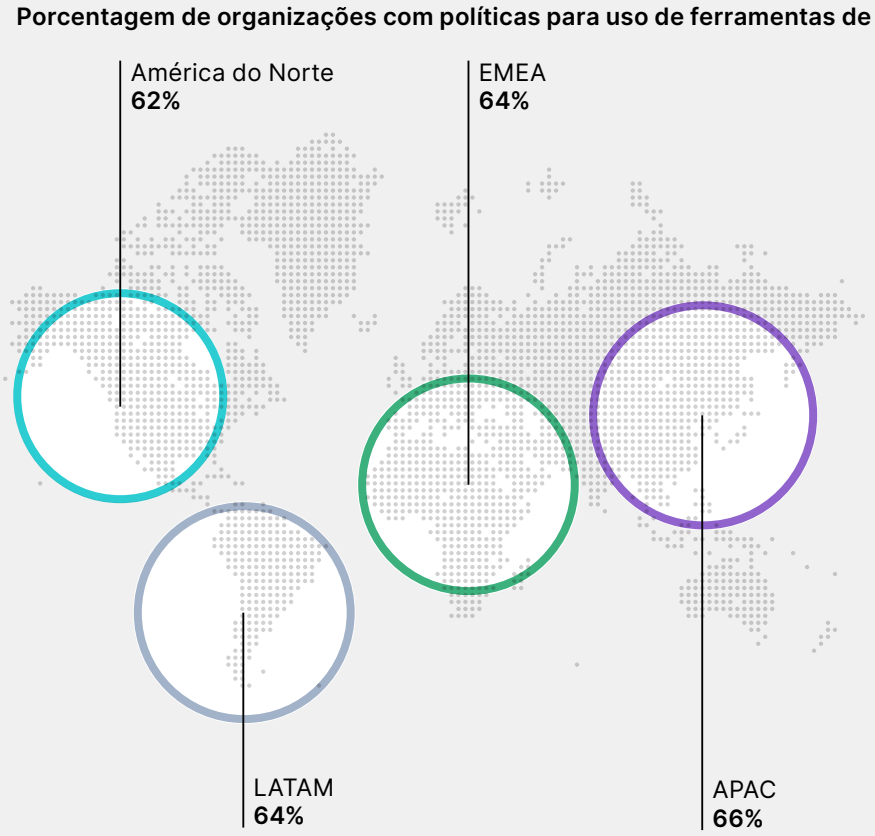
Os planos de resposta a incidentes são menos prováveis na Europa,Oriente Médio e África

Menos empresas na Europa, Oriente Médio e África (EMEA) têm planos de resposta a incidentes para as ameaças relacionadas à IA, enquanto aquelas na América do Norte são mais propensas a ter esses planos.



A maioria das organizações tem políticas de segurança para controlar Ferramentas de IA

Os entrevistados em todas as regiões são quase igualmente propensos a ter políticas para controlar o uso de ferramentas de IA.



A maioria (**67%**) dos tomadores de decisão acham que seus funcionários não têm consciência sobre segurança.

Os líderes precisam de funcionários com reconhecimento cibernético

Quer as ameaças estejam relacionadas a novas tecnologias como IA ou sejam ataques cibernéticos mais convencionais, os tomadores de decisão permanecem preocupados com o fato de que os funcionários podem não ter o grau de conscientização de segurança de que precisam para proteger a si mesmos e suas organizações.

Pouco mais de dois terços (67%) dos entrevistados dizem que acreditam que seus funcionários não têm conscientização e conhecimento sobre segurança, um aumento notável em relação a 56% em 2023. Isso se correlaciona com as constatações do Relatório de Pesquisa Global da Fortinet sobre a Lacuna de Habilidades de Segurança Cibernética de 2024, em que a falta de conscientização sobre segurança é considerada uma das três principais causas de violações.

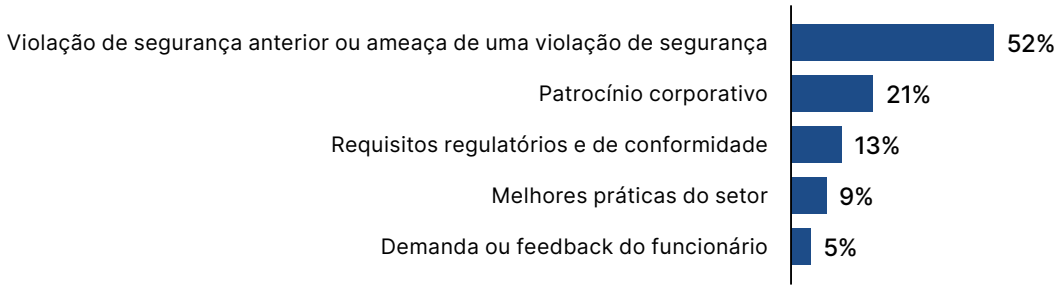
Dadas essas descobertas, não é surpreendente que o suporte para conscientização e treinamento em segurança seja geralmente alto. Quase todos os responsáveis pela tomada de decisões (96%) dizem que sua equipe de liderança apoia a implementação de treinamento para aumentar a conscientização sobre segurança cibernética dos funcionários. Líderes de TI (57%) e líderes de segurança (54%) são geralmente os defensores da conscientização e treinamento em segurança, com CEOs/chefes de organizações em um terço distante, com 40%.

Ao mesmo tempo, reconhecendo a gravidade da situação, 94% dos líderes também dizem que estariam interessados em aplicar políticas de segurança cibernética mais rigorosas a usuários que exibem comportamento de alto risco. Esses usuários podem ser identificados por meio de métodos como campanhas de phishing realizadas pela empresa que revelam quais funcionários são mais propensos a sofrer ataques baseados em IA.

A conscientização das ameaças impulsiona a adoção do treinamento

A maioria das organizações estão motivadas a introduzir conscientização e treinamento em segurança com base em sua experiência sendo violada ou conhecimento de ameaças em seu setor. Motivos das organizações para adotar adotarem conscientização e treinamento em segurança

Motivos das organizações para adotarem conscientização e treinamento em segurança



PROFUNDIDADE

Aplacar o risco cibernético é uma prioridade corporativa crescente

O seguro de conscientização, treinamento e segurança cibernética tem fatores semelhantes

As organizações investem em seguro de segurança cibernética porque:

- É uma prioridade corporativa (51%).
- Mais violações estão ocorrendo em geral (46%).
- Mais violações estão ocorrendo em seu setor (42%).

Isso alinha-se aos principais motivos para implementar conscientização e treinamento em segurança: ameaça de violações ou violações reais (52%) e patrocínio corporativo (21%).

O seguro de segurança cibernética está crescendo em popularidade

A maioria das organizações (95%) priorizou o seguro de segurança cibernética.

- 77% têm seguro de segurança cibernética.
- 18% estão procurando obtê-lo nos próximos 12 meses.

Organizações com 1.000 a 4.999 funcionários são mais propensas a ter seguro de segurança cibernética:

- 1.000 a 2.499 funcionários (81%)
- 2.500 a 4.999 funcionários (81%)
- Mais de 5.000 funcionários (77%)
- 100 a 999 funcionários (74%)

Os recursos são fundamentais para obter conscientização e o treinamento em segurança decolarem

Quando questionados sobre o que impedia as organizações de implementar um programa de conscientização e treinamento em segurança no passado, os entrevistados disseram:

- Recursos humanos limitados (31%)
- Outras prioridades corporativas — conscientização e treinamento classificados em níveis inferiores (26%)
- Orçamento limitado (22%)
- Não achou que precisava de um programa (18%)

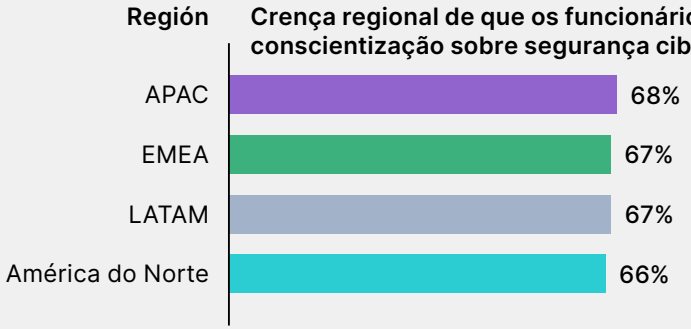
As grandes organizações (mais de 5.000 funcionários) tendem a ter programas de conscientização e treinamento de segurança mais estabelecidos, com uma duração média de 12 anos em comparação com sete para aqueles com 100 a 999 funcionários.

Um terço **(31%)** dos entrevistados dizem que as restrições de recursos humanos os impediram de implementar programas de conscientização e treinamento em segurança.

Destaques regionais

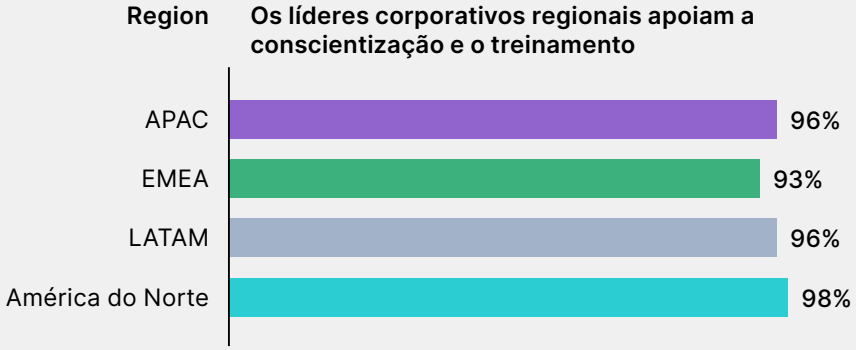
Preocupações sobre conscientização e treinamento de segurança insuficientes são generalizadas

As organizações em todas as regiões têm preocupações aproximadamente equivalentes de que os funcionários não tenham conscientização sobre segurança cibernética.



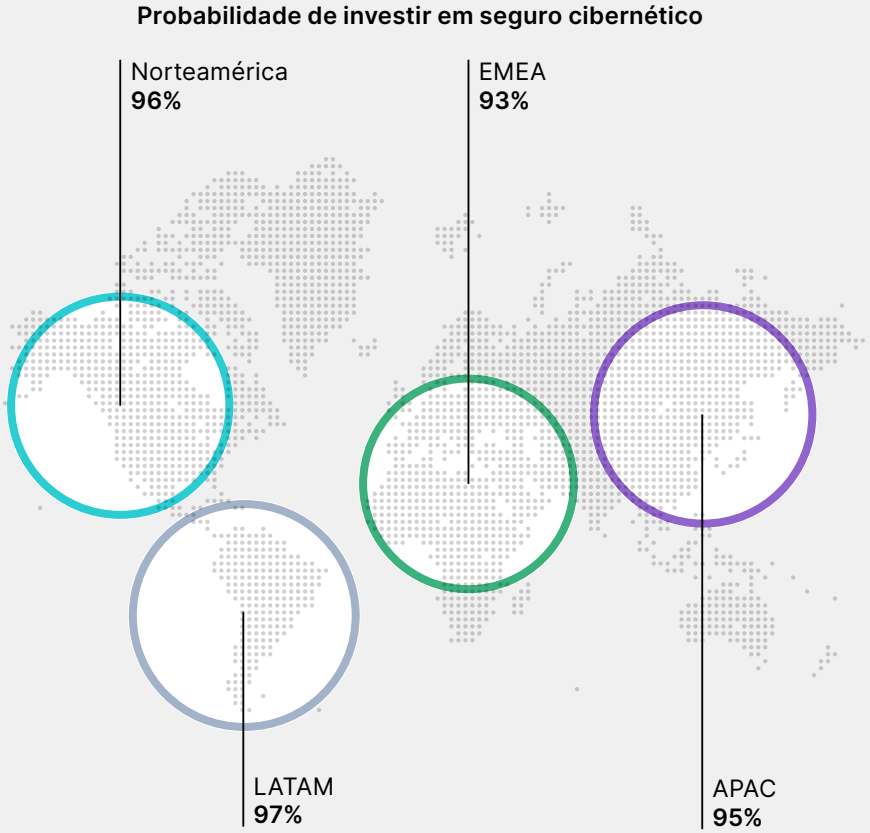
O suporte à conscientização e treinamento em segurança também é predominante

As equipes de liderança em todas as regiões são favoráveis à oferta de conscientização e treinamento de segurança para os funcionários.



As organizações na LATAM são mais propensas a investir em seguro cibernético

Mais entrevistados na LATAM dizem que adquiriram ou estão planejando adquirir seguro cibernético do que em qualquer outra região.



97% dos tomadores de decisão acreditam que o aumento da conscientização sobre segurança ajudaria a reduzir os ataques cibernéticos

O treinamento é fundamental para aumentar a conscientização sobre segurança

Os tomadores de decisão concordam que uma maior conscientização melhoraria a postura de segurança cibernética de sua organização e que campanhas e treinamentos internos são maneiras eficazes de gerenciar ainda mais os riscos.

De acordo com a pesquisa deste ano, 97% dos líderes acreditam que o aumento da conscientização dos funcionários fortaleceria a segurança cibernética. Isso aumentou ligeiramente em relação a 93% no Resumo de pesquisa global do Serviço de conscientização e treinamento em segurança de 2023.

Os entrevistados parecem ter um bom motivo para manter essa visão. Uma maioria esmagadora (89%) diz que sua organização viu pelo menos alguma melhoria em sua postura de segurança após a implementação da conscientização e do treinamento em segurança, e nem um único entrevistado alegou não ver nenhuma melhoria. A maioria (86%) adiciona que seus funcionários veem a conscientização e o treinamento em segurança de forma positiva, com 55% dizendo “muito positiva”.

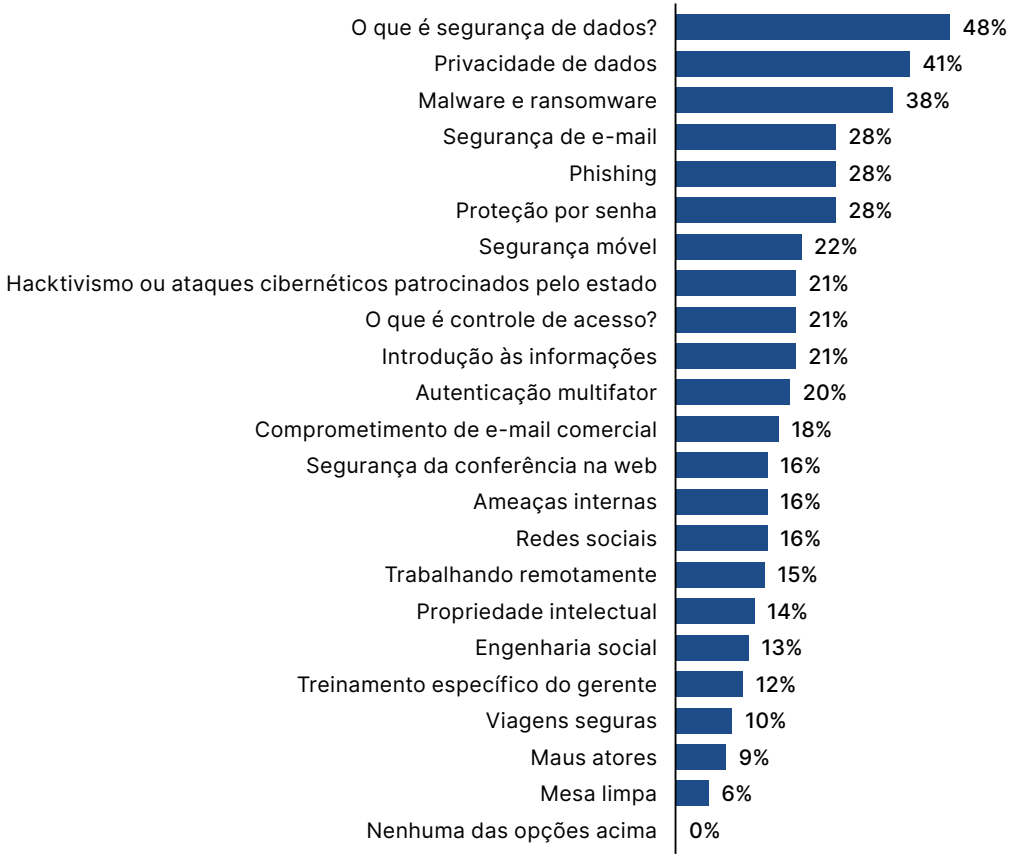
Quando se trata de prioridades de treinamento, a segurança e a privacidade de dados estão no topo da lista, com 48% e 41%, respectivamente. A conscientização sobre ataques de phishing também é fundamental:

Uma grande parte dos entrevistados (98%) dizem que seus programas incluem ou incluirão campanhas relacionadas a phishing. Isso se alinha ao nosso Relatório de pesquisa global sobre lacunas de habilidades em segurança cibernética de 2024, descobrindo que ataques de phishing são a segunda forma mais comum de ataque encontrada pelas organizações.

Manter os dados seguros é o mais importante

O que os líderes mais querem é conscientização e treinamento de segurança que ensinam seus funcionários a manter os dados seguros e privados. Isso ecoa as respostas de 2023, o que indicou que os funcionários que sabem como manter dados confidenciais seguros ao trabalhar remotamente eram uma prioridade máxima.

Prioridades de conscientização e treinamento em segurança em 2024



PROFUNDIDADE

O treinamento requer gerenciamento e suporte

Todas as organizações se beneficiam da conscientização e do treinamento em segurança

Independentemente do tamanho, a maioria das organizações relatam pelo menos alguma melhoria em sua postura de segurança após implementar conscientização e treinamento em segurança:

- 100 a 999 funcionários (88%)
- 1.000 a 2.499 funcionários (92%)
- 2.500 a 4.999 funcionários (91%)
- Mais de 5.000 funcionários (88%)

Como uma possível indicação dessas melhorias, mais de dois terços (69%) dos líderes classificam a capacidade média de seus funcionários de identificar um e-mail falsificado como bom ou muito bom.

O apoio à liderança produz melhores resultados

Quando os líderes apoiam fortemente a conscientização e o treinamento em segurança, as organizações são mais propensas a ver alguma ou significativa melhoria após a implementação:

- 96% com suporte de liderança "extensivo" relatam alguma melhoria ou melhoria significativa após a implementação.
- Com "uma certa extensão" de apoio à liderança, isso cai para 79%.
- Apenas 47% das organizações com pouco ou nenhum apoio à liderança relatam alguns ou significativos benefícios após a implementação.

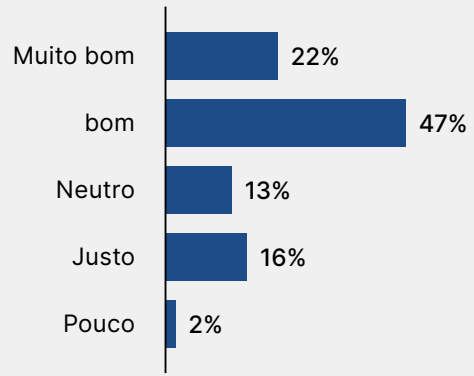
Os funcionários equilibram vários compromissos de treinamento

Embora 86% dos entrevistados digam que seus funcionários veem a conscientização e o treinamento em segurança de forma positiva, mais da metade (58%) acha que a equipe priorizaria outros treinamentos. Gerenciar a "fadiga do treinamento" é uma realidade para as organizações.

Os outros tipos de treinamentos obrigatórios mais comumente vistos são:

- Saúde e segurança (71%)
- Conformidade (66%)
- Atendimento ao cliente (61%)
- Produto ou serviço (61%)

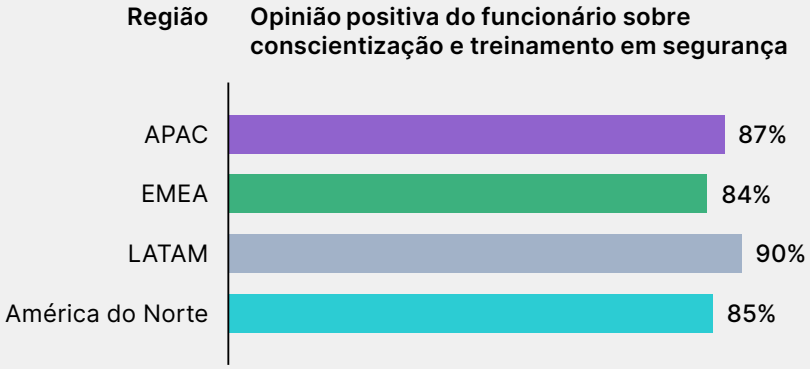
Mais de dois terços (69%) classificariam a média de sua organização capacidade do usuário de identificar um e-mail falsificado como bom ou muito bom



Destaques regionais

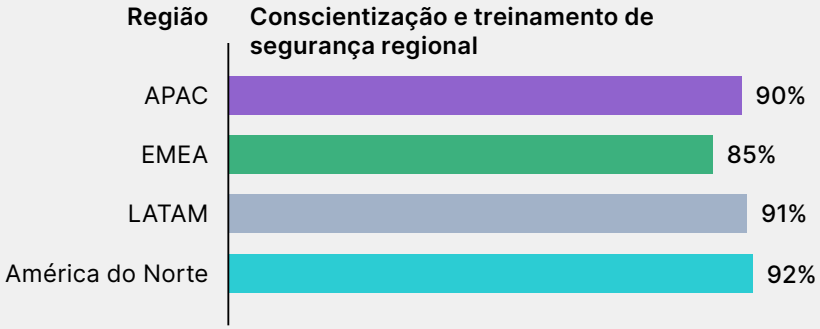
Os funcionários em todas as regiões veem a conscientização e o treinamento em segurança de forma positiva

A LATAM publica o resultado mais alto, com 90%, e a EMEA, com 84%.



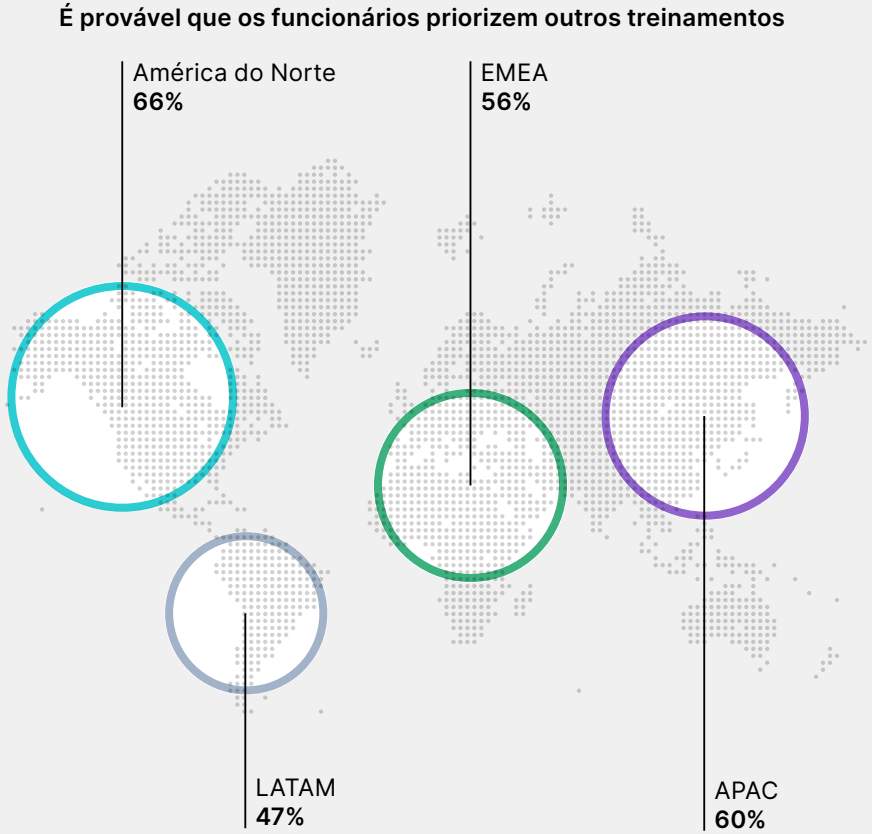
Nem todas as regiões experimentam ganhos igualmente

Os entrevistados na EMEA tiveram menos chances de ver melhorias na segurança cibernética após a implementação do treinamento.



Funcionários da LATAM com menor probabilidade de priorizar outros treinamentos

Os entrevistados na LATAM tinham menos probabilidade de pensar que os funcionários priorizariam outro treinamento em vez de treinamento de conscientização sobre segurança.



41% dos tomadores de decisão que estão insatisfeitos com o treinamento atual têm preocupações de que o conteúdo não seja envolvente.

O treinamento precisa ser intencional e envolvente

Como prova de que a conscientização e o treinamento em segurança são um empreendimento disciplinado e bem considerado na maioria das organizações, 75% dos entrevistados dizem que suas campanhas são planejadas com antecedência, com uma média de três horas de treinamento por ano consideradas suficientes.

Oitenta e um por cento (81%) das organizações realizam conscientização e treinamento em segurança para funcionários mensal ou trimestralmente. Essa regularidade oferece oportunidades de atualizações e reforço, bem como treinamento líquido novo sobre ameaças e tópicos emergentes relevantes para a organização.

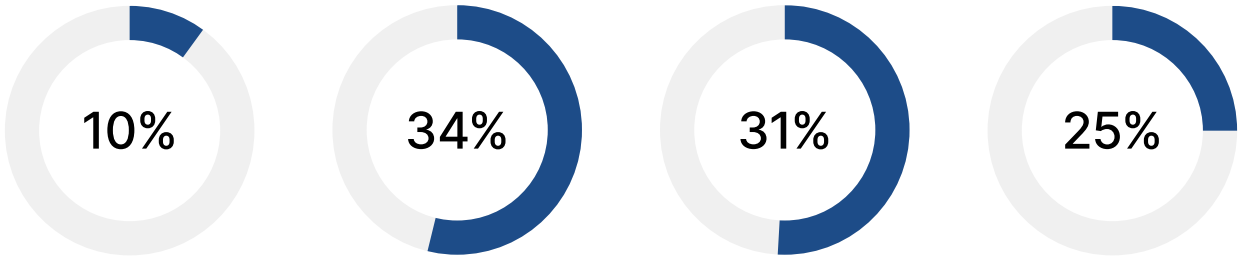
A média de três horas está alinhada com a pesquisa do ano passado, onde 59% dos entrevistados disseram que seria razoável que os funcionários passassem de 1 a 3 horas por ano em treinamento de conscientização sobre segurança. Com as melhores práticas sugerindo um intervalo de 5 a 15 minutos por módulo de aprendizagem (e até 30 minutos para tópicos complexos), o que permite a cobertura de até 12 tópicos discretos no decorrer de um ano.

Embora 86% dos tomadores de decisão digam que estão satisfeitos com sua solução atual de conscientização e treinamento em segurança, entre aqueles não satisfeitos, uma das maiores reclamações de longe foi a falta de conteúdo envolvente, em 41%.

Tempo suficiente para causar impacto

Pouquíssimo tempo alocado para conscientização e treinamento de segurança pode levar a resultados abaixo do ideal. No entanto, exigir muito tempo dos funcionários também pode sobrecarregá-los ou forçá-los a priorizar outros treinamentos obrigatórios. Entre 1,1 e 2,0 horas é a quantidade de tempo mais comum proposta, com três horas como média.

34% dos tomadores de decisão sentem que 1,1 a 2 horas é um período razoável para os funcionários gastarem em conscientização e treinamento de segurança Média: 3 horas



PROFUNDIDADE

A importância da qualidade do conteúdo

A falta de material envolvente é a maior causa de insatisfação

Embora a maioria das organizações esteja muito satisfeita com seu serviço de conscientização e treinamento em segurança (41%), aquelas que estão um pouco ou muito insatisfeitas têm vários motivos:

- Falta de conteúdo envolvente (41%)
- Integração complicada (26%)
- Serviço de atendimento ao cliente ruim (23%)
- Falta de recursos e relatórios (9%)

As organizações confiam numa combinação de tecnologias para gerenciar o treinamento

Os entrevistados têm acesso a diferentes aplicativos para diferentes treinamentos:

- 51% gerenciam a conscientização e o treinamento sobre segurança dos funcionários por meio de uma combinação de sistemas internos de gerenciamento de aprendizagem (LMSs) e programas de software como serviço (SaaS).
- 30% usam apenas LMS interno.
- 19% usam apenas SaaS externo.

O conteúdo do treinamento vem de várias fontes

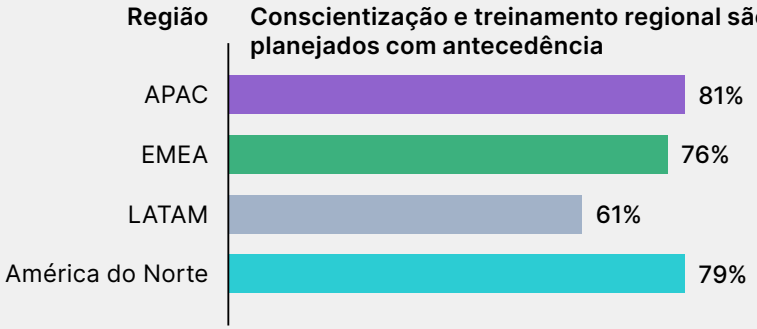
A responsabilidade pelo desenvolvimento de conscientização de segurança e conteúdo de treinamento difere entre as organizações:

- 22% desenvolvem seu próprio material internamente.
- 22% confiam em provedores terceirizados.
- 22% confiam em uma combinação dos dois.

Destaques regionais

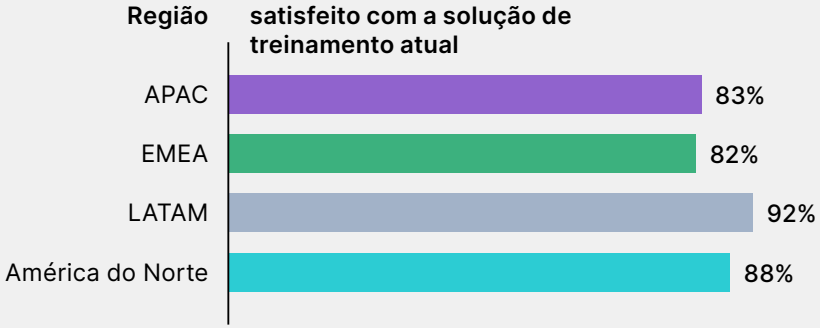
A América do Norte e a APAC são mais propensas a planejar com antecedência

Os entrevistados na América do Norte e Ásia-Pacífico (APAC) são mais propensos a planejar campanhas de conscientização e treinamento em segurança com antecedência, enquanto aqueles na LATAM são menos propensos.



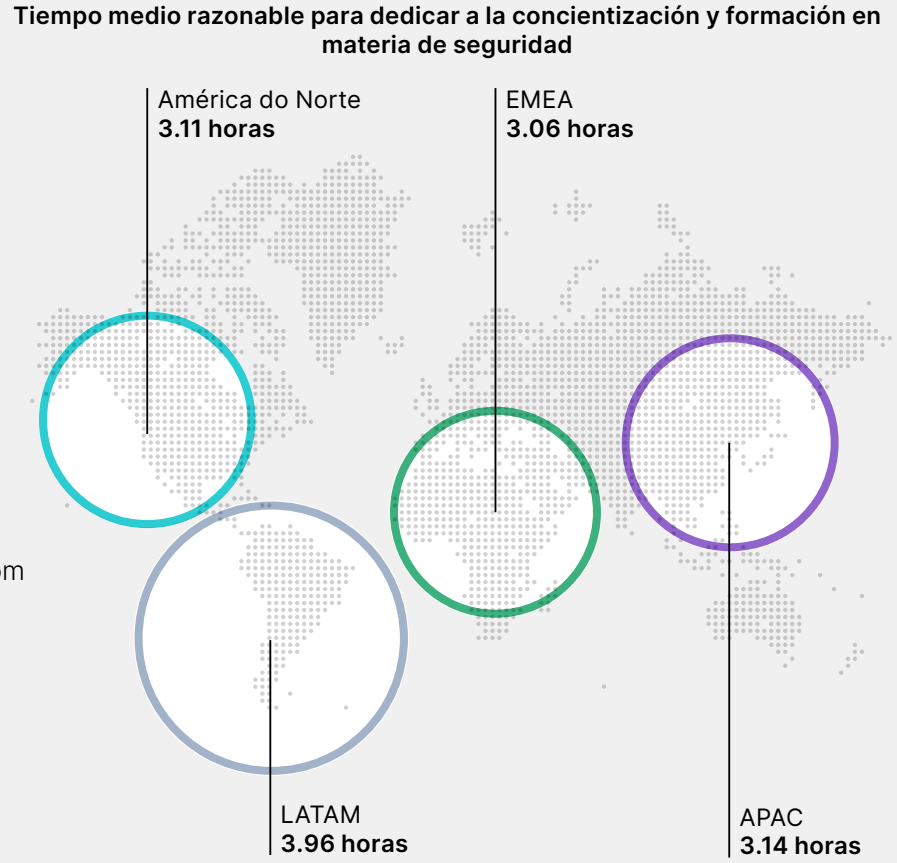
As organizações da LATAM são mais felizes com suas soluções de treinamento

Os entrevistados na LATAM estão mais satisfeitos com as suas soluções atuais de conscientização e treinamento em segurança em comparação com outras regiões.



Las organizaciones de LATAM dedicarían más tiempo a la formación

Los líderes de LATAM afirman que un promedio de casi cuatro horas de formación anual sería adecuado, frente a las tres horas de las demás regiones.



Conclusão

Os responsáveis pela tomada de decisões sabem que a conscientização sobre segurança contribui diretamente para a força da postura de segurança de sua organização. A maioria está investindo tempo e dinheiro em programas estruturados de treinamento e conscientização para os funcionários. Embora eles estejam vendo resultados, está claro que o trabalho está longe de ser concluído, especialmente à luz de ameaças emergentes como a IA.

As organizações precisam garantir que seus funcionários saibam como se proteger contra-ataques novos e cada vez mais poderosos. Como até mesmo uma única violação tem repercussões significativas para uma empresa, é fundamental construir uma defesa tripla de conscientização e treinamento, habilidades técnicas de segurança cibernética e soluções avançadas de segurança.

Com quase todos os entrevistados (94%) da pesquisa deste ano usando ou planejando usar ferramentas de IA para segurança cibernética, está claro que a IA será uma parte fundamental dessas soluções daqui em diante.

As organizações também estão procurando complementar a conscientização e o treinamento em segurança com boa governança: políticas corporativas para orientar o comportamento digital dos funcionários, incluindo o uso de ferramentas de IA e seguro cibernético para impedir perdas e ajudar a fortalecer as práticas internas. Embora, a partir de hoje, muitos ainda precisem acompanhar quando se trata de gerenciar e monitorar o uso de ferramentas de IA relacionadas ao trabalho.

Também está claro que o conteúdo do treinamento precisa ser envolvente para ser eficaz. O que isso significa pode variar de organização para organização, no entanto

em termos gerais, aponta para o material centrado no aluno e interativo com módulos concisos e fáceis de entender e elementos multimídia ou interativos para aprofundar o conhecimento e apoiar a retenção. Isso também significa manter o treinamento relevante por meio de atualizações regulares que refletem as necessidades em evolução.

Nossa pesquisa de conscientização e treinamento em segurança de 2024 mostra que um forte apoio organizacional contribui para atitudes mais positivas dos funcionários e maior confiança da liderança nos resultados do treinamento. Na experiência da Fortinet com os clientes, esse apoio deve incluir coordenação entre executivos, líderes de RH, representantes de TI e equipes de segurança cibernética para estabelecer um programa consistente para os funcionários. Isso pode ser um desafio quando os recursos são apertados e é um motivo pelo qual muitas empresas buscam fazer parceria com fornecedores de conscientização e treinamento.

No final das contas, à medida que os ataques continuam a evoluir, cada vez mais com os usuários finais dos funcionários como seus alvos, a conscientização e o treinamento em segurança só se tornarão mais vitais. As organizações podem ajudar a garantir que obtenham o melhor retorno possível sobre seus investimentos em treinamento, construindo e mantendo programas que estejam engajados e atualizados.

Além de ensinar aos indivíduos o que fazer quando encontrarem ameaças, a conscientização e o treinamento visam criar uma cultura de segurança cibernética para orientar a organização hoje e no futuro.