Atraente para os funcionários, eficiente para os gerentes.

Avaliação gratuita
k-asap.com/br

Kaspersky ASAP: Automated Security Awareness Platform

kaspersky bring on the future

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP: Automated Security Awareness Platform

82% de todos os incidentes cibernéticos são causados por erro humano, causando um prejuízo milionário para as empresas. Os programas de treinamento tradicionais não são desenvolvidos para resolver esse problema, e uma nova abordagem é necessária - é aí que o Kaspersky ASAP entra em jogo!

O erro humano é o maior risco cibernético

79%
dos funcionários
admitem ter se envolvido em pelo menos uma atividade de risco no ano anterior, apesar de estarem ciente dos riscos*

51%
dos funcionários
acreditam que seus departamentos de TI devem ser totalmente responsáveis por impedir que seus empregadores sejam vítimas de ataques cibernéticos*

55%
das empresas
detectaram ameaças causadas pelo uso inadequado de TI pelos funcionários**

51%
das pequenas empresas
sofreram um incidente de segurança devido à violação de políticas de segurança de TI pelos funcionários**

26%
dos funcionários
afirmam que seu email pessoal tem a mesma senha da conta de trabalho***

Barreiras para lançar lançamento de um programa de conscientização de segurança eficiente

Embora as empresas estejam ansiosas para implementar programas de conscientização de segurança, muitas estão insatisfeitas com o processo e os resultados. As pequenas e médias empresas, em especial, acham isso desafiador, pois tendem a não ter a experiência ou os recursos necessários.

Ineficiente para estudantes

Considerado como difícil, chato e uma tarefa entediante irrelevante.

Totalmente centrado em "não fazer", em vez de "como fazer"

O conhecimento não é retido

Ler e ouvir não são tão eficazes como fazer

Um problema para os administradores

Como criar um programa e definir objetivos?

Como gerenciar tarefas de treinamento?

Como controlar o progresso

Como garantir que a equipe esteja totalmente engajada?

* Balancing Risk, Productivity, and Security."Delinea, 2021

** "ITSecurity Economics 2022", Kaspersky

*** https://www.beyondidentity.com/blog/password-sharing-work

Treinamento eficiente e fácil de gerenciar - para organizações de qualquer tamanho

Apresentamos o Kaspersky ASAP, ou Automated Security Awareness Platform, que constitui o núcleo do portfólio do treinamento em conscientização de segurança da Kaspersky. A plataforma é uma ferramenta online que desenvolve competências de higiene cibernética robustas e práticas para os funcionários ao longo do ano.

Lançar e gerenciar a plataforma não requer recursos nem planos especiais e inclui ajuda integrada em cada fase do percurso rumo a um ambiente cibernético empresarial seguro.

Conteúdo significativo que você não pode ignorar

Um dos critérios mais importantes ao escolher um programa de conscientização é a eficiência e, com o ASAP, a eficiência é incorporada ao conteúdo e ao gerenciamento do treinamento. O conteúdo é baseado na experiência acumulada de **mais de 25 anos em segurança cibernética,** expressa em um modelo de aulas composto por mais de **350 habilidades práticas e essenciais de cibersegurança** que todos os funcionários devem ter.

Treine seus funcionários na conscientização em cibersegurança.
Mude a atitude e o comportamento dos funcionários e proteja seus negócios e sistemas de TI.

Formação eficiente

Consistente	– Conteúdo estruturado e bem pensado – Lições interativas, reforço constante, testes, ataques de phishing simulados para garantir a aplicação das aulas O conteúdo e a estrutura do material de treinamento levam em consideração as especificidades da memória humana e nossa capacidade de absorver e reter informações.
Prática e atrativa	– Relevante para as tarefas cotidianas dos funcionários – Competências que podem ser usadas imediatamente Exemplos de situações da vida real que os funcionários podem relacionar consigo mesmos para contribuir para um melhor envolvimento do aluno, ajudando na retenção de informações.
Positiva	– Atribui uma ênfase proativa ao comportamento seguro – Explica "por quê" e "como fazer" em vez de apenas tabus Regras e restrições em excesso podem causar descontentamento e descomprometimento, enquanto explicações e princípios alinhados com a forma como as pessoas pensam contribuem naturalmente para a adoção e mudanças de comportamento.

Gerenciamento fácil

Fácil de gerenciar	– O gerenciamento de aprendizado totalmente automatizado faz com que todos os funcionários alcancem o nível de competências adequado ao seu perfil de risco sem qualquer intervenção do administrador da plataforma – Sincronização com AD (Active Directory), SSO (Single Sign-On), Open API (capacidade de interagir com soluções de terceiros), integração online durante a primeira visita, uma seção de perguntas frequentes e dicas tornam o gerenciamento da plataforma conveniente e eficiente.
Fácil de controlar	Painel "tudo em um" e relatórios acionáveis: – relatórios do andamento das lições – relatórios de testes e ataques de phishing simulados
Fácil de manter os alunos motivados	A plataforma envia automaticamente convites e lembretes, além de relatórios para alunos e administradores.

Gerenciamento do ASAP: simplicidade via automação total

Inicie o seu programa em 4 passos simples

1

Adicionar usuários

Use a **sincronização com o AD** ou faça o upload de um arquivo .xlsx ou adicione-os manualmente

2

Dividir os usuários por grupos

Divida os usuários manualmente ou usando regras com base no nível de destino desejado

3

Iniciar o treinamento

Divida os usuários manualmente ou usando regras com base no nível de destino desejado e defina a data de início para cada grupo

4

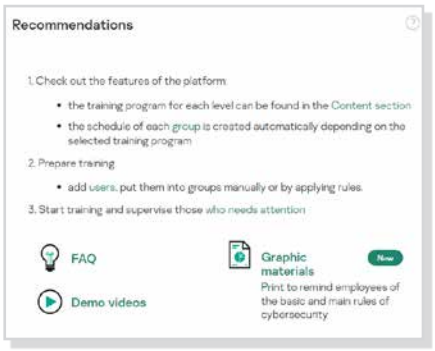
Gerenciamento automatizado de treinamento feito pelo ASAP

O ASAP cria uma programação para cada grupo, para convites, lembretes e outras comunicações – automaticamente

Uma abordagem nova e aprimorada ao treinamento

O Kaspersky ASAP está mudando a maneira como fornecemos conteúdo de aprendizado de cibersegurança. Agora você pode optar por atribuir aos funcionários um Curso Express básico que os ajudará a atender rapidamente aos requisitos regulamentares para treinamento em segurança cibernética, atualizar seus conhecimentos ou optar pelo Curso principal dividido em níveis de complexidade

Integração durante o primeiro login, recomendações, perguntas frequentes e vídeos de demonstração explicando como a plataforma funciona da perspectiva do administrador e do usuário – tudo o que você precisa para iniciar o processo de aprendizado está na página principal do administrador



Tópicos abordados

Tópicos abordados

Curso Principal	Curso Express
E-mail	E-mail
Senhas e contas	Senhas e contas
Websites e Internet	Websites e Internet
Redes sociais e aplicativos de mensagens	Segurança de dispositivos móveis
Segurança do PC	Mídias sociais
Dispositivos móveis	Meu computador
Proteção de dados confidenciais	Proteção de dados confidenciais
Dados pessoais	Doxing
GDPR	Segurança de criptomoedas
Cibersegurança para a indústria	Segurança da informação ao trabalhar remotamente
Segurança de cartões bancários e PCI DSS	Lei federal 152-FZ (para a Rússia)

Os tópicos são divididos em grandes blocos, abrangendo vários conceitos de segurança de TI *.

#Senhas #Phishing #Contas corporativas #Mensagens perigosas #Cartões bancários #Ransomware #Engenharia social #Arquivos perigosos #Trabalhar com navegadores #Ética corporativa #Antivírus #Software malicioso #Aplicativos #Navegador #Informações confidenciais #Armazenamento de informações #Envio de informações #Dados pessoais #Internet e a lei #Legislação europeia #Negócios #Links perigosos #Sites falsos #Sites de ransomware #Backup #Dados móveis #Criptografia #Serviços em nuvem #Espionagem industrial #PCI DSS #Autenticação de dois fatores #Pegada digital #Torrents #Catfishing #Ataque direcionado #Hashing #Tokens #Bloqueios de padrões #Mineração #Controle parental

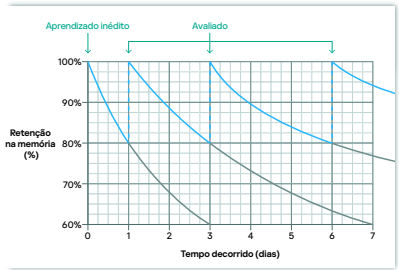
* Para obter a lista mais recente de tópicos e conceitos, consulte k-asap.com/br

Cada tópico tem vários níveis que abordam competências de segurança específicas. Os níveis são definidos de acordo com o grau de risco que ajudam a eliminar – por exemplo, o nível 1 normalmente é suficiente para proteger contra os ataques mais simples, bem como ataques em massa. Os níveis mais altos precisam ser estudados para que você possa aprender a se proteger contra os ataques mais sofisticados e direcionados.

Exemplo: Habilidades treinadas no módulo "Sites e Internet"

Iniciante Para evitar ataques em massa (baratos e fáceis)	**Elementar** Para evitar ataques em massa em um perfil específico	**Intermédio** Para evitar ataques focados bem preparados	**Avançado*** Para evitar ataques direcionados
23 aulas, incluindo: – Reconhecer pop-ups falsos – Prestar atenção a redirecionamentos – Distinguir links de download genuínos de falsos – Reconhecer arquivos executáveis encontrados na Web – Ser capaz de determinar a autenticidade de uma extensão do navegador	**34 aulas, incluindo:** – Inserir dados apenas em sites com um certificado SSL válido – Usar senhas diferentes para diferentes registros – Reconhecer sites falsos por vários sinais – Evitar links numéricos – Reconhecer endereços de link de rede inválidos por subdomínios falsos	**12 aulas, incluindo:** – Verificar os links de compartilhamento antes de enviar – Usar software apenas de fabricantes confiáveis para torrents – Baixar apenas conteúdo legal de torrents – Limpar os cookies do navegador regularmente	**13 aulas, incluindo:** – Reconhecer links falsos sofisticados (incluindo links que parecem websites empresariais, links com redirecionamentos) – Verificar sites usando utilitários especiais – Reconhecer se o navegador está minerando – Evitar sites black SEO
	+ reforço de competências elementares	+ reforço das competências anteriores	+ reforço das competências anteriores

"Curva do esquecimento" de Ebbinghaus



Curso express do ASAP

Uma versão curta do treinamento em formato de áudio e vídeo. Cada tópico de cibersegurança contém várias lições curtas para ajudar o usuário a compreender as habilidades básicas de cibersegurança.

- Teoria interativa
- Vídeos
- Testes

Ataques de phishing simulados não estão incluídos no caminho de aprendizado, mas podem ser atribuídos separadamente pelo administrador.

Curso principal do ASAP

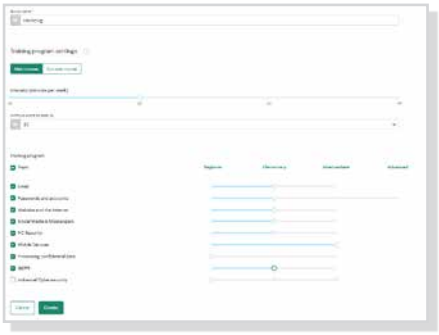
O treinamento é baseado nas especificidades da memória humana:

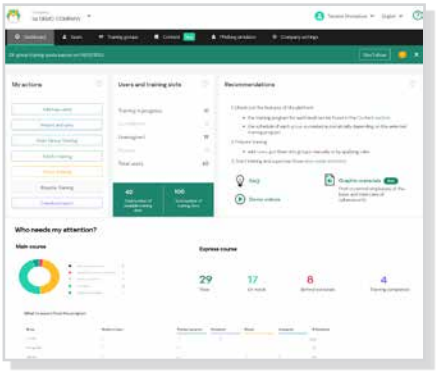
- Conteúdo multimodal:
  - cada unidade inclui uma lição interativa, reforço, avaliação (teste e ataque de phishing simulado, quando aplicável)
  - todos os elementos de formação consolidam a competência particular que é ensinada em cada unidade para que as competências sejam verdadeiramente dominadas e se tornem parte do novo comportamento pretendido

- Aprendizado em intervalos:
  - os elementos do treinamento seguem uns aos outros em determinados intervalos, o que elimina a abordagem de simplesmente clicar em lições e melhora a retenção da memória. Os intervalos são baseados no estudo "Curva do esquecimento" de Ebbinghaus
  - a repetição cria hábitos seguros e previne o esquecimento

- O conteúdo estruturado e equilibrado relevante para a vida real garante eficiência:
  - repleto de exemplos da vida real que destacam a importância pessoal da segurança cibernética para os funcionários
  - a plataforma tem como foco a formação em competências, não apenas na transmissão de conhecimento. Assim, exercícios práticos e tarefas voltadas para o funcionário são a base de cada módulo.

Caminho de aprendizado flexível





Aprendizagem flexível

O escopo do treinamento é completamente flexível, mantendo as vantagens do gerenciamento de aprendizado automatizado sequencial. Para cada grupo de treinamento, é possível escolher:

- Curso principal ou Curso express, ou ainda uma combinação de ambos.
- Tópicos para treinar no Curso principal e/ou no Curso express que os alunos do grupo precisam aprender.
- O nível que você deseja que os alunos atinjam para cada tópico escolhido no Curso principal.

O caminho de aprendizado será construído automaticamente pela plataforma para cada grupo de alunos com base nessas configurações.

Faça tudo isso no painel

- Tudo o que você precisa para controlar e gerenciar o treinamento – estatísticas, resumos das atividades e progresso dos usuários, slots de treinamento, treinamento em grupo, sugestões sobre como melhorar os resultados – pode ser feito no painel. Você pode baixar relatórios com um único clique, além de configurar a frequência desses relatórios.

Confiança para um bom desempenho

- Os funcionários podem estudar sempre que for conveniente para eles e em qualquer dispositivo: o design compatível com dispositivos móveis do ASAP torna o aprendizado conveniente e confortável.
- Os usuários podem acessar o portal de treinamento a partir de links personalizados fornecidos no convite de treinamento ou por meio de um único link para todos os usuários com tecnologia Single Sign-On (SSO) – se configurada pelo administrador.

Personalização

O administrador pode alterar facilmente a aparência do programa:

- substituir o logotipo da Kaspersky pelo logotipo da sua empresa no painel de administração, no portal de treinamento e nos e-mails da plataforma;
- personalizar certificados;
- adicionar conteúdo pessoal a qualquer lição.

Integração

Você pode usar a Open API para interagir com soluções de terceiros – a Open API funciona via HTTP e oferece um conjunto de métodos de solicitação/resposta.

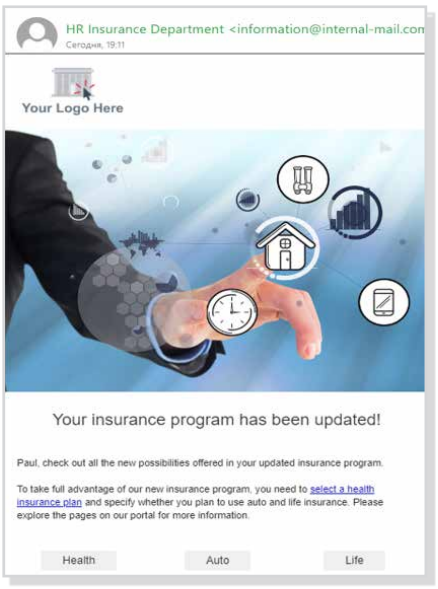
O ASAP pode ser integrado às plataformas Kaspersky KUMA e XDR:
– O administrador pode ver um evento no XDR e obter a resposta apropriada, incluindo a atribuição de um treinamento no ASAP
– Enriquecimento automático das fichas de incidentes com informação sobre o nível de conscientização do usuário atacado

Localização

O ASAP está disponível em 25 idiomas*. A localização no ASAP vai além da simples tradução – os textos e imagens não são apenas traduzidos para diferentes idiomas, mas também ajustados para refletir diferentes culturas e atitudes locais.

* A lista atual de idiomas oferecidos está disponível em k-asap.com/br

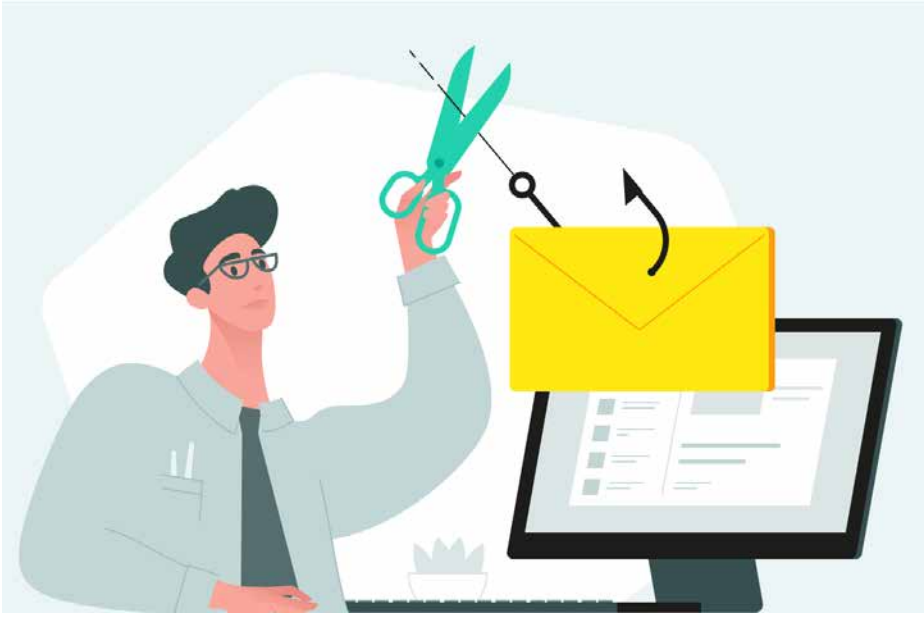
Exemplo do modelo editável de phishing simulado e feedback



Campanhas de simulação de phishing

Além do treinamento principal, campanhas de phishing também são oferecidas. Elas testam as habilidades práticas dos funcionários para evitar ataques de phishing, ajudam os gerentes de treinamento a identificar rapidamente as brechas no conhecimento dos usuários e incentivam o estudo mais aprofundado de tópicos problemáticos. As campanhas de phishing também são uma excelente ferramenta para ensinar os funcionários a reconhecer sinais potencialmente prejudiciais e colocar seus conhecimentos em prática.

A plataforma oferece modelos de email prontos contendo exemplos de phishing que podem ser enviados aos usuários em todos os idiomas disponíveis. Os modelos são sempre atualizados e novos modelos são adicionados regularmente. Você também pode criar emails personalizados com base em modelos predefinidos.



Experimente um ataque de phishing simulado antes de iniciar o treinamento – verifique a resiliência dos seus funcionários! Isso ajudará os funcionários e a gerência a ver os benefícios do treinamento.

Os funcionários também podem demonstrar sua compreensão de um tópico não sendo enganados por um ataque de phishing simulado e relatando emails de phishing por meio da ferramenta "Relatar phishing".

A ferramenta "Relatar phishing" demonstra o nível de conscientização dos funcionários, remove emails da caixa de entrada e envia mensagens não apenas para o administrador da plataforma, mas também para as equipes de TI/segurança de TI para ajudar as organizações a melhorar seus níveis de detecção e resposta de phishing.

Kaspersky Security Awareness – uma nova abordagem no domínio de competências em segurança de TI

Principais diferenciais do programa

Experiência sobre cibersegurança significativa
Mais de 25 anos de experiência em cibersegurança transformados em um conjunto de habilidades relacionadas que residem no coração de nossos produtos

Treinamento que muda o comportamento dos funcionários em todos os níveis da sua organização
Nosso treinamento gamificado proporciona 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.

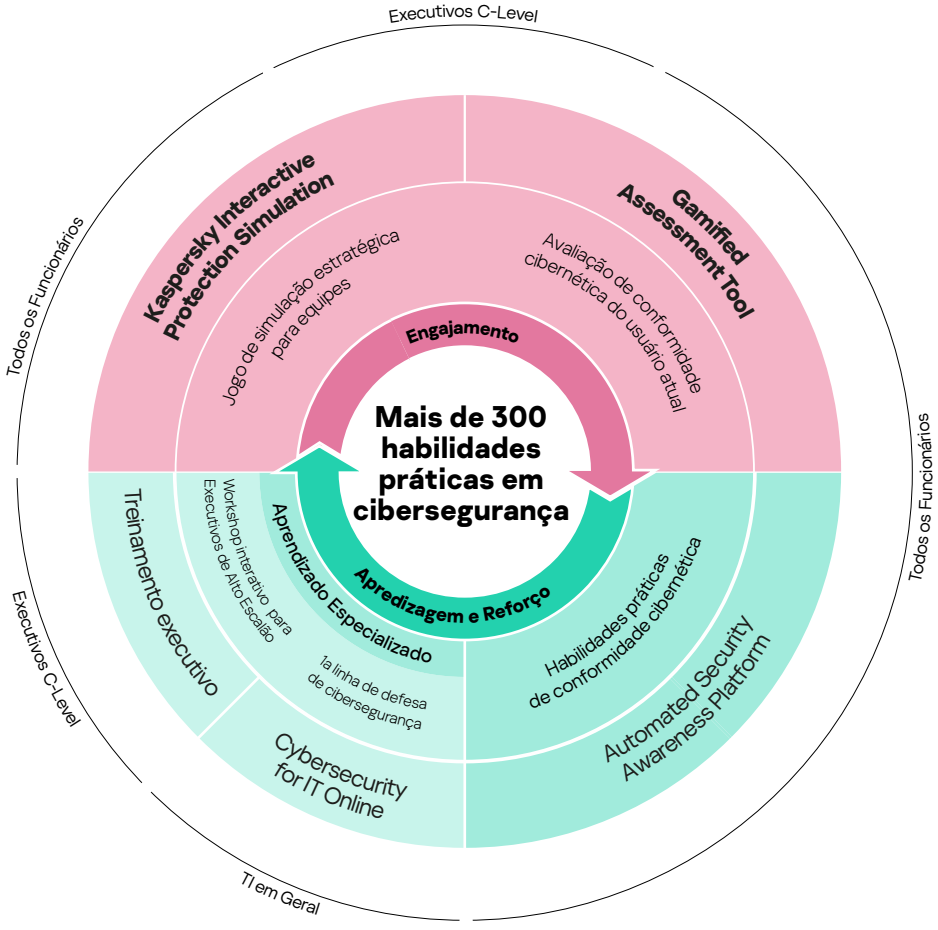
O ASAP é um produto fundamental do portfólio de conscientização de segurança da Kaspersky.

Uma solução de treinamento flexível para todos

O Kaspersky Security Awareness tem um longo histórico internacional de sucesso. Usado por empresas de todos os tamanhos para **treinar mais de um milhão de funcionários em mais de 75 países**, ele reúne os mais de 25 anos de conhecimento em segurança cibernética da Kaspersky com uma ampla experiência em educação de adultos.

O portfólio oferece toda uma variedade de opções de treinamento cativantes que aumentam a conscientização em cibersegurança dos seus funcionários em todos os níveis, capacitando-os para o desempenho de seu papel na cibersegurança geral da sua organização.

Como as mudanças de comportamento sustentáveis são demoradas, a nossa abordagem envolve criar um ciclo de aprendizado contínuo com vários componentes. O aprendizado gamificado engaja a gestão sênior, transformando-os em defensores e apoiadores das iniciativas de cibersegurança, na criação de uma cultura de comportamento de ciberproteção. A avaliação gamificada ajuda a identificar brechas nos conhecimentos da equipe e os motiva ao aprendizado continuado, enquanto plataformas online e simulações os equipam com as habilidades certas e reforçadas.



Avaliação gratuita do Kaspersky ASAP: k-asap.com/br
Cibersegurança empresarial: www.kaspersky.com.br/enterprise
Kaspersky Security Awareness: www.kaspersky.com.br/awareness
Notícias sobre segurança de TI: business.kaspersky.com.br

www.kaspersky.com.br

kaspersky bring on the future