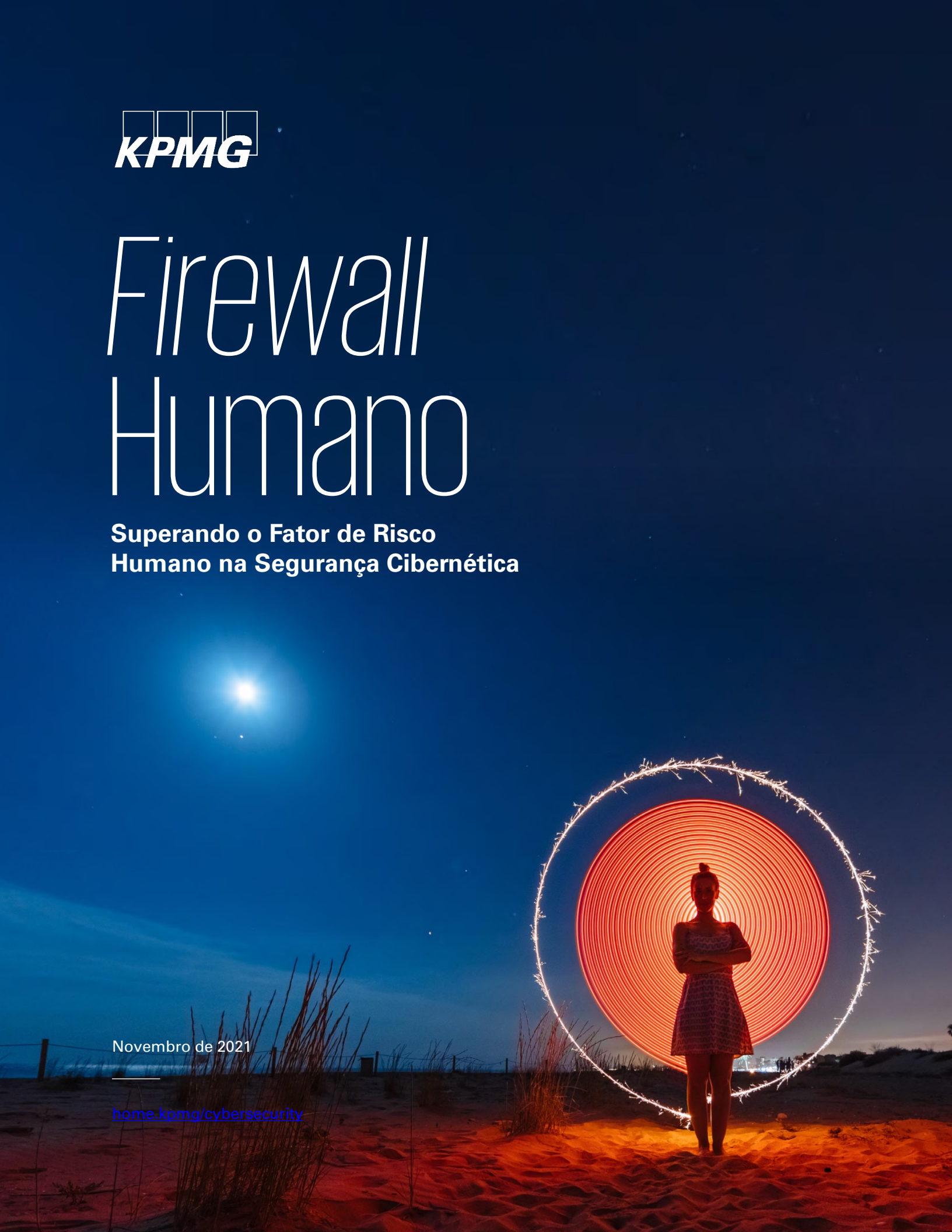
KPMG

Firewall Humano

Superando o Fator de Risco Humano na Segurança Cibernética



Novembro de 2021

home.kpmg/cybersecurity

Prefácio

Um banco envia um e-mail afirmando o seguinte: "Suas contas foram bloqueadas por causa de atividades suspeitas. Por favor, atualize suas informações neste *link*". Um serviço de *streaming* de vídeo informa: "Há algum problema com as informações de faturamento atuais. Responda agora!" Um varejista favorito anuncia: "Boa notícia! Você ganhou um novo celular! Solicite o seu prêmio clicando aqui".

As empresas que gastam milhões de dólares atualmente em soluções de tecnologia de segurança cibernética modernas continuam sendo vítimas de *hackers* que usam esquemas de *phishing* inteligentes como esses.

Embora os *firewalls* e outras tecnologias possam ser a base do programa de segurança cibernética de uma organização, eles não conseguem proteger tudo. Estudos mostram que 88% das violações reportadas incluem algum elemento de erro humano[1]. Para funcionários ocupados, cujas caixas de *e-mail* são inundadas com mensagens diariamente, é fácil ser enganado por uma mensagem maliciosa — e os *hackers* sabem disso. Isso torna fundamental o desenvolvimento e manutenção, pelas empresas, de uma estratégia de segurança cibernética abrangente que considere claramente o fator humano.

Muitas organizações geralmente abordam a segurança cibernética com seus funcionários apenas uma vez por ano — geralmente em um evento envolvendo toda a empresa realizado em um mês específico, como por exemplo o "mês da conscientização sobre segurança cibernética". Embora esses treinamentos sejam importantes, a mensagem de conscientização sobre segurança apresentada muitas vezes desaparece rapidamente e não consegue atingir nenhuma mudança significativa — e necessária — no comportamento dos funcionários.

Na KPMG, os profissionais trabalham com a equipe de gestão do comportamento e comunicações do escritório de segurança da informação da Labcorp. Eles viram provas de que, para proteger uma organização, um programa de segurança cibernética deve ir além das atividades anuais de verificação, pois há uma diferença crucial entre estar em conformidade e estar seguro. O que é necessário é uma abordagem mais integrada e holística que incorpore medidas de segurança cibernética na rotina de trabalho de cada funcionário, de maneira que as melhores práticas comprovadas se tornem um hábito, no lugar de uma escolha.

O resultado ideal é uma mudança cultural, na qual os funcionários reconheçam a importância do tema, adotem uma nova mentalidade e se considerem parte da equipe de segurança cibernética, e sejam inspirados a aprender e a fazer mais.

As páginas a seguir descrevem alguns dos principais elementos de um programa integrado de gestão do comportamento e comunicações de segurança cibernética e as etapas necessárias para a sua criação.

> *A conscientização sobre segurança cibernética não pode ser uma questão pontual. Ela não é uma campanha — é um programa contínuo que deve se tornar parte do tecido e da cultura da organização. Todos, do Conselho e equipe executiva, passando pela equipe de liderança sênior, até os funcionários, precisam estar cientes do programa e embarcar nesta jornada.*
>
> **— Jacqueline LaScala, Labcorp**

> *Camisetas e canecas não são suficientes. Um programa de segurança cibernética moderno projeta uma mensagem consistente e persistente de que a segurança cibernética faz parte da maneira como fazemos negócios. A conscientização sobre a segurança cibernética precisa evoluir de um evento para se tornar parte integrante da empresa.*
>
> **— Fred Rica, KPMG nos EUA**

Fred Rica
Sócio de Cyber Security Services
da KPMG nos EUA

Jacqueline LaScala
Diretora de Gestão do Comportamento e Comunicação
Escritório de Segurança da Informação
Labcorp

[1] HANCOCK, Jeff. *The psychology of human error*. Stanford University, 2021.

Sumário

Uma abordagem persistente para mudar comportamentos seguros

Para serem eficazes no mundo de hoje, em rápida evolução, com as ameaças cibernéticas em constante mudança, as empresas devem buscar desenvolver seus esforços de conscientização da segurança cibernética além da palestra anual envolvendo toda a empresa, ministrada pelo Diretor de Segurança da Informação (CISO) sobre a necessidade de mais vigilância em torno da proteção dos dados. As organizações devem buscar uma abordagem mais integrada e holística, que incorpore práticas de segurança cibernética no dia a dia de trabalho do funcionário.

As estatísticas mostram que o erro humano é o ponto de invasão inicial para muitas violações: abrir um *e-mail*, baixar um arquivo ou clicar em um *link* malicioso[2]. Mesmo com *firewalls* adequados, ferramentas de antivírus e outras soluções baseadas em tecnologia, os *hackers* podem se infiltrar em uma empresa por meio de um erro humano, usando táticas de engenharia social, como *phishing*, por meio das quais as pessoas são enganadas e revelam informações confidenciais.

Esse é um problema sério: o *phishing* é responsável por mais de 80% dos incidentes de segurança reportados e as estatísticas mostram que cerca de US$ 17.700 são perdidos a cada minuto com esses ataques[3].

Um botão como "denunciar *phishing*" é uma solução simples, que pode ajudar as empresas a identificar e prevenir ataques custosos. Há vários fornecedores que oferecem essa solução. O ideal seria que o botão estivesse sempre presente no ambiente de *e-mail* de uma organização, agindo como um quadro de avisos, que mantém a segurança cibernética como prioridade.

Ao tornar essa ação simples, a equipe pode reportar *e-mails* suspeitos imediatamente para investigação, basicamente tornando-os uma espécie de socorristas, agindo como *firewalls* (ou barreiras) humanos.

O botão de denúncia também pode ser usado em conjunto com um sólido programa de simulação de *phishing* para ensinar a equipe como identificar *e-mails* potencialmente maliciosos e tomar medidas para evitar se tornar uma vítima. Incentivar o uso do botão de denúncia pode ajudar a promover um comportamento seguro, tornando a equipe parte da solução da organização para os crimes cibernéticos.

Os programas de conscientização sobre segurança cibernética, projetados para impulsionar a mudança comportamental entre os funcionários, deve ter dois objetivos fundamentais:

- **Mudar a conscientização sobre segurança de ser uma opção para se tornar um hábito.** Em outras palavras, a mensagem tornar a atitude em algo natural. Deixando de ser uma reunião de um dia ou um módulo de treinamento anual, essa abordagem para a segurança cibernética exige um envolvimento pessoal persistente, que se baseia na aprendizagem de adultos e em técnicas de reforço de comportamentos para criar coesão sobre a necessidade de um comportamento seguro. Ela também deve aproveitar o apoio visível dos altos executivos e da liderança sênior, pois eles lideram pelo exemplo, comportando-se com segurança e tornando o tema uma prioridade. Esta é a técnica de modelagem.

- **Envolver a equipe em um nível emocional.** Os programas de conscientização sobre segurança cibernética devem inspirar cada funcionário a ser um cidadão digital melhor e aprimorar as práticas sobre o assunto no trabalho e em casa. Há duas mensagens principais necessárias para conseguir isso:

  - porque a segurança cibernética importa.
  - o que está em jogo para eles, individualmente e pessoalmente.

As pessoas geralmente resistem à mudança. Portanto, tornar a transição mais acessível exige que ela toque o lado emocional. Isso ocorre quando as técnicas de conscientização de segurança utilizadas no trabalho também ajudam a proteger o bem-estar pessoal dos funcionários e de suas famílias em casa, onde não há profissionais de segurança cibernética para oferecer ajuda.

[2] THE HACKER NEWS WEBSITE. *Why Human Error is #1 Cyber Security Threat to Businesses in 2021*. 4 fev. 2021.

[3] CSO WEBSITE. *Top cyber security facts, figures and statistics for 2020*. 9 mar. 2020.

Aproveitando a ciência e a metodologia de aprendizagem de adultos

Para impulsionar uma mudança comportamental que pode ajudar a melhorar a segurança cibernética, a KPMG aprendeu que a aplicação da Teoria Cognitiva Social (TCS, ou *Social Cognitive Theory*, em inglês) é uma tática eficaz.

Desenvolvida pelo professor de psicologia da Universidade de Stanford Albert Bandura, um princípio importante da TCS concentra-se no aprendizado por observação, também conhecido como modelagem. Em outras palavras, a maneira com a qual as pessoas aprendem comportamentos desejáveis (ou indesejáveis) é observando outras pessoas e imitando esses comportamentos aprendidos para maximizar as recompensas[4]. Esse método de aprendizagem é particularmente eficaz se as pessoas admiram, confiam ou respeitam a pessoa que deve ser imitada. Em resumo, as pessoas gostam de ser como seus heróis.

A aplicação desse método de aprendizado para conscientização sobre a segurança cibernética pode começar com o CEO realizando um bate-papo com os funcionários, com ênfase sobre a importância do tema. Ele deve abranger o que acontece durante uma violação, como isso pode afetar seu trabalho, qual seria o pior cenário e as possíveis consequências para a organização. A mensagem também deve descrever como o CEO e os outros líderes estão trabalhando com a equipe de segurança cibernética para evitar violações — e como cada funcionário pode ajudar.

Reforçar a mensagem, disseminando-a por meio da liderança, demonstra que o tema é importante em todos os níveis da empresa. O objetivo é refletir o compromisso dos gestores com práticas de segurança cibernética adequadas e inspirar os funcionários a adotarem e seguirem essa atitude.

[4] VINNEY, Cynthia. *Social Cognitive Theory: How We Learn from the Behaviors of Others.* ThoughtCo, 2019.

Reforçando o comportamento ao aplicar a metodologia de gestão de mudanças

O papel da liderança em apresentar a mensagem de conscientização sobre a segurança cibernética aos funcionários é apenas o início do processo de mudança comportamental. A mensagem deve ser persistentemente reforçada, para que a mudança proposta se torne um hábito.

As firmas da KPMG descobriram que o Modelo Prosci ADKAR de Gestão de Mudanças, criado por Jeffrey Hiatt, é uma ferramenta eficaz nesse esforço. ADKAR significa:

A — ***Awareness:*** **conscientização da necessidade de mudança**

D — ***Desire:*** **desejo de participar e apoiar a mudança**

K — ***Knowledge:*** **conhecimento sobre como mudar**

A — ***Ability:*** **capacidade de implementar as habilidades e os comportamentos necessários**

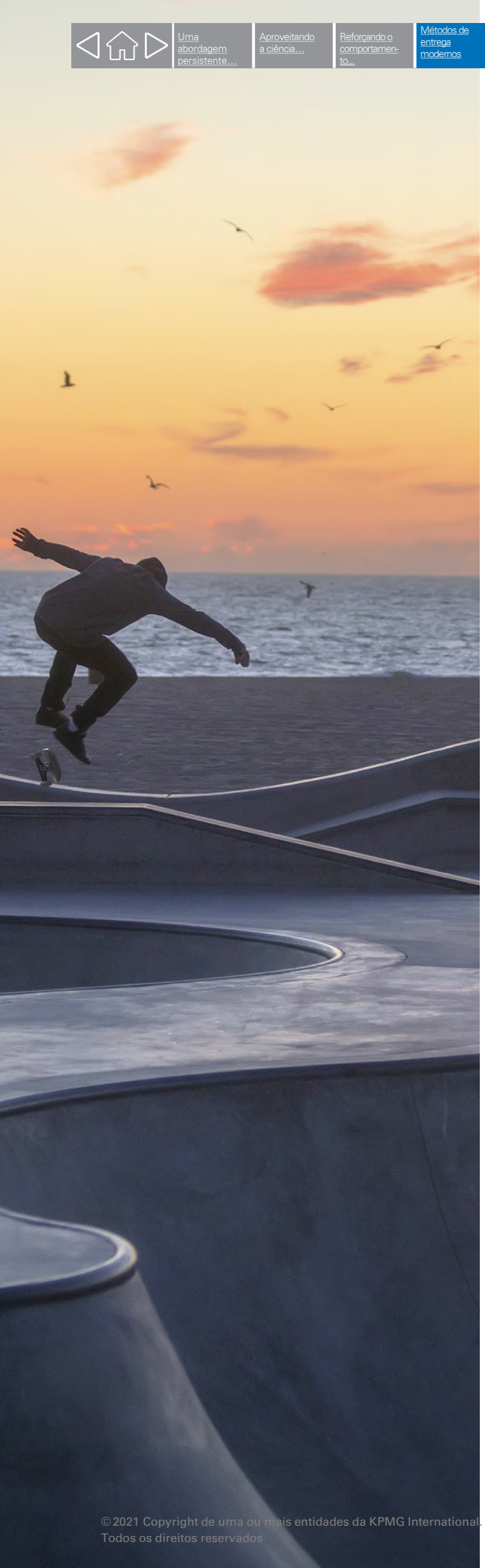
R — ***Reinforcement*****: reforço para sustentar a mudança**[5]

O modelo ADKAR possibilita um programa que reforça continuamente a razão pela qual a segurança cibernética é importante, porque os funcionários devem se manter vigilantes tanto no trabalho quanto em casa, e a função crítica que desempenham em apoiar consistentemente a equipe de segurança cibernética. Por exemplo:

- Para impulsionar a **conscientização,** as telas de *login* do funcionário podem exibir uma mensagem de lembrete, como "denuncie o *phishing*".
- Para impulsionar o **desejo,** uma série de cenários "e se?" podem delinear possíveis ramificações e ameaças ao não se praticar comportamentos seguros.
- Para impulsionar o **conhecimento,** simulações interativas de *phishing* podem ser realizadas periodicamente, incluindo informações educacionais para aqueles que são vítimas.
- Para impulsionar a **capacidade,** um botão pode ser instalado na barra de ferramentas de *e-mail* para reportar sobre mensagens suspeitas à equipe de segurança cibernética.
- Para **reforçar** esse comportamento, os funcionários que informam sobre *e-mails* suspeitos podem receber uma resposta, em agradecimento por estarem vigilantes e agirem. Se o relatório revelar alguma atividade maliciosa, o funcionário pode receber um reconhecimento adicional por sua ajuda, reforçando o bom comportamento, como por exemplo: "Obrigado! Seus esforços e vigilância nos ajudaram a prevenir o crime cibernético por meio da descoberta de um *e-mail* malicioso".

Essas estratégias não apenas fazem com que os funcionários se sintam parte da equipe, como também estimulam sentimentos de responsabilidade e propriedade. Ainda é fundamental criar um ambiente de apoio, em vez de punição, garantindo que, caso um funcionário clique acidentalmente em um *link* perigoso, ele não tenha medo de denunciá-lo imediatamente.

[5] CSO WEBSITE. *Top cybersecurity facts, figures and statistics*. 9 mar. 2020. PROSCI WEBSITE. *Prosci Change Management Methodology*.



Métodos de entrega modernos para tornar o treinamento envolvente

Programas eficazes de gestão do comportamento e comunicação exigem treinamento periódico para manter todos os funcionários, incluindo a liderança, informados sobre as melhores práticas do setor e mudanças nas políticas.

No entanto, as empresas devem considerar ir além dos métodos tradicionais de treinamento, como apresentações de *slides* e vídeos pré-gravados, e utilizar métodos de engajamento modernos que elevam as conversas sobre segurança cibernética de triviais para informativas e inspiradoras. Por exemplo, ao utilizar tecnologias inovadoras, o treinamento pode se tornar interessante, competitivo, envolvente — até mesmo divertido.

A gamificação é uma tecnologia popular, fornecendo cenários que permitem aos funcionários praticar novas habilidades em um ambiente seguro. Ela demonstrou aumentar a motivação do aluno e os níveis de engajamento e pode influenciar a mudança de comportamento[6].

As pessoas aprendem de maneiras diferentes. Há três estilos principais de aprendizagem cognitiva: visual (ver e ler), auditiva (ouvir e falar) e cinestésica (fazer). O treinamento deve atender a cada estilo de aprendizagem — eliminando barreiras de entrada e fornecendo informações no formato preferido do aluno. No mundo digital acelerado de hoje, conteúdos sucintos e de fácil entendimento parecem ser os mais bem-sucedidos.

[6] FORBES WEBSITE. *Games Companies Play: How Your Company Can Implement Gamification To Motivate Employees.* 18 fev. 2020.

Torne a questão pessoal

Os funcionários devem se sentir pessoalmente envolvidos para que a mudança de comportamento seja bem-sucedida e sustentável. Por exemplo, explicar a eles como um determinado comportamento *on-line* pode proteger seus filhos de criminosos virtuais, além de resguardar os dados da empresa ou a si próprios, pode ter um impacto profundo. Os elementos do programa devem conectar os pontos para enfatizar como as habilidades de segurança cibernética no local de trabalho podem ser aplicadas em casa.

O conceito visa incentivar os funcionários a se considerarem o diretores de segurança da informação em suas casas. Para ajudar a transmitir essa mensagem, as empresas podem criar uma plataforma *on-line* informativa, apresentando diversos recursos de segurança cibernética que podem ser compartilhados gratuitamente com familiares e amigos. Os filhos e pais idosos podem participar de eventos virtuais focados na conscientização e educação sobre segurança cibernética.

Com tantos funcionários trabalhando em casa atualmente, adotar uma abordagem pessoal tornou-se fundamental. Além de proteger os ativos corporativos, muitos deles atualmente estão gerenciando a segurança cibernética para famílias multigeracionais, com diversos níveis de sofisticação técnica, incluindo compradores *on-line*, jogadores e crianças que frequentam a escola a distância. Esse aumento no acesso remoto a serviços privados leva inevitavelmente a um maior risco de violação ou ataque.

Os programas de conscientização sobre segurança cibernética devem considerar a evolução constante da força de trabalho e os ambientes específicos nos quais os funcionários trabalham, visando enfrentar todos os riscos de maneira adequada.

Na prática, quando os funcionários sentem que sua empresa está cuidando deles e ajudando a manter suas famílias seguras *on-line*, é mais provável que ajudem a mantê-la protegida contra ameaças cibernéticas.

O poder da marca e da comunicação

Um programa de gestão do comportamento e comunicação deve ter um tema geral e uma marca. O tema — incluindo um nome específico, *slogan* envolvente e logotipo ou cabeçalho — deve ser aplicado a todos os componentes do programa para torná-los parte do tecido e da cultura da organização.

Cada elemento do programa — mensagens na tela de *login*, materiais de treinamento, *sites*, *e-mails* — deve refletir a identidade única da marca, para que todos na organização a reconheçam e entendam sua importância.

Além de uma marca difundida, um programa efetivo deve incluir comunicações contínuas que sejam programadas regularmente e específicas para cada ação. Por exemplo, um programa de comunicação deve incluir quatro elementos-chave:

Boletins mensais educativos, focados em um tema oportuno ou relevante.

Conselhos de posicionamento, por exemplo, para estabelecer o uso adequado de aplicativos de *software* de terceiros ou declarar quando eles não devem ser usados.

Notificações informativas, por exemplo, para anunciar o lançamento de uma nova ferramenta de segurança cibernética.

Alertas acionáveis e integrantes do plano de resposta a incidentes, para envolver os funcionários durante um ataque ou investigação ativa e instruí-los a tomar medidas imediatas, como alterar senhas.

Medindo o sucesso

Monitorar e comunicar o sucesso do programa de gestão do comportamento e comunicação de segurança cibernética é fundamental para o sucesso e a sustentabilidade. Em muitos casos, o progresso é informado para os altos executivos e o Conselho de Administração. Há várias métricas em torno da gestão do comportamento que podem ser consideradas para medir a mudança, incluindo:

- **Número de *e-mails* suspeitos sinalizados por meio do botão de denúncia.**
- **Número de *e-mails* mal-intencionados informados.**
- **Taxa de resiliência de programas de simulação de *phishing*.**
- **Conclusão dos módulos de treinamento.**
- **Participação em eventos e apresentações ao vivo.**
- **Visitas e interações com o *site* de segurança cibernética.**
- **Participação em eventos de competições com a equipe.**
- ***Feedback* por meio de pesquisas com os funcionários.**
- **Envolvimento com a equipe de segurança cibernética, por meio de um endereço de *e-mail* específico do departamento.**

Como começar

As seções anteriores apresentaram um programa modelo de gestão do comportamento e comunicação de segurança cibernética. No entanto, uma organização deve organizar os detalhes do seu programa para que ele se adeque à sua cultura única e aos seus negócios.

Estabeleça uma meta: os responsáveis pelo programa — aqueles que iniciam o projeto, desenvolvem, implementam e são os responsáveis pelo seu sucesso — devem começar concluindo uma análise de *gaps* para avaliar o entendimento dos funcionários sobre segurança cibernética e estabelecer uma referência para a organização. Eles precisarão se envolver com a liderança sênior da empresa para ajudar a transmitir a importância de um programa de gestão do comportamento. Além disso, precisarão de liberdade para aprender sobre a estrutura da empresa, a hierarquia de liderança, casos de uso específicos e cultura.

Esses *insights* ajudarão a determinar os meios mais eficazes de comunicação, a frequência das mensagens, o tom e a abordagem.

Planeje: construir e executar um programa abrangente exige colaboração. Para começar, os responsáveis pelo programa devem ser profissionais com experiência em marketing, vendas e comunicação. Eles devem ter habilidades de redação, com a capacidade de traduzir informações técnicas em linguagem simples. Devem ainda entender a ciência da TCS e a metodologia de aprendizagem de adultos e as práticas de gestão de mudanças. A análise de *gaps*, a pesquisa inicial e as atividades de *benchmarking* devem ser utilizadas para formular um plano estratégico abrangente que capture as metas, objetivos, táticas e cronogramas do programa.

Construa: além dos responsáveis pelo programa, grupos com várias habilidades e conhecimentos serão necessários para desenvolver e executar o programa em sua totalidade.

Patrocinadores do programa: englobam os líderes seniores que são conhecidos e respeitados pela equipe. Eles devem ser apoiadores entusiasmados do programa e estarem dispostos a ressaltar sobre a importância do programa e o papel que a equipe desempenha em apoiá-lo. Ainda devem articular claramente o que a equipe tem a ganhar, tanto profissionalmente quanto pessoalmente.

Marketing e comunicação corporativa: essas equipes podem ajudar a desenvolver a marca do programa, a identidade visual e os seus elementos iniciais que serão visíveis para a equipe. Além disso, os responsáveis pelo programa devem estabelecer, de forma proativa, procedimentos operacionais padronizados com a equipe de comunicação corporativa para a resposta a incidentes e comunicações de crises.

Profissionais de segurança cibernética: esses especialistas ajudarão os responsáveis pelo programa a desenvolver conteúdos que serão disponibilizados à equipe por meio de vários métodos de entrega (por exemplo, comunicações de rotina e específicas, conteúdo do *site*, módulos de treinamento e outros elementos passivos e ativos).

Profissionais de tecnologia da informação (TI): a equipe de TI pode ser necessária para implementar elementos do programa baseados em tecnologia, como o botão de denúncia de *phishing*.

Indo além da conscientização cibernética

Conforme os ataques de *phishing* e outros similares se tornam mais sofisticados, os riscos à segurança cibernética aumentam. Ao investir no elemento humano para proteção contra as invasões, as organizações podem fortalecer equipes que não apenas são mais experientes em segurança cibernética, mas também representam uma extensão crucial dos times de segurança cibernética por meio do seu compromisso em manter a organização segura.

Embora os *firewalls* e outras tecnologias de segurança cibernética sejam indispensáveis para aumentar a proteção no ambiente digital em constante expansão atual, eles não abordam o elemento humano.

Uma perspectiva holística para proteger uma organização exige investimento nas pessoas — o *firewall* humano — para garantir que os funcionários entendam os princípios da segurança cibernética e cumpram seu papel no apoio aos esforços de proteção, tornando os comportamentos seguros uma parte integrante da sua vida cotidiana.

Ao ir além das normas padronizadas, e aplicando a ciência da TCS e a metodologia de aprendizagem de adultos, as empresas podem inovar a conscientização tradicional sobre segurança, desenvolvendo um programa de gestão do comportamento e comunicação mais eficaz e contemporâneo — e ajudando os funcionários a se tornarem cidadãos digitais melhores no trabalho e em casa.

Fale com o nosso time

Fred Rica
Sócio-líder de Serviços de Cyber Security da KPMG nos EUA
E: frica@kpmg.com

Akhilesh Tuteja
Sócio-líder global de Cyber Security da KPMG na Índia
E: atuteja@kpmg.com

Dani Michaux
Sócia-líder de Cyber Security da região EMA (Europa, Oriente Médio e África) da KPMG na Irlanda
E: dani.michaux@kpmg.ie

Jacqueline LaScala
Diretora de gestão do comportamento comunicação do escritório de segurança da informação da Labcorp
E: lascalj@labcorp.com

Matt O'Keefe
Sócio-líder de Cyber Security da região ASPAC (Ásia-Pacífico) da KPMG na Austrália
E: mokeefe@kpmg.com.au

Prasad Jayaraman
Sócio-líder de Cyber Security das Américas da KPMG nos EUA
E: prasadjayaraman@kpmg.com

Klaus Kiessling
Sócio de Cyber Security e Privacidade da KPMG no Brasil
kkiessling@kpmg.com.br

Ser inovador transforma negócios.

#KPMGTransforma

Baixe o nosso APP

kpmg.com.br /kpmgbrasil

Projeto da Evalueserve.
Nome da publicação: Firewalls humanos