Kaspersky Interactive Protection Simulation

Promova
a conscientização
sobre cibersegurança
para a alta gestão
e os tomadores
de decisão

kaspersky bring on the future

Saiba mais em
kaspersky.com.br/awareness

Kaspersky Interactive Protection Simulation

O "problema das pessoas"

Um dos maiores desafios de segurança enfrentados na atualidade é que diferentes funções de gerenciamento sênior veem a segurança cibernética de diferentes perspectivas e têm prioridades diferentes. Isso pode resultar em uma espécie de "Triângulo das Bermudas de Segurança" para tomada de decisão:

- Empresas veem as medidas de segurança
- como contrárias às suas metas de negócios (mais barato/rápido/melhor).
- Os gerentes de segurança de TI podem sentir que a cibersegurança como uma questão de infraestrutura e investimento está fora de suas atribuições.
- Os gerentes encarregados do controle de custos podem não ver como os gastos com cibersegurança se relacionam com as receitas e como geram economia, em vez de gerar custos.

A compreensão mútua e a parceria entre esses 3 são cruciais para uma cibersegurança eficaz. No entanto, os formatos tradicionais de conscientização, como palestras e exercícios vermelho/azul, são falhos: longos, excessivamente técnicos e inadequados para gerentes ocupados, e não conseguem construir uma "linguagem comum".

A ciber-imunidade de uma empresa começa pela alta gestão.

Para muitas empresas da atualidade, buscar a sustentabilidade de sua infraestrutura de TI é prioridade. No entanto, lidar com os problemas de cibersegurança é geralmente uma responsabilidade do pessoal de TI e de segurança de TI, o que pode criar uma cultura fragmentada de comportamento de cibersegurança dentro da empresa. Líderes de negócios focam majoritariamente em vendas, experiência do cliente, riscos e custos e, geralmente, negligenciam a cibersegugrança, conforme trabalham para atingir seus objetivos. Mas sem o apoio da diretoria, liderar pelo exempo, criando uma cultura unificada de cibersegurança, pode ser uma meta inatingível.

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

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

51% do pessoal de Segurança da Informação acha que o mais difícil é abordar a necessidade de mais orçamento para a segurança de TI... mas estão alinhados quando se trata de criar estratégias de comunicação que funcionam.

A maioria dos executivos **(56%) e do pessoal de TI (48%)** concorda que fornecer exemplos que acontecem na vida real é o melhor método para facilitar a comunicação sobre problemas relacionados à cibersegurança**.

Como a conscientização sobre segurança da Kaspersky é útil

O Kaspersky Security Awareness é uma solução comprovada, eficiente e eficaz, com um longo histórico de sucesso internacional. Usado por empresas de todos os portes para **treinar mais de um milhão de funcionários em mais de 75 países**, a solução reúne mais de 25 anos da experiência da Kaspersky em cibersegurança, com o know-how abrangente da Kaspersky Academy em educação para adultos.

O porfólio é composto de produtos de treinamento que engajam e **aumentam a conscientização sobre cibersegurança** dos colaboradores em todos os níveis, capacitando-os a fazer a sua parte para contribuir com a cibersegurança para toda a empresa.

Cada produto no portfólio tem um papel específico no ciclo de aprendizagem geral, estando disponível também de forma independente.

Um jogo estratégico corporativo de cibersegurança para executivos

O Kaspersky Interactive Protection Simulation (KIPS) é uma simulação estratégica de negócios, um jogo para equipe que demonstra a conexão entre eficiência empresarial e cibersegurança.

Os participantes são posicionados em um ambiente simulado de empresa como membros da equipe de segurança de TI, e enfrentam uma série de ciberameaças inesperadas, tendo que manter a empresa operando perfeitamente e gerando receita.

Eles têm que criar uma estratégia de ciberdefesa ao escolher entre os melhores controles proativos e reativos disponíveis. Cada escolha gera mudanças na maneira que o cenário se desenrola, afetando em última instância o volume de receita que a empresa é capaz de gerar ou não.

Equilibrando as prioridades de engenharia, negócios e segurança com o custo de um ataque cibernético realista, as equipes analisam dados e tomam decisões estratégicas com base em informações incertas e recursos limitados. Se isso lhe parece familiar, é porque todos os cenários são baseados em eventos que aconteceram na vida real.

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

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

O KIPS é um jogo dinâmico de conscientização, com uma abordagem "aprenda na prática":

- Divertido, envolvente e rápido (2 horas).
- O trabalho em equipe desenvolve a cooperação.
- A concorrência estimula iniciativas e habilidades de análise.
- A jogabilidade promove o entendimento sobre as medidas de cibersegurança.
- Todos os cenários e ataques são baseados em casos da vida real

Como o KIPS funciona

O treinamento KIPS é direcionado a especialistas em sistemas de negócios, pessoal de TI e gerentes de linha, e deve aumentar sua conscientização sobre os riscos e problemas de segurança de sistemas computadorizados modernos.

Cada equipe de 4 a 6 pessoas tem a tarefa de administrar uma empresa, o que envolve unidades de produção e os computadores que as controlam. Durante o jogo, as unidades de produção geram receita, reconhecimento público e resultados de negócios. Ao mesmo tempo, as equipes têm que lidar com ciberataques que ameaçam impactar no desempenho de negócios.

Ao final do jogo, os participantes adquiriram insights acionáveis e importantes que podem aplicar no seu trabalho.

- Ciberataques prejudicam a receita e devem ser tratados pela alta gestão
- A cooperação entre tomadores de decisão de TI e não TI é essencial para uma cibersegurança eficaz em toda empresa.
- Um orçamento de segurança adequado não vai falir a empresa, mas a perda de receita devido a um ciberataque bem sucedido pode...
- As pessoas se tornam rapidamente confortáveis com os controles de segurança e sua importância (treinamento de auditoria, antivirus etc).

O KPIS está dipsonível em duas versões:

A opção mais popular **KIPS presencial** cria uma atmosfera empolgante e envolvente e é uma excelente ferramenta para engajar e fomentar uma cultura de cibersegurança dentro da organização.

Na versão **KIPS Online**, os usuários podem interagir com um grande número de participantes estando localizados onde for mais conveniente.

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 treinees) em simultâneo, 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.
- 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.
- Outro benefício da versão online é obter estatísticas sobre as escolhas feitas pelos jogadores, dados sobre as ações das equipes em deerminadas situações, além de um parâmetro de ações de jogadores em relação à partida anterior.

O KIPS demonstra:

- O papel desempenhado pela cibersegurança para a continuidade dos negócios e para a lucratividade.
- Os desafios e ameaças emergentes enfrentados pelas empresas.
- Os erros típicos cometidos por empresas ao desenvolver sua cibersegurança.
- Como a cooperação entre as equipes de negpocios e cibersegurança mantém as operações estáveis e uma proteção sustentável contra as ciberameaças.

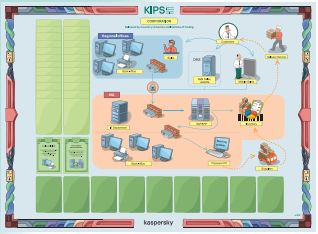
Dependendo do cenário, as equipes são resonsáveis pela segurança de TI da empresa em determinado setor. Sua tarefa é garantir o funcionamento normal, ininterrupto da empresa, manter as relações com os clientes e fornecedores, identificar e neutralizar ciberameaças.

À medida que a empresa sofre um ciberataque, os jogadores experimentam o impacto na produção e nas receitas e aprendem a adotar diferentes estratégias e soluções de negócios e de TI para minimizar o impacto do ataque sem perder mais receita.

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, **VENCE!**

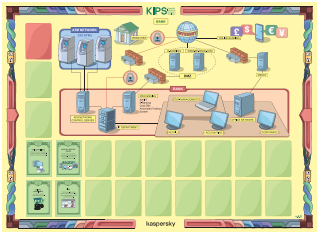
Cenários de KIPS corporativos para todos os verticais de mercado

Corporação



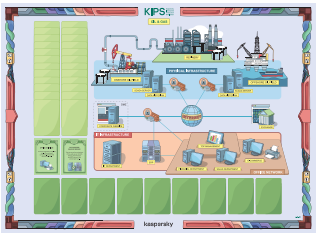
Proteja a empresa contra **ransomware, APTs, falhas de segurança de automação.**

Banco



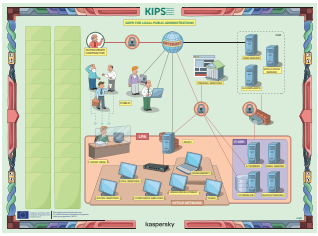
Proteja as instituições financeiras contra **APTs emergentes de alto nível, como Tyukpin, Carbanak.**

Petróleo e gás



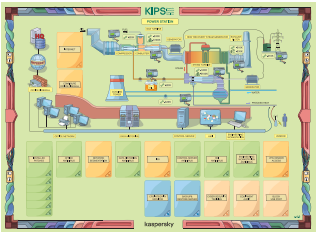
Explore o impacto de uma variedade de ameaças, desde **fraude de websites até um ransomware real e uma APT sofisticada.**

Administrações públicas locais



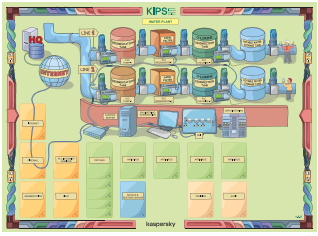
Proteja os servidores web públicos contra ataques e exploits.

Centrais elétricas



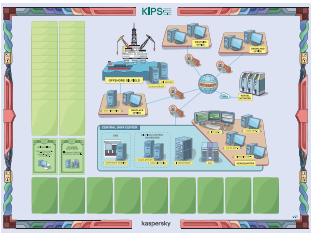
Proteja sistemas de controle industrial e infraestrutura crítica contra ataques cibernéticos em estilo Stuxnet.

Tratamento de água



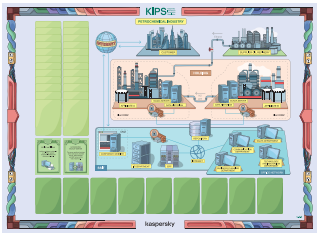
Proteja a infraestrutura de TI de estações de tratamento de água, garantindo a estabilidade das linhas de produção.

Holding de petróleo



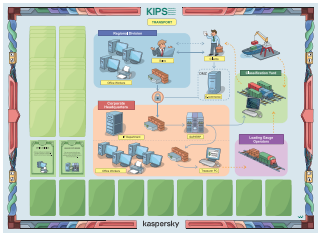
Preserve a cibersegurança para proteger a receita de uma empresa global no setor de Petróleo e Energia, com escritórios em todo o mundo.

Indústria petroquímica



Garanta o funcionamento normal da nova filial de uma grande holding petroquímica, com foco na produção de etileno.

Transporte

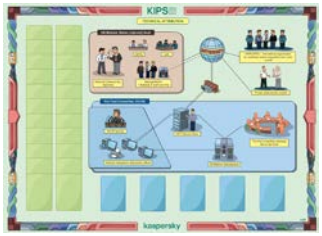


Proteja empresas de logística contra **Heartbleed, APT, B2B Ransomware, Insider.**

Aeroportos

Garanta a segurança dos passageiros e entrega pontual de mercadorias no aeroporto, protegendo seus ativos de inúmeros ciberataques e ameaças.

Atribuição técnica



Investigue e conduza uma atribuição técnica de um complexo ataque APT contra servidores da ONU.

Pequenas e médias empresas

Ajude PMEs a protegerem seus negócios contra ameaças de cibersegurança relacionadas a DDoS, ransomware, hackeamento de aplicativo móvel e roubo de identidade.

Telecomunicações

Proteja os ativos de uma grande holding de telecomunicações, formada por um provedor de telecom, um provedor de serviços na nuvem e um desenvolvedor de jogos, além do escritório sede.

Quer saber mais sobre o KIPS?

Que tal aprofundar sua experiência sobre o KIPS com um **Treinamento Executivo**, parte do portfólio do Kaspersky Security Awareness? Esse treinamento voltado para gestores pode ser feito antes ou depois de jogar KIPS, dependendo da abordagem de Conscientização de Segurança. Impulsione sua experiência sobre o KIPS ao descobrir mais sobre o cenário atual de ciberameaças para a sua empresa, que açoes tomar no caso de um ciberataque, além de uma gama de informações relevantes e úteis. (O Treinament Executivo está disponível em dois formatos: um workshop offline interativo e um curso online)

O que os usuários do KIPS têm a dizer sobre o jogo

A simulação de proteção industrial da Kaspersky foi uma verdadeira revelação e deve ser obrigatória para todos os profissionais de segurança.

Warwick Ashford,
Computer Weekly

Aqui no CERN temos um grande número de sistemas de TI e engenharia, com milhares de pessoas trabalhando neles. Assim, do ponto de vista da cibersegurança, aumentar a conscientização e engajar as pessoas para cuidar da cibersegurança é tão crucial quanto os controles financeiros. O treinamento da Kaspersky provou ser envolvente, brilhante e eficiente.

Stefan Luders,
CERN CISO

Foi realmente revelador, e vários participantes pediram para usar este jogo em suas empresas.

Joe Weiss PE,
CISM, CRISC, ISA Fellow

Temos que construir uma rede de pessoas com base na afiliação e cooperação e o KIPS é uma maneira perfeita de dar o pontapé inicial.

Daniel P. Bagge,
Národní centrum kybernetické bezpeč nosti, Republica Tcheca

Como preparar uma sessão de KIPS

Agenda: Planeje o KIPS como um evento separado ou uma sessão dentro de um evento/conferência/seminário existente (neste caso, o horário ideal para o KIPS é a noite do primeiro dia).

Grupo: 20 a 100 pessoas, divididas em equipes de 3 a 4 participantes, idealmente cada equipe é uma mistura de pessoas da gerência, engenheiros, CISO/segurança de TI:

- é melhor ter pelo menos 1 membro de cada cargo/função,
- as equipes podem ser compostas por pessoas de diferentes ou da mesma empresa/departamento,
- não importa se os participantes se conhecem.

Configuração: O jogo leva de 1,5 a 2 horas, mas a sala deve estar disponível para a equipe de facilitadores Kaspersky por 2 horas antes do jogo para preparação e configuração.

Ambiente: Planeje um espaço de 3m2 por pessoa, numa sala sem colunas, com equipamento audivisual padrão: projetor (6 a 8 lumens), tela, sistema de som (autofalantes, controle remoto, microfones).

Wi-Fi com acesso à internet (para acesso ao servidor de jogos KIPS), com iPad ou tablet 4 Mbps para cada equipe (4 pessoas) compatível com Wi-Fi

Mobiliário: mesas para 4 pessoas (tamanho retangular não inferior a 75x180 cm, ou redonda com diâmetro não superior a 1,5 m), os participantes devem sentar-se em grupos de 4 nas mesas. Mesas para os facilitadores, cadeiras para todos os participantes.

Referências e estudos de caso

O KIPS Game já foi jogado por profissionais de segurança industrial de mais de 50 países.

- O KIPS está traduzido para inglês, russo, alemão, francês, japonês, espanhol UE, espanhol, português, turco, italiano, chinês, holandês e árabe;
- O KIPS é usado por inúmeras agências governamentais, incluindo a agência de Cibersegurança da Malásia, a NSA da República Tcheca, e Cyber Security Centrum na Holanda, impulsionando a conscientização essencial de infraestrutura para centenas de especialistas em organizações de infraestrutura crítica nacionais.
- O KIPS é licenciado para autoridades líderes no setor da educação, como o SANS Institute, onde é usado para treinamento por estudantes de todo o mundo
- O KIPS é licenciado para provedores e fornecedores de serviços de segurança, incluindo Mitsubishi-Hitachi Power Systems, onde é usado para treinaemnto de clientes de infraestrutura crítica
- O KIPS é parte do projeto Geiger da Comissão Europeia para treinar e proteger pequenas e médias empresas contra ciberameaças e aprimorar a gestão de privacidade.

"Treino para o treinador" disponível

Para os casos em que o cliente deseja usar o KIPS para treinar um público mais amplo, como um grande número de funcionários, gerentes e especialistas de vários departamentos ou locais, pode ser útil adquirir a licença para o treinamento KIPS, para educar instrutores internos e executar sessões KIPS no ritmo e comodidade próprios do cliente.

Esse tipo de licença inclui:

- O direito de usar o programa de treinamento KIPS internamente.
- Um conjunto de materiais de treinamento e o direito de utilização/reprodução.
- Login/senha para o servidor de software KIPS pelo tempo de duração da licença.
- Guia do instrutor, educação e treinamento para líderes de programa sobre como executar o treinamento KIPS.
- Manutenção e suporte (atualizações e suporte para o software KIPS e o conteúdo de treinamento).
- Personalização opcional dos cenários KIPS (aplica-se uma taxa extra).

KIPS para parceiros e centros de treinamento

O KIPS é uma excelente oportunidade para parceiros se beneficiarem das soluções de Conscientização de várias maneiras. Além de poder vendê-lo como um produto, eles podem também vender aos seus clientes de centros de treinamento ou até mesmo realizar sessões. (Os especialistas em treinamento Kaspersky podem capacitar os parceiros para o treinamento, caso optem por isso).

Kaspersky Security Awareness

Principais diferenciais do programa

Experiência sobre cibersegurança significativa

Mais de 25 anos de experiência em cibersegurança transformados em habilidades de ciberproteção no cerne dos 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.

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

Como mudanças de comportamento sustentáveis levam tempo, a nossa abordagem envolve criar um ciclo de aprendizagem 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 lacunas nos conhecimentos da equipe e os motiva ao aprendizado continuado, enquanto plataformas online e simulações os equipam com as habilidades certas e reforçadas.

Ciclo de aprendizado contínuo

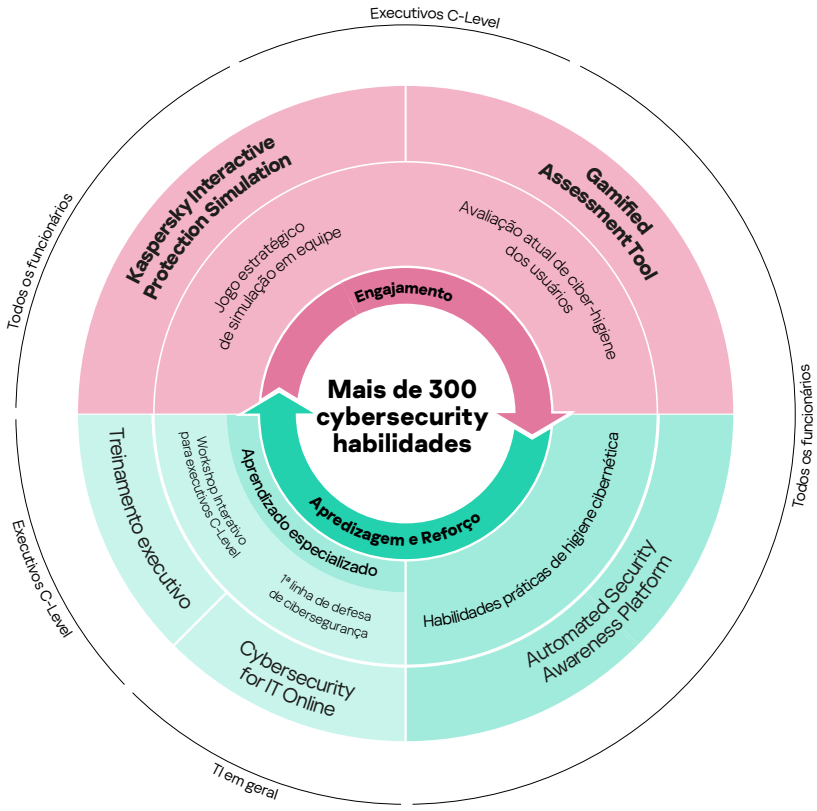
Engajamento/motivação
- Por que preciso disso?
- Cognição

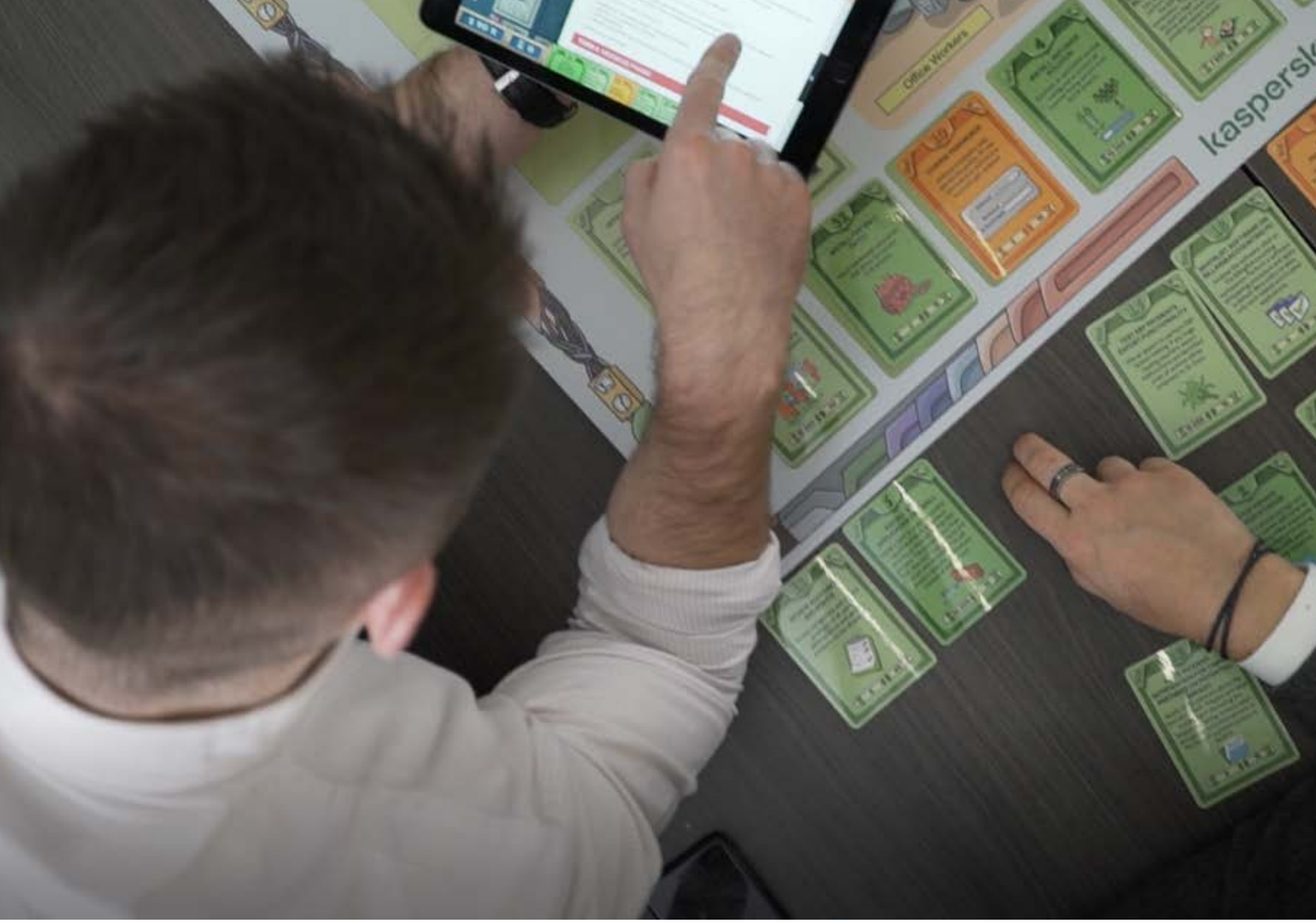
Início
- Eu tenho consciência?
- O que sei e onde estão as lacunas?

Aprendizado
- Microaprendizado
- Aprendizado contínuo
- Adaptabilidade

Reforço
- Entendi corretamente?
- Eu lembro disso?
- Tenho ações condizentes?

Diferentes formatos de treinamento para diferentes níveis organizacionais





Cibersegurança empresarial: www.kaspersky.com.br/enterprise
Kaspersky Security Awareness: kaspersky.com.br/awareness

www.kaspersky.com.br

kaspersky