kaspersky cybersecurity true to business

Kaspersky Security Awareness

Construindo uma cultura de cibersegurança que mantém sua empresa segura



Por que uma cultura de segurança é importante



Erros humanos

62 a 80% dos vazamentos são causados por ações humanas, incluindo erros, uso indevido de privilégios e engenharia social[1][2]



US$ 4,99 milhões

é o custo médio de uma violação de dados por organização[3]



Os regulamentos exigem a conscientização em segurança como parte da conformidade: PCI DSS, ISO/IEC 27001, GDPR, NIS 2 e outras normas exigem ou recomendam fortemente a adoção de programas de conscientização em segurança para proteger dados confidenciais



Mais de 85%

dos profissionais que concluíram o treinamento sobre conscientização relatam melhoria na vigilância e no cuidado, o que representa uma mudança comportamental que ajuda a evitar incidentes [4]

90%

dos usuários recomendariam o Kaspersky Security Awareness a outros usuários[4]

3 milhões

de funcionários concluíram com sucesso nossos programas de treinamento

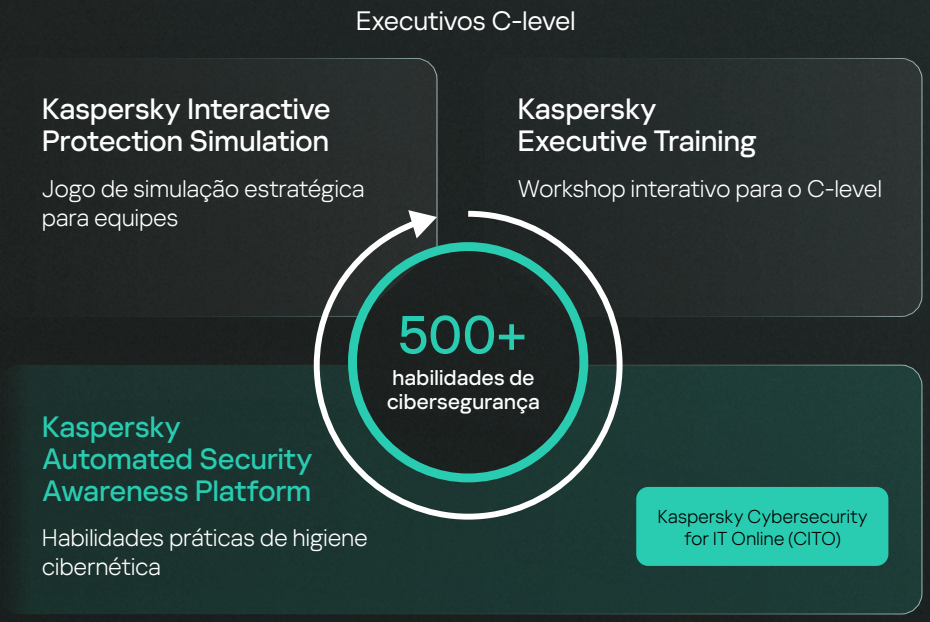
Mais de 160

países onde as organizações protegem os profissionais com nossas soluções de treinamento

Reduza os riscos cibernéticos decorrentes de falhas humanas com o Kaspersky Security Awareness

Construa uma cultura de cibersegurança em sua organização, com conscientização em segurança digital e habilidades práticas. Isso ajuda a reduzir o número de incidentes causados por erro humano. A melhor maneira de lidar com esse fator humano consiste em adotar um programa de treinamento estruturado que combine conteúdo relevante e atualizado, além de métodos e tecnologias de aprendizado mais recentes.

O Kaspersky Security Awareness permite que empresas de todos os portes ao redor do mundo aumentem a conscientização digital dos profissionais e promovam uma cultura onde a segurança seja responsabilidade de todos. Como as mudanças sustentáveis de comportamento levam tempo, nossa abordagem envolve a construção de um ciclo de aprendizagem contínuo com várias ferramentas e materiais de reforço: Kaspersky Interactive Protection Simulation, Executive Training, Automated Security Awareness Platform e Cybersecurity for IT Online.



Descubra por que o Kaspersky Security Awareness é a melhor escolha

Quase 30 anos de experiência em cibersegurança

A experiência dos profissionais globais da Kaspersky permite desenvolver treinamentos em cibersegurança com conteúdos bastante relevantes. Conforme o avanço das novas ameaças, nosso conteúdo evolui e ajuda a garantir que seus profissionais estejam sempre preparados.

Aprendizagem acessível e interativa

Nosso treinamento adota a aprendizagem interativa que ajuda os profissionais a relacionar o conteúdo das lições com suas tarefas rotineiras para melhorar a retenção e a aplicação no mundo real.

Mudança comportamental duradoura

Nossa metodologia reforça novas habilidades, oferece motivação contínua e ajuda a integrar a aprendizagem nas rotinas organizacionais.

Engajamento abrangente

Entregamos o conteúdo certo, no formato certo para cada público, desde executivos até a equipe operacional.

1 2026 Data Breach Investigations Report, Verizon
2 2026 Cyber risk Survey, Kaspersky
3 Cost of a Data Breach Report, IBM 2026
4 2024 Security Awareness & Training Data Quadrant, Info-Tech Research Group

Kaspersky Automated Security Awareness Platform

A Kaspersky Automated Security Awareness Platform (ASAP) é uma ferramenta on-line que entrega treinamento contínuo para munir os profissionais de habilidades e conhecimento para reconhecer e interromper os ataques do mundo real.

Desenvolvida por especialistas de alto nível, a Kaspersky ASAP empodera a equipe e fortalece o negócio:



Reduz o número de incidentes por falha humana

e os danos financeiros e à reputação resultantes



Reduz o risco de multas por não conformidade

ao cumprir requisitos regulatórios



Reduz o tempo e o esforço

necessários para gerenciar o treinamento sobre conscientização e alivia a carga de trabalho das equipes de TI

A Kaspersky ASAP é muito mais do que uma ferramenta antiphishing. O treinamento mapeia as técnicas MITRE ATT&CK para demonstrar quais vetores de ataques provocados por humanos podem ser evitados pelos profissionais. Exemplos:

MITRE ATT&CK

Técnica MITRE	Ameaça	Habilidades e resultados comportamentais
T1566: Phishing	E-mails maliciosos	Reconhecimento e relato de tentativas de phishing
T1585: Estabelecimento de contas	Contas/perfis falsos	Verificação de autenticidade antes do compartilhamento de informações
T1199: Relação confiável	Abuso da relação de confiança com parceiros	Questionamento de solicitações incomuns
T1091: Replicação por meio de mídia removível	Mídia removível	Compreensão do perigo de malware em dispositivos USB
T1078: Contas válidas	Roubo de credenciais	Não concessão de acesso por meio de engenharia social

95%

dos funcionários treinados agora conseguem identificar ataques de phishing

20 vezes

menos violações de dados quando os profissionais recebem treinamento contínuo[1]

Tópicos fundamentais cobertos pela ASAP, entre outros:

- Email
- Senhas e contas
- Sites e Internet
- Segurança de PCs
- Dados confidenciais
- Dados pessoais
- Segurança de dados física
- LGPD
- Inteligência artificial e redes neurais
- Ataques direcionados à alta gestão
- Dispositivos móveis
- Redes sociais e aplicativos de mensagens
- Ataques a cadeias de suprimentos
- Cibersegurança para a indústria
- Vishing
- Segurança de cartões bancários e PCI DSS
- Como responder aos incidentes

1 2025 Kaspersky Automated Security Awareness Platform Research

Treine, teste e fortaleça o nível de conscientização em segurança dos funcionários com especialização global e flexibilidade

A Kaspersky ASAP está disponível em três planos compatíveis com organizações de todos os portes e níveis de cultura de segurança.

		Essential	Proactive	Advanced
		Ideal para equipes pequenas Treinamento de conscientização em segurança em conformidade com requisitos regulatórios	Ideal para empresas em expansão Avaliação e treinamento de conscientização em segurança proativos	Ideal para empresas com requisitos específicos e uma cultura de segurança madura Treinamento de conscientização em segurança personalizado e de alto impacto
Phishing	Avalia a capacidade de resposta dos funcionários contra ciberataques por meio de simulações de phishing personalizáveis e realistas	●	●	●
Curso rápido	Aulas interativas que desenvolvem habilidades práticas no enfrentamento de ameaças de origem humana e mantêm a empresa em conformidade	●	●	●
Curso principal	Treinamento de conscientização em segurança totalmente automatizado e adaptado aos níveis de risco, com microaprendizado e reforço de habilidades		●	●
Personalização de conteúdo	Módulos, testes, páginas de phishing, domínios personalizáveis, entre outros			●
Implementação local	Opção de implementação na sua própria infraestrutura para obter controle total sobre dados confidenciais, integrações e conformidade regulatória			●

Solução fácil de gerenciar para organizações de qualquer tamanho

Entrada simples

Registro on-line rápido e acesso demonstrativo para até cinco usuários por dois meses. Inclui o guia "como começar" e suporte on-line

Gerenciamento proativo do risco humano

A integração simplificada com Kaspersky SIEM e XDR, além de APIs para integração com aplicativos de terceiros, oferece um panorama completo sobre o comportamento dos profissionais e atribui o treinamento baseado em eventos de segurança reais diretamente pelo console

Agrupamento de usuários automatizado de acordo com as regras personalizadas previamente definidas

Organização por função, departamento ou perfil de risco

Implementação flexível

Disponível como plataforma SaaS ou instalação on-premises

Automação completa

Módulos de treinamento, testes e simulações de phishing são atribuídos automaticamente em alinhamento com as configurações do grupo de treinamento

Suporte multilocatário e funções administrativas flexíveis

Ideal para organizações com subsidiárias e equipes distribuídas, viabilizando a supervisão centralizada e delegando o gerenciamento para os administradores locais

Elaboração de relatórios clara e adequada aos executivos

Os painéis oferecem dados essenciais com visualizações detalhadas sobre o progresso de cada profissional, atrasos ou desempenhos insatisfatórios, além de um relatório em PDF pronto para ser enviado para a gerência com apenas um clique

Inscrição descomplicada

Integração com Active Directory e SSO

Kaspersky Interactive Protection Simulation

O KIPS aumenta a conscientização dos riscos e dos desafios associados ao uso de todos os tipos de sistemas de TI e de processos corporativos. É um jogo de equipe interativo de duas horas voltado para a gestão sênior, especialistas em sistemas corporativos e profissionais de TI. Os cenários específicos do setor expõem os participantes às técnicas de ataque modernas observadas pelos especialistas da Kaspersky em campanhas ativas, inclusive ataques à cadeia de suprimentos, exploração de acesso de terceiros, engenharia social ou malware. O trabalho com restrições temporais e orçamentárias exige das equipes estratégia, antecipação aos impactos dos incidentes de segurança e resposta eficaz para proteger o desempenho e a receita corporativa.

Estabelece um entendimento
entre os tomadores de decisão

Ajuda a visualizar
os riscos de cibersegurança e associá-los diretamente à receita e às operações

Engaja as equipes
nas questões de cibersegurança e promove uma cultura que prioriza a segurança

KIPS Live

Uma atividade lúdica que pode ser executada como um evento isolado ou como uma sessão dentro de uma conferência em andamento, seminário ou evento corporativo.

- Até 100 participantes, com 4 a 5 pessoas em cada equipe
- Facilitador no local e assistente de treinamento

KIPS on-line

Uma versão on-line é perfeita para as atividades de organizações globais ou públicas. Ela também pode ser utilizada em conjunto com o KIPS Live para incluir as equipes remotas em um evento presencial.

- Até 300 equipes (1.000 participantes), onde quer que estejam

14 cenários específicos do setor com adições contínuas

- TI
- Aeroportos
- Corporações
- Bancos
- Petróleo e gás
- Transportes
- Centrais elétricas
- Tratamento de Água
- Administração pública local
- Indústria Petroquímica
- Holding de petróleo
- Pequenas e médias empresas
- Telecomunicações
- Atribuição técnica



Opções de personalização do KIPS

- Quadros, cartões ou números de mesa com marca conjunta ou marca do cliente
- Um cenário exclusivo, construído em parceria com a Kaspersky, que pode espelhar sua rede, incidentes passados ou ameaças específicas do setor

Kaspersky Cybersecurity for IT Online

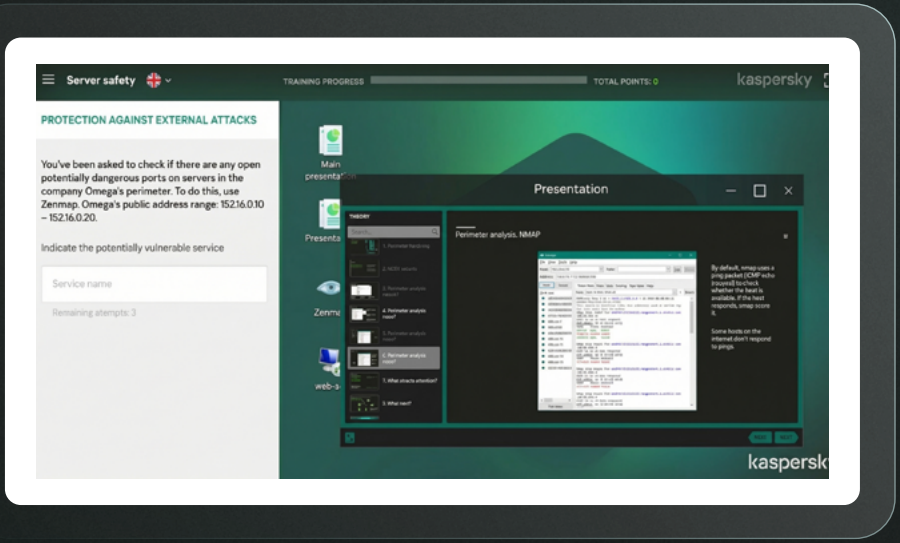
O Cybersecurity for IT Online (CITO) é um programa de treinamento interativo voltado para profissionais de suporte técnico especializado, administradores de sistemas e membros de equipes de segurança de TI não especializados. O programa desenvolve habilidades práticas para detectar ciberataques ocultos em incidentes cotidianos em PCs, coletar dados relevantes e atuar como a primeira linha de defesa cibernética.

Os participantes avançam por seis módulos que combinam teoria concisa e dicas práticas, além de 4 a 13 to alguns por módulo focados nas ferramentas de segurança de TI do mundo real e tarefas cotidianas.

- Software mal-intencionado
- Programas e exploits potencialmente indesejados
- Segurança de servidores
- Noções básicas sobre investigação
- Phishing e inteligência de código fonte aberto
- Segurança do Active Directory

Habilidades práticas de resposta a incidentes e reforço da segurança:

- Aprenda a detectar, analisar e responder a malware, programas potencialmente indesejados, exploits e ataques de phishing
- Aplique ferramentas e técnicas no mundo real para fortalecer a segurança da infraestrutura de TI e investigar eficazmente os incidentes
- Desenvolva habilidades em análises de log, coleta de evidências digitais e investigação de ameaças
- Aprenda a proteger servidores e o Active Directory por meio de fortificação, configuração de políticas e monitoramento



Kaspersky Executive Training

Promove uma cultura de segurança em toda a organização, começando pela liderança, mostrando como as decisões dos executivos influenciam diretamente a postura de risco, a conformidade regulatória e a resiliência organizacional de longo prazo.

O Kaspersky Executive Training é um workshop ao vivo, voltado para a liderança corporativa e a alta gestão, que explica o que o panorama atual de ameaças significa para sua empresa, quais são as ações necessárias que devem ser adotadas na ocorrência de um ataque virtual e muito mais. O ideal é combinar este treinamento com o KIPS.

Aspectos críticos de segurança virtual relativos aos negócios explicados em linguagem clara, acessível e não técnica:

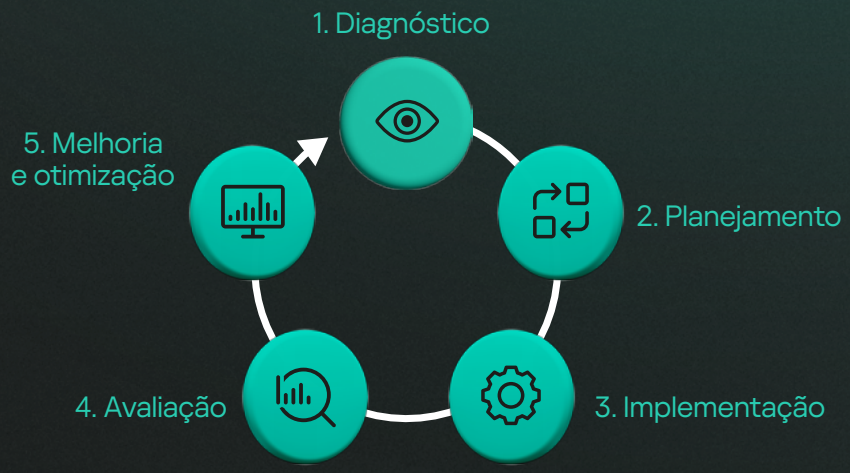
- Saiba como a segurança virtual atua como parte de todo um sistema
- Saiba como os riscos virtuais afetam as operações corporativas e como eles podem ser gerenciados
- Entenda o papel da gestão sênior na governança em segurança virtual

Construção de uma cultura de segurança digital

A verdadeira resiliência digital não se resume apenas a políticas e tecnologias; na verdade, trata-se de cultura. E a cultura é moldada de acordo com a atitude das pessoas, a atuação da liderança e o desenvolvimento de processos, bem como pela forma como a tecnologia viabiliza tudo isso.

Pessoas e comportamento + Liderança e cooperação + Integração operacional + Viabilização e prontidão em segurança

Uma cultura de segurança digital sustentável é mantida por meio do compromisso perene. É por isso que desenvolvemos uma abordagem sistemática em cinco etapas, em que é possível usar as soluções da Kaspersky Security Awareness.



Qual é o nível atual de maturidade da cultura de segurança virtual em sua organização?

0 Fragmentação

Risco: a ausência de práticas e estruturas básicas cria um alto nível de vulnerabilidade. Mesmo o menor incidente pode gerar graves consequências.

1 Conscientização e reatividade

Risco: apenas regras explícitas são seguidas. Em situações incomuns, os profissionais agem conforme o seu próprio julgamento.

2 Neutralização

Risco: o número de incidentes está diminuindo, mas o sistema permanece vulnerável diante de cenários mais complexos.

3 Integração

Risco: os processos parecem estar funcionando bem, mas, se a cultura cibernética não funcionar como um sistema autorregulável, o "risco de defasagem" persistirá.

4 Resiliência

Resultado: o número e a gravidade de incidentes continuam caindo. A organização consegue se adaptar rapidamente para continuar evoluindo no panorama de ameaças.

> Quando a segurança deixa de ser uma campanha e se torna uma cultura, os riscos diminuem e os resultados seguem firmes.
>
> CISO
>
> Consultorias de serviços ao cliente

Faça uma avaliação gratuita e descubra agora o nível da sua cultura de segurança



Kaspersky Security Awareness

Fique atento.
Mantenha-se protegido.

www.kaspersky.com.br

© 2026 AO Kaspersky Lab.
As marcas comerciais registradas e as marcas de serviço pertencem aos seus respectivos proprietários.

#kaspersky
#truetobusiness