Competências em Cybersegurança para funcionários de todos os níveis

Kaspersky Security Awareness

kaspersky bring on the future

Saiba mais em
kaspersky.com.br/awareness

Kaspersky Security Awareness

Crie uma cultura de cibersegurança em toda sua organização

Mais de 80% de todos os ciberincidentes são causados por erro humano. Ao construir uma cultura comportamental que preza pela cibersegurança, juntamente com competências básicas e conscientização por toda a organização, é possível reduzir a superfície de ataque e o número de incidentes com os quais você precisa lidar. A melhor maneira de alcançar as mudanças comportamentais que resolveriam o problema do "fator humano" na segurança de TI é por meio de treinamentos que utilizam as técnicas e tecnologias mais recentes na educação de adultos, e fornecem o conteúdo mais relevante e atualizado.

Fator humano – o elemento mais vulnerável da cibersegurança

As soluções de cibersegurança estão rapidamente se desenvolvendo e se adaptando às ameaças complexas, dificultando a vida dos criminosos e tornando-os mais focados no elemento mais vulnerável da segurança de TI – o fator humano.

55% das empresas relatam violações da política de segurança de TI por seus próprios funcionários*

43% das pequenas empresas relatam que as violações da política de segurança de TI pelos funcionários causam incidentes de segurança **

Vazamento de dados é o problema de segurança mais comum**, causado com mais frequência** por funcionários (22%) e invasores (23%).*

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

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

Kaspersky Security Awareness – uma nova abordagem no domínio das competências em Cibersegurança

O Kaspersky Security Awareness é uma solução comprovada e eficiente com um longo histórico de sucesso internacional. Utilizada por empresas de todos os tamanhos no treinamento de mais de um milhão de funcionários em mais de 75 países, esta solução reúne mais de 25 anos de conhecimento em cibersegurança da Kaspersky com uma ampla experiência na educação de adultos.

As soluções de treinamento extremamente eficientes e altamente envolventes melhoram a conscientização em cibersegurança da sua equipe, de forma em que todos desempenhem seu papel na segurança geral da organização. Como as mudanças de comportamento sustentáveis são demoradas, a nossa abordagem envolve criar um ciclo de aprendizado contínuo com vários componentes.

Ciclo de aprendizado contínuo

1	2	3	4
Compromisso/ motivação	**Início**	**Aprendizado**	**Consolidação**
– Por que preciso disso? – Cognição	– Eu sou cibercon-sciente? – O que eu sei, e o que eu não sei?	– Microaprendizado – Aprendizado contínuo – Adaptabilidade	– Entendi certo? – Eu lembro disso? – Tenho ações condi-zentes?

Principais fatores que diferenciam o programa

Experiência sobre cibersegurança significativa

Mais de 25 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 trinamento gamificado fornece engajamento e motivação por meio de "edutretenimento", 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.

* "IT Security Economics 2022" Kaspersky

** Relatório "IT security economics 2021", Kaspersky

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

Alimentando motivação para uma consciência sobre segurança eficaz

Mudar o comportamento dos funcionários é o nosso maior desafio na cibersegurança. Geralmente, as pessoas não se sentem motivadas a adquirir habilidades e mudar seus hábitos. Por isso, muitos esforços educacionais acabam sendo em vão. 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 reconhece a importância de comportamentos ciberseguros no ambiente corporativo. 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.

Funcionários cometem erros. Organizações perdem dinheiro...

52,887 mil dólares
por organização empresarial
O custo médio de um ciberataque causado pelo uso inadequado de recursos de TI pelos funcionários*

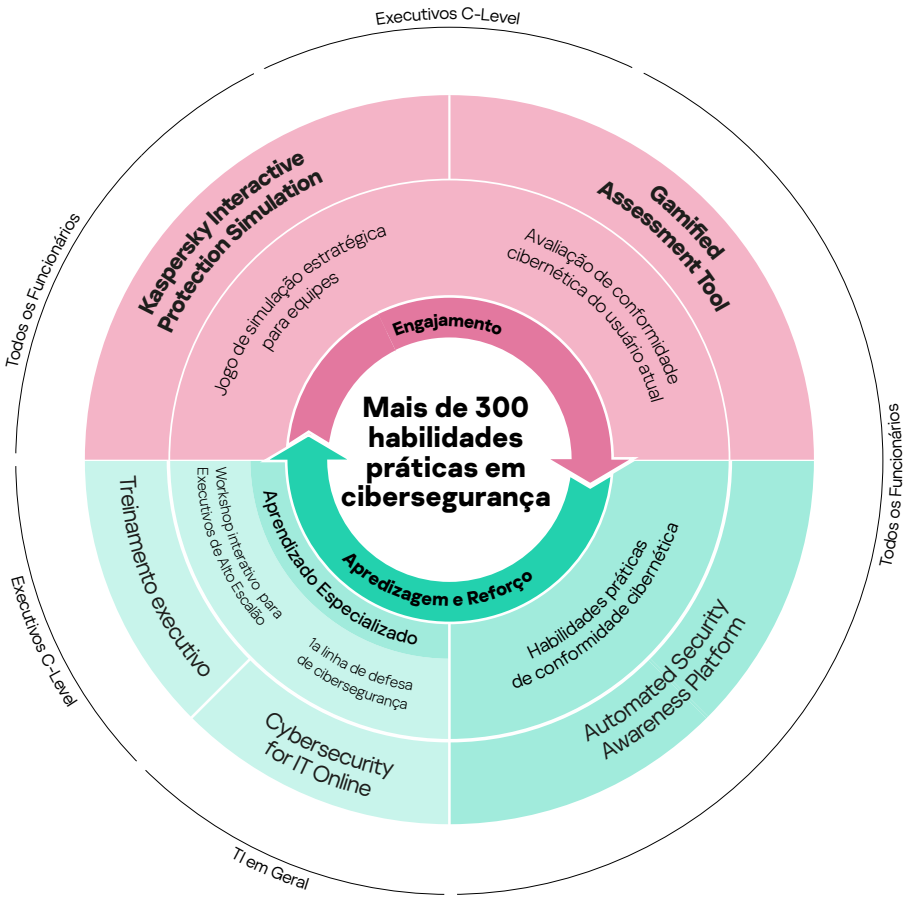
30%
das violações de malware
ocorrem por meio de emails com links e anexos falsos**

79%
dos funcionários
admitem ter se envolvido em pelo menos uma atividade de risco ao longo do ano, apesar de estarem cientes dos riscos***

164,00 dólares
por registro
O custo global médio para violações, envolvendo entre 2.200 e 102.000 registros****

42% dos entrevistados
que trabalham em empresas com mais de 1000 funcionários
disseram que a maioria dos programas de treinamento dos quais participaram foram inúteis e tediantes*****

Diferentes formatos de treinamento para diferentes níveis organizacionais



* "IT Security Economics 2022" Kaspersky
** Data Breach Investigation Report, 2022
*** Balancing Risk, Productivity, and Security, Delinea 2021
**** Cost of a Data Breach, 2022. IBM
*****Capgemini "The digital talent gap"

Soluções Kaspersky Security Awareness

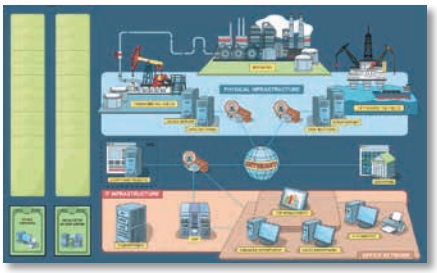
Engajamento e motivação

Nem sempre os funcionários estão interessados em mais treinamentos obrigatórios e, quando se trata de cibersegurança, vários deles consideram isso muito complicado e tediante, 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 encarregados na educação corporativa é envolver os executivos de negócios nos treinamentos; mesmo que seus erros possam custar à empresa tanto quanto os de todos os outros. É aqui que entra o formato de jogos – por serem tão envolventes, é a maneira mais eficaz de incentivar sua equipe a superar a resistência inicial ao treinamento.

76% dos CEOs admitem contornar os protocolos de segurança para fazer algo mais rápido, sacrificando a segurança pela agilidade*.

62% dos gerentes admitem que as falhas de comunicação em relação à segurança de TI dentro da organização levam a pelo menos um incidente de cibersegurança**

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



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

O KIPS é um jogo interativo para equipe com duração de 2 horas que estabelece uma compreensão entre os tomadores de decisões (executivos seniores de negócios, TI e funcionários de cibersegurança) 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 comerciais – o objetivo principal é manter tudo 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 para diferentes indústrias (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.

O KIPS está disponível em duas versões

A versão mais popular - KIPS Live cria uma atmosfera indescritível de emoção e entusiasmo graças à competitividade presencial. É uma ótima ferramenta para engajar e construir uma cultura de cibersegurança dentro de uma organização.

Na versão KIPS Online, os usuários podem interagir com um grande número de participantes de qualquer lugar. Perfeito para organizações globais ou atividades públicas, o KIPS Online pode ser combinado ao KIPS presencial para incluir equipes remotas ao evento local.

- Até 300 equipes (= 1000 trainees) ao mesmo tempo, de qualquer local.
- Diferentes equipes podem escolher uma interface de jogo em diferentes idiomas.
- Os clientes podem personalizar os cenários pré-instalados ao determinar a quantidade e tipos de ataques na biblioteca do jogo.
- Outro benefício da versão online é obter estatísticas sobre as escolhas feitas pelos jogadores, dados sobre as ações das equipes em determinadas situações, além de um parâmetro de ações de jogadores em relação à partida anterior.

KIPS para grandes empresas

Clientes com uma licença que permite jogar o KIPS ilimitadamente durante sua validade podem executá-lo com configurações predefinidas ou personalizar o cenário do jogo para cada partida, escolhendo e combinando diferentes ataques disponíveis na biblioteca. Essa funcionalidade modifica o jogo a cada execução, tornando-o ainda mais interessante.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritysgreatest-insider-threat-is-in-thec-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speak-fluent-infosec-2023/

Início

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

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 cenário, com explicações e dicas úteis.

A abordagem gamificada do GAT motiva os funcionários e, ao mesmo tempo, demonstra que, ao resolver determinadas situações de cibersegurança, pode haver brechas 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.

Aprendizado

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

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 constrói um cronograma educacional para cada grupo de funcionários, proporcionando aprendizado em intervalos oferecido automaticamente por meio de uma combinação de formatos de treinamento.

- **Facilidade de uso para administradores** Gerenciamento automatizado da plataforma, sincronização com AD (Active Directory), SSO (Single Sign-On), Open API (capacidade de interagir com soluções de terceiros), painel fácil de usar, integração online durante a primeira visita, uma seção de perguntas frequentes e dicas tornam o gerenciamento da plataforma conveniente e eficiente.

- **E também para alunos:** Estrutura de aulas clara, lições pequenas, exemplos da vida real, interface amigável, lembretes por e-mail, capacidade de retornar e repetir as aulas, se necessário, interface amigável para PC ou celular – tudo isso torna o processo de aprendizado agradável, interessante e eficaz.

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
- Email
- Websites e Internet
- Redes sociais e aplicativos de mensagens
- Segurança do PC
- Dispositivos móveis
- Proteção de dados confidenciais
- GDPR
- Cibersegurança para a indústria
- Dados pessoais
- Segurança de cartões bancários e PCI DSS
- Doxing
- Segurança de criptomoedas
- Segurança da informação ao trabalhar remotamente
- Lei federal russa 152-FZ

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 multi-idiomas.

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.

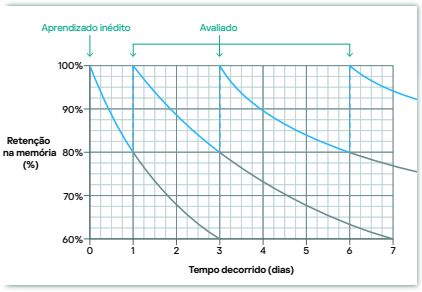
Consolidação

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.

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



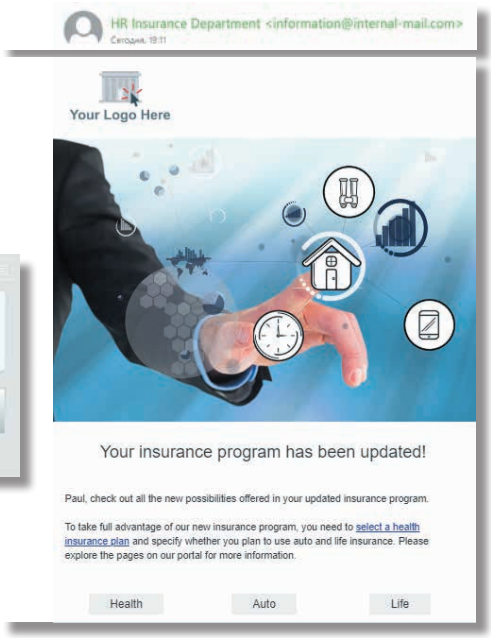
- **Eficiência de aprendizado predefinida:** o conteúdo do programa é estruturado para oferecer aprendizado incremental em intervalos com reforço constante. A metodologia baseia-se na especificidade da memória humana para garantir a retenção de conhecimentos e a subsequente aplicação de habilidades.
- **Personalização:** É fácil alterar a aparência do programa de treinamento – substitua o logotipo da Kaspersky pelo logotipo da sua empresa no portal do aluno e no portal do aluno e nos emails da plataforma, personalize certificados e adicione conteúdo pessoal a qualquer aula.
- **Aprendizado flexível:** escolha a opção de treinamento de funcionários certa para você: atribuir aos funcionários um Curso expresso básico que ajudará você a atender rapidamente aos requisitos regulamentares para treinamento de segurança cibernética ou atualizar seus conhecimentos, ou escolha o Curso principal dividido em níveis de complexidade para fornecer informações mais detalhadas e desenvolver habilidades de segurança cibernética mais sólidas.
- **Licenciamento flexível** (para provedores de serviços gerenciados): o modelo de licenciamento por usuário pode começar com apenas 5 licenças e várias empresas podem ser gerenciadas a partir de uma única conta.

Campanhas de simulação de phishing

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

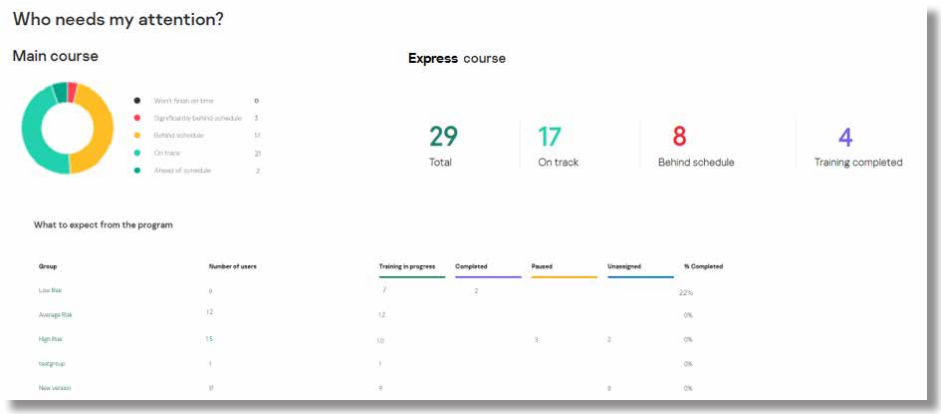
Aulas interativas

Simulações de ataques de phishing



Acompanhando 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.



Aprendizado especializado

Especialistas gerais de TI: membros da equipe de Helpdesk e outros funcionários com conhecimento técnico geralmente são deixados de fora de treinamentos similares, pois os programas de conscientização padrão não são suficientes para eles. Porém, ao mesmo tempo as empresas também não precisam transformá-los em especialistas de cibersegurança: esse processo 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 um treinamento padrão para os demais funcionários.

Módulos de treinamento CITO:

- Softwares maliciosos
- Programas e arquivos potencialmente indesejados
- Noções básicas sobre investigação
- Reação a incidentes de phishing
- Segurança de servidores
- Segurança do Active Directory

Método de entrega CITO:

Formato em Nuvem ou SCORM

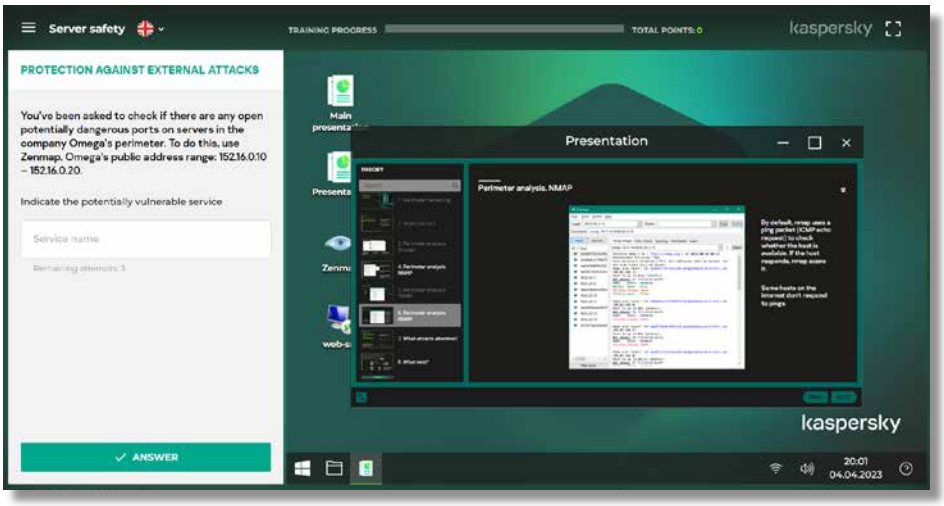
Cybersecurity for IT Online: a primeira linha de defesa contra incidentes

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 inofensivo. Ele também gera um interesse pela busca de sintomas causados por atividades maliciosas – 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.



Trazendo os executivos a bordo

Os gerentes C-Level estão entre os alvos mais desejados dos cibercriminosos, mas, muitas vezes, eles são um verdadeiro desafio para os educadores. No entanto, sem seu envolvimento e apoio nas várias iniciativas e advocacia de cibersegurança, é impossível criar uma cultura de segurança de TI na organização.

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

Treinamento para executivos:

Em nosso programa de treinamento para executivos, os líderes de negócios e os principais gerentes aprendem os fundamentos da cibersegurança por meio de um workshop interativo conduzido por um tutor ou curso on-line que dá a eles uma melhor compreensão das ciberameaças e como se proteger contra elas.

Atenção especial é dedicada 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 nos negócios. Eles descobrirão o que o cenário atual de ameaças significa para a empresa, quais ações tomar em caso de um ciberataque, além de uma série de outras informações interessantes, relevantes e úteis.

Para aproveitar ainda mais este curso, o ideal é combiná-lo com o treinamento KIPS. O treinamento para executivos pode ser feito antes ou depois do KIPS, dependendo de sua abordagem de conscientização de segurança.

* A lista atualizada de módulos está disponível em cito-training.com

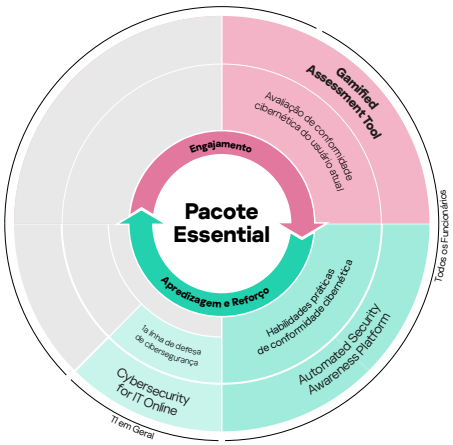
Kaspersky Security Awareness: maneiras flexíveis de treinamento

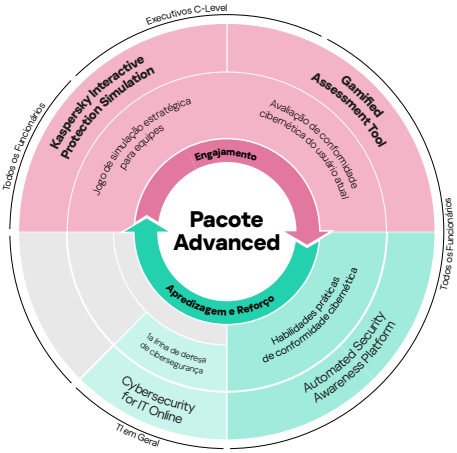
As soluções Kaspersky cobrem todos os níveis da sua empresa e podem ser usadas isolada ou coletivamente. Oferecemos também pacotes adaptados às suas necessidades, facilitando a adoção da solução.

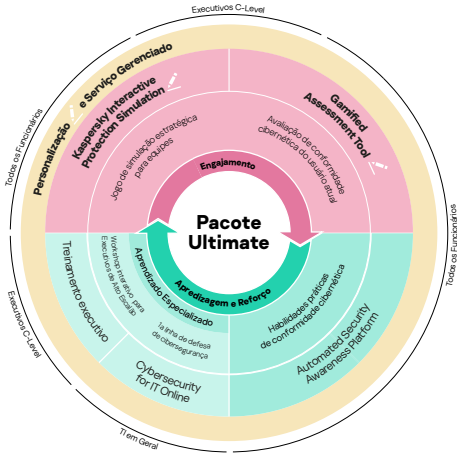
A solução fácil de usar e que aumenta a conscientização sobre cibersegurança dos funcionários – simples de configurar, fácil de gerenciar.
Fornece um nível básico de treinamento em segurança para ajudar você a operar com sucesso e atender aos requisitos regulatórios ou de terceiros de treinamento geral em cibersegurança.

Ajuda as organizações maiores a manter a continuidade dos negócios usando uma solução de treinamento simples e pronto para uso. É compatível com todos os níveis organizacionais, abordando todas as etapas do ciclo de aprendizagem.

Garante o máximo de conscientização em cibersegurança, fornecendo serviços de personalização e gerenciamento para que os executivos se tornem experientes em caso de ameaças. Os funcionários adquirem habilidades de cibersegurança automáticas, e a equipe geral de TI 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 Security Awareness: kaspersky.com.br/awareness
Notícias sobre segurança de TI: business.kaspersky.com/

kaspersky.com.br

kaspersky