Programas de treinamento em computador para todos os níveis organizacionais

# Kaspersky Security Awareness

kaspersky PREPARADOS PARA O FUTURO

Saiba mais em kaspersky.com.br/awareness

# Kaspersky Security Awareness

## A forma econômica de criar cibersegurança na sua organização

**Mais de 80% de todos os incidentes cibernéticos são causados por erro humano. Uma cultura de comportamento de cibersegurança com habilidades básicas e conscientização por toda a organização é importante para reduzir a superfície de ataque e o número de incidentes com os quais você precisa lidar. Frequentemente, as organizações enfrentam dificuldades para encontrar as ferramentas e os métodos corretos para implementar um treinamento de funcionários eficaz capaz de melhorar o comportamento. A chave para conseguir isso é implantar um treinamento que empregue as últimas técnicas e tecnologias em educação para adultos e forneça o conteúdo mais relevante e atualizado.**

### O fator humano – o elemento mais vulnerável da cibersegurança

Soluções de cibersegurança estão rapidamente se desenvolvendo e adaptando a ameaças complexas, dificultando a vida dos criminosos que estão se voltando para o elemento mais vulnerável da segurança – o fator humano.

**52% dos executivos de nível C** afirmam que os funcionários são a maior ameaça à segurança operacional*

**43% das pequenas empresas** sofreram um incidente de segurança devido à violação de políticas de segurança de TI por funcionários**

**60% dos funcionários** possuem dados confidenciais em seus dispositivos corporativos (dados financeiros, base de dados de email etc.)***

**30% dos funcionários** admitem que compartilham seus detalhes de login e senha do PC com os colegas***

**23% das organizações** não têm regras ou políticas de cibersegurança implementadas para armazenamento de dados corporativos***

## Kaspersky Security Awareness – uma nova abordagem para dominar habilidades de segurança de TI

O Kaspersky Security Awareness oferece uma gama de soluções de treinamento extremamente eficientes e altamente envolventes que melhoram a conscientização sobre cibersegurança da sua equipe de forma que todos desempenhem seu papel na segurança geral da organização. Como mudanças de comportamento sustentáveis levam tempo, a nossa abordagem envolve criar um ciclo de aprendizado contínuo com vários componentes.

**Ciclo de aprendizado contínuo**

| Compromisso/ motivação | Início | Aprendizado | Reforço |
|---|---|---|---|
| – Por que preciso disso?<br>– Cognição | – Eu tenho consciência?<br>– O que sei e onde estão as lacunas? | – Microaprendizado<br>– Aprendizado contínuo<br>– Adaptabilidade | – Entendi corretamente?<br>– Lembro disso?<br>– Tenho ações condizentes? |

## Principais fatores diferenciadores do programa

### Conhecimentos de cibersegurança substanciais

Mais de 20 anos de experiência em cibersegurança transformados em habilidades de ciberproteção que residem no coração de nossos produtos

### Treinamento que muda o comportamentos dos funcionários em todos os níveis da sua organização

Nosso treinamento com jogos fornece engajamento e motivação por meio de educação e entretenimento, enquanto as plataformas de aprendizado ajudam a internalizar o conjunto de habilidades de cibersegurança para garantir que as habilidades aprendidas não sejam perdidas pelo caminho.

* Relatório "Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure", 2020

** Relatório "IT security economics 2021", Kaspersky

*** "Sorting out a Digital Clutter". Kaspersky Lab, 2019.

**Funcionários cometem erros. Organizações perdem dinheiro...**

**US$ 1.315.000**
**por organização empresarial**
O impacto financeiro médio de uma violação de dados causada por uso inadequado dos recursos de TI pelos funcionários*

**50%**
**das empresas**
relataram sofrer ameaças diretamente causadas pelo comportamento inadequado da equipe, tornando essa a ameaça mais comum à segurança de TI*

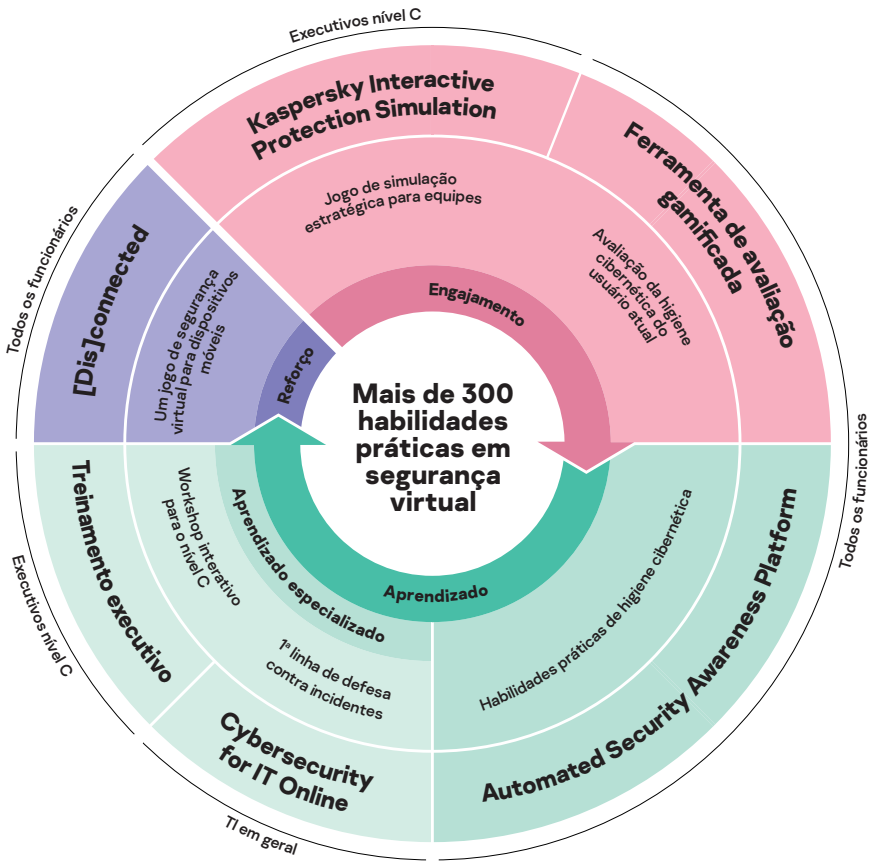
**86%**
**das empresas**
afirmou que pelo menos uma pessoa clicou em um link de phishing**

**US$ 5,01 milhões**
**de custo médio por violação**
de ataques BEC (BEC – Comprometimento de email corporativo – um tipo de phishing em que os criminosos sequestram ou falsificam contas de email corporativas legítimas)

# Alimentando motivação para uma consciência sobre segurança eficaz

Mudar o comportamento dos funcionários é o nosso maior desafio em cibersegurança. Geralmente, as pessoas não se sentem motivadas a adquirir habilidades e mudar seus hábitos. Por isso, muitos esforços educacionais se transformam em um pouco mais do que uma formalidade vazia. Um treinamento eficaz consiste em diferentes componentes, leva em consideração as especificidades da natureza humana e a capacidade de assimilar as habilidades adquiridas. Como especialista em cibersegurança, a Kaspersky conhece comportamentos cibernéticos seguros dos usuários. Com nossos insights e experiência, adicionamos técnicas e métodos de aprendizado para imunizar os funcionários dos nossos clientes contra ataques, ao mesmo tempo que fornecemos a eles liberdade para agir sem restrições.

## Diferentes formatos de treinamento para diferentes níveis organizacionais




* Relatório "IT security economics 2021", Kaspersky

** Cybersecurity threats trends 2021, CISCO

*** Cost of a Data Breach, 2021. IBM

# Soluções Kaspersky Security Awareness

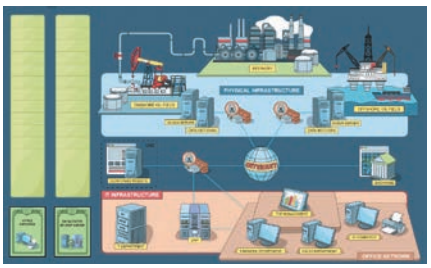
**Motivação**

Nem sempre os funcionários estão interessados em mais treinamentos obrigatórios e, quando se trata de cibersegurança, vários deles consideram isso muito complicado ou enfadonho ou acreditam que não diz respeito a eles. Sem a motivação de aprender, é improvável que o resultado do aprendizado seja muito positivo. Outro desafio para os responsáveis pelo ensino é envolver os executivos de negócios nos treinamentos, embora os erros desses executivos possam custar à empresa tanto quanto de todos os outros. Aqui é onde os jogos entram. Como eles são muito envolventes, essa é a maneira mais eficaz de encorajar a sua equipe a superar a resistência inicial a treinamentos.

**70%**
**do que é aprendido**
é esquecido em um dia com as formas tradicionais de treinamento

**42% dos entrevistados que trabalham em empresas com mais de 1.000 funcionários**
disseram que a maioria dos programas de treinamento dos quais participaram foram inúteis e desinteressantes**

**O treinamento KIPS** destina-se a gerentes seniores, especialistas em sistemas de negócios e profissionais de TI e visa aumentar a conscientização sobre os riscos e desafios associados ao uso de todos os tipos de sistemas e processos de TI.



## Jogo estratégico Kaspersky Interactive Protection Simulation (KIPS): cibersegurança do ponto de vista corporativo

O KIPS é um jogo de equipe interativo de 2 horas que estabelece uma compreensão entre responsáveis por decisões (encarregados de negócios, TI e cibersegurança seniores) e muda suas percepções sobre cibersegurança. Ele representa uma simulação de software do verdadeiro impacto que malware e outros ataques causam no desempenho e na receita da empresa. Os jogadores são levados a pensar estrategicamente, antecipar as consequências de um ataque e reagir de acordo com as restrições de tempo e dinheiro. Cada decisão afeta todos os processos de negócios – o objetivo principal é manter as coisas funcionando sem problemas. A equipe que terminar o jogo com a maior receita e encontrar, analisar e responder de forma apropriada a todas as armadilhas no sistema de cibersegurança, vencerá.

## 13 cenários relacionados ao setor (com outros constantemente adicionados)


Cada cenário demonstra a verdadeira função da cibersegurança em termos de continuidade dos negócios e lucratividade, destacando desafios e ameaças emergentes, e os erros típicos que as organizações cometem ao implantar suas seguranças cibernéticas. Eles também promovem a cooperação entre as equipes comerciais e de segurança, o que ajuda a manter as operações estáveis e a sustentabilidade contra as ameaças cibernéticas.

## Personalização dos cenários

A partir do terceiro trimestre de 2022, para cenários industriais selecionados, as empresas poderão criar seus próprios cenários de jogo com diferentes ataques. Ao usar diferentes combinações de ataques, as empresas com licença corporativa KIPS podem jogar o mesmo cenário industrial várias vezes.

## Realidade virtual KIPS

**O KIPS Power Station VR** é uma nova experiência imersiva em um ambiente realista o mais próximo possível das operações reais de uma usina de geração de energia. A tecnologia permite que os gerentes "trabalhem" como especialistas em segurança da informação, demonstrando visualmente o papel da segurança cibernética e seu impacto nos negócios para que possam ver as consequências de suas decisões de TI em gráficos 3D altamente realistas, em vez de apenas ter uma ideia abstrata deles.

**Início**

Geralmente, as pessoas não têm consciência do seu nível de incompetência, o que as torna particularmente vulneráveis. Elas precisam ser testadas, e receber feedback claro e detalhado sobre o seu nível de competência em cibersegurança para que treinamentos posteriores sejam eficazes. Isso também garante que tempo não seja desperdiçado com material já familiar.

**Aprendizado**

A nossa plataforma de aprendizado online é o coração do programa de conscientização. Ela contém **mais de 300 habilidades de cibersegurança** que abrangem todos os principais tópicos de segurança de TI. Cada lição inclui casos e exemplos reais para que os funcionários possam sentir uma conexão com o que eles precisam lidar em seus trabalhos diários. E eles podem usar essas habilidades imediatamente após a primeira lição.

**Kaspersky ASAP: uma ferramenta online fácil de gerenciar que desenvolve as habilidades de cibersegurança dos funcionários estágio por estágio**

Tópicos abordados no KASAP:
- Senhas e contas
- E-mail
- Sites da Web e Internet
- Mídias sociais e Mensagens
- Segurança do PC
- Dispositivos móveis
- PROTEÇÃO DE DADOS CONFIDENCIAIS
- GDPR
- Industrial Cybersecurity

**Curso expresso do ASAP**

Uma versão curta do treinamento em formato de áudio e vídeo.

- Teoria interativa
- Vídeos
- Testes

O Kaspersky ASAP é uma solução multilíngue.

# **Gamified Assessment Tool**: uma maneira rápida e empolgante de avaliar as habilidades de cibersegurança dos funcionários

O Kaspersky Gamified Assessment Tool (GAT) permite que você avalie rapidamente os níveis de conhecimento sobre cibersegurança dos seus funcionários. A abordagem envolvente e interativa elimina a monotonia frequentemente encontrada em ferramentas de avaliação clássicas. Apenas 15 minutos são necessários para que os funcionários percorram as 12 situações do dia a dia relacionadas a cibersegurança, avaliando se as ações do personagem são arriscadas ou não e expressando o nível de confiança em suas respostas.

Após a conclusão, os usuários receberão um certificado com uma pontuação que refletirá o seu nível de conscientização sobre cibersegurança. Eles também obterão feedback sobre cada zona, com explicações e dicas úteis.

A abordagem em jogos do GAT motiva os funcionários e, ao mesmo tempo, demonstra que, ao resolver determinadas situações de cibersegurança, pode haver lacunas em seus conhecimentos. Isso também é útil para que os departamentos de TI/RH adquiram melhor compreensão dos níveis de conscientização sobre cibersegurança em suas organizações, e pode servir como uma etapa introdutória para uma campanha de educação mais ampla.


# **Kaspersky Automated Security Awareness Platform**: eficiência e facilidade de gestão de treinamento para organizações de qualquer tamanho

O Kaspersky ASAP é uma ferramenta online eficaz e fácil de usar que molda as habilidades de cibersegurança dos funcionários e os motiva a se comportarem da forma correta.

Embora o treinamento atenda às necessidades de conscientização de segurança para todas as empresas, o gerenciamento automatizado atrairá especialmente aqueles sem recursos dedicados de gerenciamento de treinamento.

## Principais benefícios:

- **Simplicidade através de automação total:** o programa é muito fácil de iniciar, configurar e monitorar, e seu gerenciamento contínuo é totalmente automatizado – não há necessidade de envolvimento administrativo. A própria plataforma cria um cronograma de ensino para cada grupo de funcionários, oferecendo, automaticamente, aprendizado em intervalos e vários formatos de treinamento, incluindo módulos de aprendizado, reforço sobre emails, testes e ataques simulados de phishing.
- **Eficiência:** o conteúdo do programa é estruturado para oferecer aprendizado incremental em intervalos com reforço constante. A metodologia baseia-se na especificidade da memória humana para garantir a retenção de conhecimentos e a subsequente aplicação de habilidades.
- **Aprendizado flexível:** escolha a opção de treinamento de funcionários certa para você: atribuir aos funcionários um curso expresso básico que o ajudará a atender rapidamente aos requisitos regulamentares para treinamento de segurança cibernética ou atualizar seus conhecimentos, ou escolher um curso principal dividido em níveis de complexidade para fornecer informações mais detalhadas e desenvolver habilidades de cibersegurança mais sólidas.
- **Licenciamento flexível** (para provedores de serviços gerenciados): o modelo de licenciamento por usuário pode começar com apenas 5 licenças.

**O ASAP é ideal para MSPs e xSPs** – os serviços de treinamento para várias empresas podem ser gerenciados por meio de uma única conta, e assinaturas de licença mensais estão disponíveis.

Experimente uma versão totalmente funcional do Kaspersky ASAP em asap.kaspersky.com/br – veja você mesmo como é fácil configurar e gerenciar seu próprio programa de conscientização em segurança corporativa.

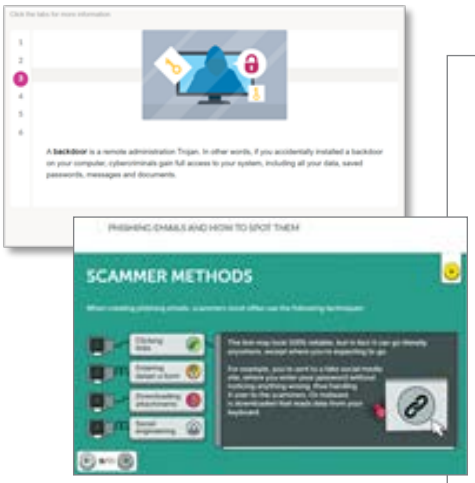
## Campanhas de phishing simuladas

Ataques de phishing simulados podem ser usados antes, durante e após o treinamento para testar a capacidade dos funcionários de resistir a ataques cibernéticos e ajudá-los – além de ajudar o gerenciamento da empresa a perceber os benefícios do treinamento.

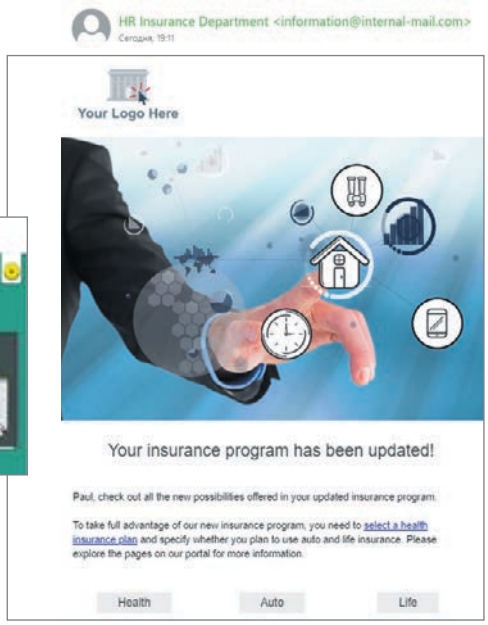
### Lições interativas

**Curso principal**

**Curso expresso**




### Ataques de phishing simulados




## Acompanhe os resultados

Você pode acompanhar o progresso dos funcionários do painel e avaliar o progresso de toda a empresa, e todos os grupos, em um relance. Você também pode pesquisar mais detalhes em um nível individual.

**Reforço**

O reforço é uma parte essencial do programa de aprendizado. Ele é necessário para consolidar o conhecimento e as habilidades obtidas durante o aprendizado.

A melhor maneira de transformar as habilidades aprendidas em hábitos é colocá-las em prática. Além disso, às vezes as pessoas cometem erros e aprendem com experiências pessoais. Mas quando se trata de cibersegurança, aprender com os próprios erros pode ser muito caro.

Treinando com jogos, você pode vivenciar uma situação e experimentar suas consequências sem qualquer prejuízo a você ou à sua empresa.

## [Dis]Connected: uma missão de segurança cibernética móvel

[Dis]Connected é um jogo de cibersegurança para dispositivos móveis altamente imersivo e baseado em uma história visual rica onde os usuários são desafiados a manter o equilíbrio entre vida pessoal e trabalho e serem bem-sucedidos pessoal e profissionalmente.

Os elementos de cibersegurança estão incorporados ao enredo do jogo, o qual revela como as nossas decisões de segurança podem ajudar a atingir – ou arruinar – objetivos. Há 24 casos a serem solucionados, incluindo tópicos sobre senhas e contas, emails, navegação na Web, redes sociais e aplicativos de mensagens instantâneas, segurança de computadores e dispositivos móveis. Aplicativos emulados integrados – aplicativos de mensagens instantâneas, aplicativos de bancos etc. – garantem uma experiência ainda mais completa e imersiva.

No final do jogo, os jogadores receberão um resumo sobre o quão bem-sucedidos eles foram no projeto e descobrirão se suas habilidades de segurança são suficientes para o momento e o futuro.




O jogo funciona em telefones celulares. Uma **demonstração gratuita** está disponível no Google Play e na AppStore: https://kas.pr/mobilestore

**Aprendizado avançado**

Especialistas gerais de TI: membros de equipes de helpdesk e outros funcionários tecnicamente experientes são frequentemente deixados de fora do treinamento porque os programas de conscientização padrão não são suficientes para eles, mas as empresas também não precisam transformá-los em especialistas em segurança cibernética: é muito caro, demorado e desnecessário.

Temos o prazer de anunciar um treinamento que preenche esta lacuna – não tão detalhado quanto um treinamento especializado, mas mais avançado do que o treinamento para os demais funcionários.

**Módulos de treinamento CITO:**

- Software mal-intencionado
- Programas e arquivos potencialmente indesejados
- Noções básicas sobre investigação
- Resposta a incidentes de phishing
- Segurança de servidores
- Segurança do Active Directory

**Método de entrega do CITO:**
Formato de nuvem ou SCORM

**Experimente um dos módulos CITO grátis:**
cito-training.com

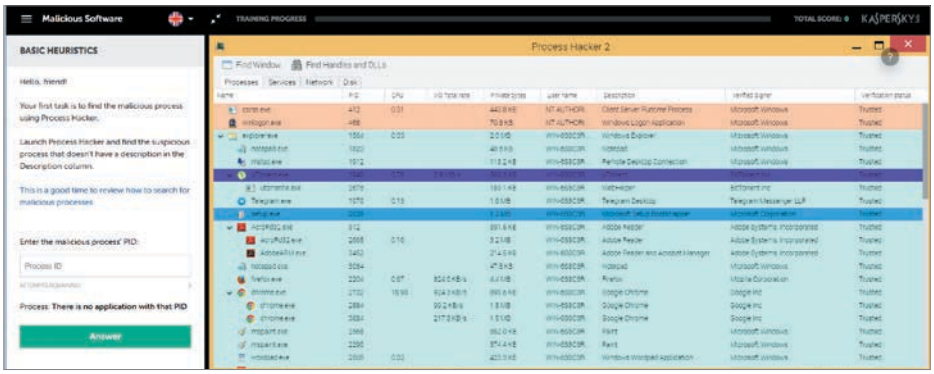
# Cybersecurity for IT Online: a primeira linha de defesa contra incidentes

O Cybersecurity for IT Online é um treinamento interativo para qualquer pessoa envolvida em TI. Ele desenvolve fortes habilidades em cibersegurança e resposta a incidentes de primeiro nível.

O programa equipa os profissionais de TI com habilidades práticas para reconhecer um possível cenário de ataque em um incidente de PC aparentemente benigno. Ele também gera um interesse pela busca de sintomas maliciosos – consolidando a função de todos os membros da equipe de TI como a primeira linha de defesa de segurança.

O CITO também ensinará noções básicas de investigação e como usar ferramentas e software de segurança de TI para equipar seus profissionais de TI com habilidades teóricas, práticas e baseadas em exercícios, permitindo a eles coletar dados de incidentes que usarão na segurança de TI.

Esse treinamento é recomendado para todos os especialistas de TI em sua organização, mas principalmente de centrais de serviços e administradores de sistemas. A maioria dos membros da equipe de segurança de TI não especializados também irão se beneficiar desse curso.




Os gerentes de nível superior estão entre os alvos mais desejáveis para os cibercriminosos, mas muitas vezes são um verdadeiro desafio para os educadores. No entanto, sem seu envolvimento e apoio a várias iniciativas e advocacia de segurança cibernética, é impossível criar uma cultura de segurança cibernética na organização.

A cibersegurança é um aspecto importante da geração de receita, juntamente com o gerenciamento de projetos, instrumentos financeiros e eficiência operacional de negócios. Este é o foco do nosso curso para executivos.

# Treinamento executivo: aumentando a resiliência dos negócios para a transformação digital

Os líderes de negócios e os principais gerentes aprendem os fundamentos da segurança cibernética por meio de um curso ministrado por tutores que dá a eles uma melhor compreensão das ameaças cibernéticas e como se proteger contra elas.

Pesquisas mostram que existe uma ligação direta entre a velocidade e a eficiência da resposta a incidentes e o grau de danos que um incidente pode causar. O curso dedica atenção especial aos aspectos financeiros da segurança cibernética e à viabilidade de investir nela, proporcionando aos executivos de nível C uma melhor compreensão da conexão entre segurança cibernética e eficiência dos negócios.

O Kaspersky Interactive Protection Simulation (KIPS) pode ser usado além deste treinamento para consolidar ainda mais o material por meio de exercícios práticos.

## Objetivos do curso

- Compartilhar as informações mais recentes sobre ameaças cibernéticas modernas e seus riscos para os negócios
- Atualizar os participantes com o cenário moderno das ameaças cibernéticas
- Proporcionar uma oportunidade para praticar as regras básicas da cultura de cibersegurança corporativa e pessoal
- Garantir que o impacto para os negócios das principais questões regulatórias no campo da segurança da informação seja entendido
- Esclarecer os conceitos básicos de segurança cibernética e os métodos de proteção contra ataques direcionados
- Fornecer recomendações práticas para a política corporativa
- Aconselhar sobre comunicações para responder e investigar incidentes

# **Kaspersky Security Awareness:** maneiras flexíveis de treinar

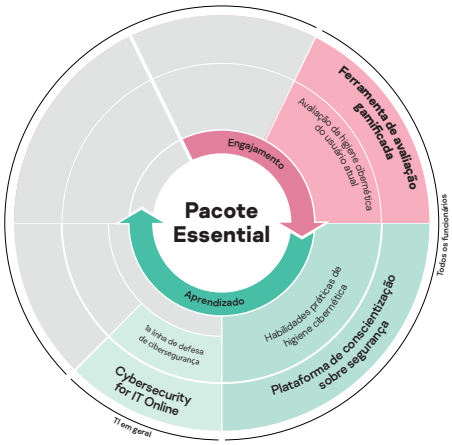
As soluções Kaspersky cobrem todos os níveis da sua empresa e podem ser usadas isolada ou coletivamente. Também facilitamos para você começar oferecendo pacotes adaptados às suas necessidades.

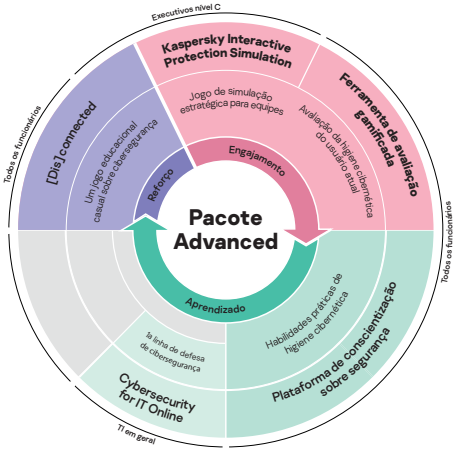
A opção fácil de usar para aumentar a conscientização sobre cibersegurança dos funcionários – simples de configurar, fácil de gerenciar.

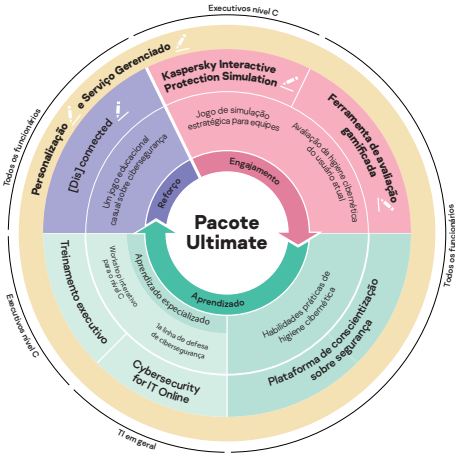
Fornece um nível básico de treinamento de segurança para ajudar você a operar com sucesso e atender aos requisitos regulamentares ou de terceiros para treinamento geral de segurança cibernética

Ajuda as organizações maiores a manter a continuidade dos negócios usando uma simples solução de treinamento completo pronto para uso. É compatível com todos os níveis organizacionais e muda de comportamento cobrindo todas as fases do ciclo de aprendizado.

Garante o máximo de conscientização em cibersegurança, fornecendo serviços de personalização e gerenciamento para que os executivos sejam bem versados em cenários de ameaças. Os funcionários adquirem habilidades de segurança virtual automáticas e a equipe de TI generalista oferece suporte como a primeira linha de defesa.




O treinamento Kaspersky Security Awareness usa os métodos de treinamento mais recentes e técnicas avançadas para garantir o sucesso. Novos pacotes de soluções flexíveis podem ser adaptados às suas necessidades – assim, há sempre uma solução para todos. Saiba mais em [kaspersky.com.br/awareness](kaspersky.com.br/awareness)

Kaspersky Security Awareness: kaspersky.com.br/awareness
Notícias sobre segurança de TI: business.kaspersky.com

**kaspersky.com.br**



kaspersky PREPARADOS PARA O FUTURO