Kaspersky Security Awareness

Construção de uma cultura de segurança virtual para manter seu negócio seguro

kaspersky cybersecurity true to business

Erros humanos

são a maior ameaça: em média, de 64 a 86% das violações envolvem ações humanas não maliciosas[1]

USD 4,4 milhões

é o custo médio de uma violação de dados por organização[2]

Regulamentos que exigem conscientização em segurança

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

Vale a pena construir uma cultura voltada para a conscientização em segurança

A pesquisa da Kaspersky demonstra que mais de 85% dos profissionais que concluíram o treinamento sobre conscientização relatam melhoria na vigilância e no cuidado, ou seja, uma mudança comportamental que ajuda a evitar incidentes.

92%

dos usuários recomendariam o Kaspersky Security Awareness para outros usuários

3 milhões

funcionários concluíram com sucesso nossos programas de treinamento

Mais de 160

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

Uma abordagem eficaz para reduzir o risco virtual humano

Construção de uma cultura de comportamento virtual seguro em sua organização, compatível com uma forte conscientização em segurança virtual e habilidades práticas. Isso ajuda a reduzir o número de incidentes causado 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.

Soluções Kaspersky Security Awareness

O Kaspersky Security Awareness empodera as empresas de todos os tamanhos ao redor do mundo para que o letramento virtual entre os profissionais aumente e para promover uma cultura onde a segurança seja uma responsabilidade de todo mundo. 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.

Por que os clientes escolhem o Kaspersky Security Awareness

Habilidades e confiança para identificar e responder a ameaças do mundo real

Contando com quase 30 anos da expertise da Kaspersky em segurança virtual e inteligência contra ameaças ao vivo, criamos o conteúdo de treinamento em segurança virtual altamente relevante. 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 com uma estrutura clara e lógica que ajuda os profissionais a relacionar o conteúdo das lições com suas tarefas rotineiras para melhorar o entendimento, 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. O resultado é uma mudança sustentável de comportamento onde as práticas seguras se tornam uma segunda natureza.

Engajamento abrangente

De executivos que necessitam de insights práticos de alto nível, à equipe da linha de frente que precisa de orientação prática, entregamos o material certo, no formato certo, para o público certo.

1 Kaspersky Human Factor 360 Report, Cybersecurity Ventures e Verizon Data Breach Reports
2 Cost of a Data Breach Report 2025, IBM

Kaspersky Automated Security Awareness Platform: a construção de um firewall humano

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 vetores de ataque do mundo real.

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

Reduz o número de incidentes provocados por humanos e, consequentemente, os prejuízos financeiros e reputacionais decorrentes

Minimiza os riscos de multas por não conformidade ao cumprir requisitos regulatórios

Reduz o tempo e os esforços 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 são os vetores de ataque provocados por humanos que os profissionais podem evitar. Exemplos:

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 x

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

Tópicos fundamentais abrangidos pela ASAP, entre outros:

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

Empodere seus profissionais para que se tornem uma camada extra de proteção juntamente com as ferramentas técnicas.

Comece a avaliação gratuita

1 2025 Kaspersky Automated Security Awareness Platform Research

Conteúdo e metodologia que fixam o aprendizado e transformam conhecimento em prática

Guiado por especialistas

Conteúdo produzido ao longo de quase 30 anos de expertise em segurança virtual e um modelo de competência que abrange habilidades práticas e essenciais em segurança virtual em diversos tópicos.

Várias opções de personalização

Acrescente seu logotipo, os certificados da marca, enriqueça as lições com slides internos, documentos ou políticas, acrescente os módulos personalizados SCORM/PDF e ajuste as estruturas de teste.

Conteúdo variado

Oferece suporte à retenção de conhecimento por meio de módulos interativos, além de exercícios, casos, testes e vídeos do mundo real e um cenário múltiplo com simulações de phishing.

Centrado no ser humano

Concebido de acordo com a maneira pela qual as pessoas absorvem, retêm e aplicam as informações

Como funciona

Todas as pessoas em sua organização precisam de conscientização sobre segurança virtual, mas a profundidade desse conhecimento varia de acordo com o perfil de função e de risco. É nesse ponto que um treinamento padronizado não funciona. Nossas plataformas ajudam sua equipe a desenvolver mais de 500 habilidades práticas, agrupar os profissionais com facilidade e atribuir o treinamento certo para cada participante com apenas alguns cliques por meio dos componentes abaixo.

Curso principal

Desenvolva conhecimentos aprofundados com microaulas organizadas por nível de complexidade.

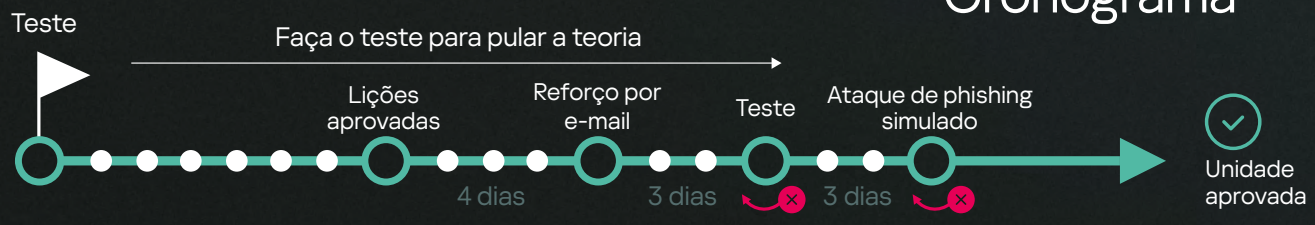
Curso expresso

Cumpra de forma rápida os requisitos de conformidade para treinamento de segurança virtual ou atualize os conhecimentos com treinamento em formato audiovisual, breve e altamente envolvente.

Simulador de phishing

Execute ataques simulados de phishing antes, durante e depois do treinamento para testar a capacidade de resistência dos profissionais contra ataques virtuais.

Cronograma



Blocos com diferentes tipos de atividades para maximizar a memorização

Solução fácil de gerenciar para organizações de qualquer tamanho

Entrada simples

Faça o registro on-line e tenha acesso à demonstração 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 real diretamente pelo console

Agrupamento de usuário 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 a multilocação e funções administrativas flexíveis

Ideal para organizações com subsidiárias e equipes distribuídas para viabilizar a supervisão centralizada e delegar, simultaneamente, o gerenciamento para os administradores locais.

Relatórios transparentes

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

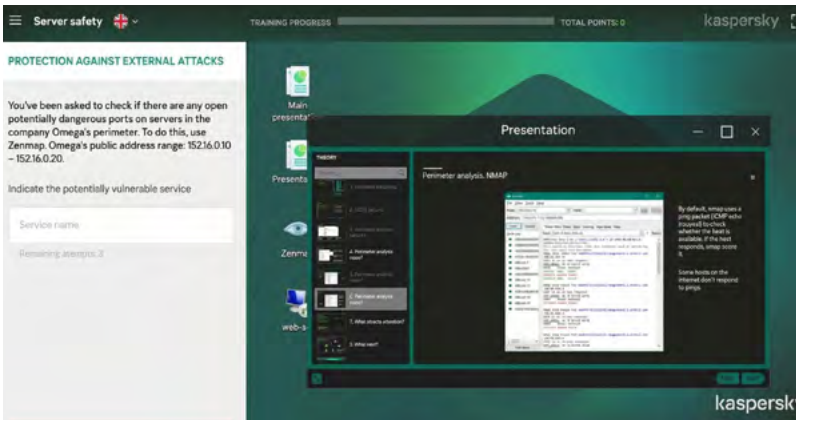
Integração com Active Directory e SSO

Cibersegurança para TI on-line

O Cybersecurity for IT Online (CITO) é um programa de treinamento interativo que ensina a especialistas de suporte técnico especializado, administradores de sistema e membros não especializados da equipe de segurança de TI habilidades práticas para detectar ataques virtuais ocultos no âmbito de incidentes cotidianos para PC, coletar dados pertinentes e atuar como a primeira linha de defesa de segurança virtual.

Habilidades práticas para resposta a incidentes de primeiro nível:

- Aprenda a detectar, analisar e responder a malware, programas potencialmente indesejados, exploits e ataques de phishing
- Aplique ferramentas e técnicas do 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



Os participantes avançam em 6 módulos que combinam teoria concisa e dicas práticas, além de 4 a 13 exercícios 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

Kaspersky Executive Training

Promova uma cultura de segurança abrangente e demonstre como as decisões executivas exercem influência direta sobre a postura de riscos, 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. Além dos princípios fundamentais de segurança virtual, os participantes desenvolvem insights críticos em relação à viabilidade financeira dos investimentos de segurança para empoderar a liderança de alto escalão a aliar proteção com desempenho corporativo. 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

Kaspersky Interactive Protection Simulation (KIPS): segurança virtual do ponto de vista corporativo

O KIPS aumenta a conscientização dos riscos e dos desafios associados por meio do 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 o entendimento entre os tomadores de decisão
- Ajuda a visualizar os riscos de segurança virtual para mapeá-los diretamente com a receita e as operações
- Engaja a equipe com os problemas de segurança virtual e promove uma cultura que prioriza a segurança

14 cenários específicos do setor com a adição constante de outros cenários

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

KIPS Live

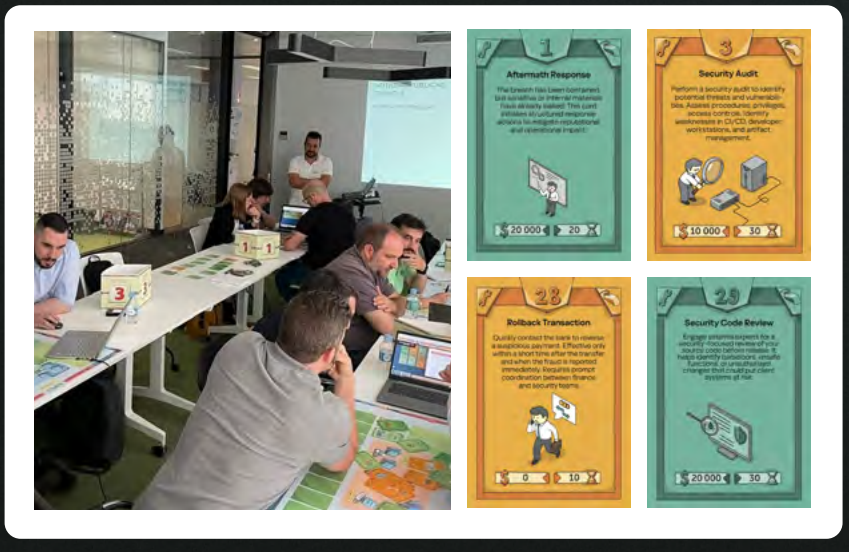
Uma atividade lúdica que pode ser executada como um evento isolado ou como uma sessão dentro de uma conferência em andamento, seminário ou evento corporativo.

- 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 combinada com o KIPS Live para incluir as equipes remotas em um evento presencial.

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



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

Construção de uma cultura de segurança virtual

A verdadeira resiliência virtual 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 maneira pela qual a liderança atua, como os processos são concebidos e como a tecnologia viabiliza tudo isso:

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

Uma cultura de segurança virtual 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 Fragmentado
Risco: a ausência de práticas e estruturas básicas cria um alto nível de vulnerabilidade. Mesmo o menor incidente pode gerar sérias consequências.

1 Consciente e proativo
Risco: apenas as regras explicitamente definidas são seguidas. Em situações fora do padrão, os profissionais atuam de acordo com o próprio julgamento.

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

3 Integrado
Risco: o processo parece estar dentro dos conformes, mas se a cultura virtual não estiver funcionando como um sistema autorregulamentado, o "risco de defasagem" persistirá.

4 Resiliente
Resultado: o número e a gravidade dos incidentes continuam caindo. A organização pode 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

Comece a construir uma cultura virtual resiliente pelo alinhamento de pessoas, processos e tecnologias com a Kaspersky ASAP.

Experimente agora

Kaspersky Security Awareness

Fique atento.
Mantenha-se protegido.

www.kaspersky.com.br

#kaspersky
#segurançavirtualverdadeiraparaosnegocios