knowbe4

Mês da conscientização em segurança cibernética de 2026

Dossiê estratégico do kit de recursos

SEMANA 1

SEMANA 2

SEMANA 3

SEMANA 4

RESUMO DA MISSÃO:

Mês da conscientização em segurança cibernética de 2026

Sua missão, caso decida aceitá-la: colocar à disposição da sua equipe as informações necessárias para que ela se antecipe às ameaças globais.

Aproveite ao máximo o conjunto de ferramentas, os equipamentos e os especialistas em segurança cibernética disponibilizados este ano, como parte de uma equipe de elite conhecida como “Divisão de risco da força de trabalho” (em inglês, Workforce Risk Division; WRD). Como integrante da WRD, você ajudará seus usuários a participar de quatro missões de uma semana cada, com foco em uma ameaça cibernética específica.

Transformar sua força de trabalho em uma força de defesa de primeira linha ficou muito mais fácil. Já fizemos o trabalho pesado com uma coleção gratuita de recursos.

Esta campanha pronta para uso, criada para o Mês da conscientização em segurança cibernética, transforma seus funcionários em “agentes secretos” na luta contra o crime cibernético. Além dos módulos de treinamento gratuitos e dos pôsteres e documentos de apoio, incluímos quatro cartões de personagens “especialistas” que representam as habilidades necessárias para lidar com o panorama atual de ameaças. Você também terá acesso a quatro cenários prontos para exercícios de simulação, concebidos para serem realizados presencial ou virtualmente, a fim de ajudar sua equipe a desenvolver resiliência diante de ameaças futuras.

Seu equipamento

Nossa página da web do kit oferece:

FOR YOUR EYES ONLY

Somente para você

- **Webinar:** Como proteger a adoção da IA na sua organização
- **Whitepaper:** A segurança da força de trabalho híbrida: protegendo pessoas e agentes de IA na nova era
- **Quatro documentos de cenários para exercícios de simulação** baseados em tópicos
- **Planejador semanal de conscientização em segurança baseado na web**, que organiza todos os recursos abaixo destinados aos usuários em temas planejados semanalmente para uso ao longo do mês de outubro, disponíveis aqui:

PLANEJADOR SEMANAL

Para seus agentes

Acesse todos os cursos e conteúdos pelos links fornecidos até **31 de outubro de 2026.**

- **Seis módulos interativos de treinamento ou de vídeo gratuitos**
  - Ataque de smishing (disponível em 35 idiomas)
  - Um ataque de engenharia social com deepfake (disponível em 35 idiomas)
  - Como proteger a propriedade intelectual (disponível em 12 idiomas)
  - Senhas fortes, contas seguras (disponível em 35 idiomas)
  - Audiocast sobre hábitos à prova de hackers (disponível em 12 idiomas)
  - Jogo “Em busca da privacidade” (disponível em 13 idiomas)
- **Quatro cartões/pôsteres com personagens da Divisão de risco da força de trabalho**
- **Quatro pôsteres e recursos de comunicação digital, perfeitos para ajudar a relembrar conceitos-chave**

Divisão de risco da força de trabalho: conceitos básicos

Para os agentes da WRD, a luta constante contra os agentes mal-intencionados já é difícil o suficiente. Por isso, tentamos facilitar ao máximo o recrutamento de novos agentes. Para começar, cada conteúdo está alinhado a um tema geral a ser abordado em cada uma das quatro semanas completas de outubro. A cada semana, considere compartilhar um ou mais destes tipos de conteúdo:

- **Módulos de treinamento interativos ou em vídeo**
- **Pôster/documento informativo**
- **Cartão do personagem “Especialista da WRD”**
- **Documento do exercício de simulação**

Mais adiante neste dossiê, vamos explicar cada tema semanal em mais detalhes, mas aqui está o resumo:

- **Semana 1:** Phishing e engenharia social
- **Semana 2:** Segurança da IA e deepfakes
- **Semana 3:** Segurança de dados e senhas
- **Semana 4:** Denúncia de incidentes

Para ajudar você a visualizar como tudo se encaixa, confira nosso Planejador de conscientização em segurança, disponível aqui:

PLANEJADOR SEMANAL

Use o planejador como ponto de acesso único aos recursos da WRD disponibilizados para você.

Perfis dos especialistas da WRD

As missões já estão claras. Chegou a hora de conhecer os especialistas. Ao longo do Mês da conscientização em segurança cibernética, informe seus usuários sobre os quatro conjuntos de habilidades necessárias para as operações cibernéticas por meio desses quatro perfis de especialistas. Cada um tem uma função para ajudar a cumprir as missões do mês. O resto ficará por conta dos seus usuários.

PHISHING/ENGENHARIA SOCIAL

GHOST

LEMA:
CONFIE,
MAS VERIFIQUE...
E DEPOIS
VERIFIQUE DE NOVO

FUNÇÃO: ESPECIALISTA EM CONTRAESPIONAGEM

ESPECIALIDADE: IDENTIFICAR O USO DE PRETEXTO E DE TÉCNICAS SOFISTICADAS DE ENGENHARIA SOCIAL

CONSELHO: SE UM E-MAIL CRIAR UMA FALSA SENSAÇÃO DE URGÊNCIA, PROVAVELMENTE É UMA ARMADILHA

PÁGINA

AMEAÇAS DE IA/SEGURANÇA

GADGET

LEMA:
MANTENHA SUAS
FERRAMENTAS AFIADAS
E SUA MENTE
MAIS AFIADA AINDA

FUNÇÃO: ESPECIALISTA TÉCNICO

ESPECIALIDADE: SEGURANÇA DA IA E DETECÇÃO DE DEEPFAKES

CONSELHO: USE UMA PALAVRA-CÓDIGO COM A FAMÍLIA OU OS COLEGAS PARA VERIFICAR A IDENTIDADE DURANTE LIGAÇÕES "URGENTES" SUSPEITAS

PÁGINA

SEGURANÇA DE DADOS E SENHAS

LOCK N KEY

LEMA:

[SUPRIMIDO]

FUNÇÃO: CRIPTÓGRAFO

ESPECIALIDADE: CHAVES DE ACESSO, AUTENTICAÇÃO MULTIFATOR (MFA) E CRIPTOGRAFIA

CONSELHO: SUA SENHA NÃO DEVE SER UMA PALAVRA; DEVE SER UMA HISTÓRIA QUE SÓ VOCÊ CONHECE

PÁGINA

DENÚNCIA DE INCIDENTES

SCOUT

LEMA:

SE PARECE UMA
VIOLAÇÃO DE DADOS
E SOA COMO UMA
VIOLAÇÃO DE DADOS,
É MELHOR DENUNCIAR

FUNÇÃO: AGENTE DE CAMPO

ESPECIALIDADE: DENÚNCIA DE INCIDENTES E SEGURANÇA FÍSICA

CONSELHO: SE VOCÊ VIR ALGO, DIGA ALGO

PÁGINA

Promovendo a participação de todas as pessoas

Disponibilizamos quatro planos de aula completos para ajudar a orientar sua equipe em exercícios de simulação que reproduzem crises de segurança.

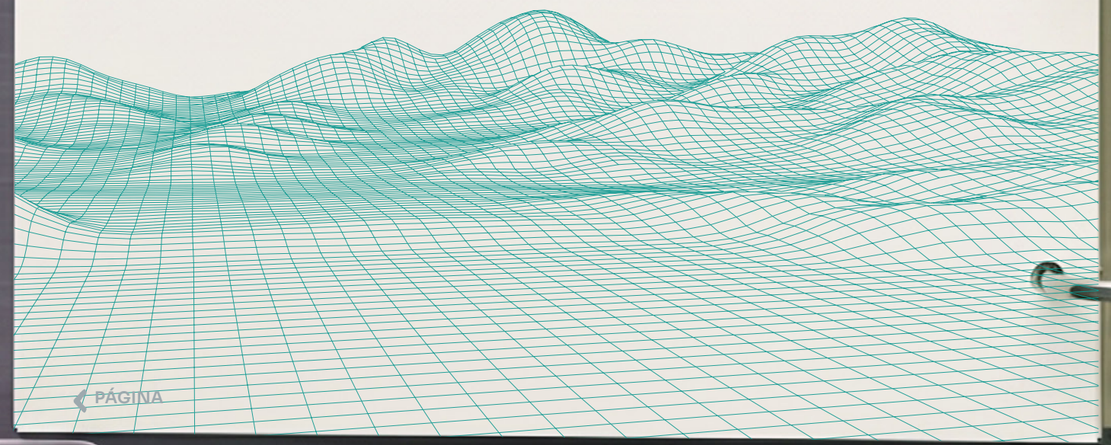
O objetivo é atender aos usuários de qualquer nível técnico, com foco na identificação de funções, na tomada de decisões e na coordenação da equipe. As atividades incluem a priorização de listas de verificação de respostas e a realização de simulações realistas de cenários contendo situações complicadoras. Sua equipe aprenderá sobre procedimentos estabelecidos de resposta a incidentes, comunicação entre equipes e adaptabilidade durante incidentes de segurança por meio de exercícios práticos e sessões estruturadas de análise dos resultados.

Aqui estão algumas sugestões práticas para aproveitar ao máximo esses recursos:

1. Missão pronta do gerente:
Compartilhe esses recursos com os chefes de departamento por meio de uma nota intitulada *Informe do diretor*. Sugira que eles escolham um tema que seja mais relevante para o departamento deles e realizem uma versão de 30 minutos de *Respostas rápidas* durante uma reunião semanal de sincronização que já ocorre.

2. Simulação de ataque que visa a força de trabalho remota:
Para uma força de trabalho predominantemente remota, utilize as seções dos *Cartões de cenário* dos recursos de simulação como perguntas de enquete durante as reuniões gerais por videoconferência realizadas em outubro, no formato de quizzes rápidos. Discuta os resultados da semana anterior na reunião da próxima semana para avaliar o desempenho da sua equipe.

3. Mensagem instantânea *surpresa*:
Escolha um dia da semana e publique um *Cartão de cenário* no seu canal de segurança da informação ou de conscientização em segurança no aplicativo de mensagens interno de sua preferência. O primeiro agente a denunciar o incidente corretamente nessa discussão, explicando por que ele é um problema e o que poderia ser feito para resolvê-lo, poderá ganhar um prêmio temático ou outro incentivo, conforme permitido pela sua organização.



Dicas dos gênios da WRD: Estratégias de campanha

A equipe de cientistas e pesquisadores que atua nos bastidores da WRD talvez não seja de aparecer muito, mas seus integrantes entendem muito do assunto. Os idealizadores de todos esses recursos constataram que as seguintes estratégias centrais de campanha têm se mostrado eficazes para organizações de todos os portes:

Pense como um coordenador, execute como um agente de campo
Seu objetivo é mudar comportamentos de risco, e não apenas transmitir informações. Pense em como as agências de inteligência globais sustentam uma identidade secreta: elas utilizam diversos pontos de contato para reforçar uma narrativa consistente. É por isso que disponibilizamos recursos suficientes para adotar uma estratégia multicanal de conscientização. Ao implantar diferentes mídias (vídeos, jogos e informes) ao longo da semana, você condiciona os reflexos de segurança dos funcionários por meio de um engajamento regular. É assim que você transforma funcionários passivos em uma última linha de defesa sólida.

Consiga ajuda de todos os setores
Nenhuma operação de inteligência tem sucesso no vácuo. Para construir uma cultura de segurança verdadeiramente resiliente, é preciso recrutar aliados fora do perímetro da TI. Aproveite o mês de outubro para mobilizar os “talentos adormecidos” nos departamentos de RH, Jurídico e Marketing. Mostre a eles que desempenham um papel de grande importância na WRD. Quando as orientações sobre segurança vêm de um colega de confiança da própria área, e não apenas do pessoal de TI, é muito mais provável que sejam assimiladas e incorporadas à rotina.

Priorize informações essenciais para a missão
Não atrapalhe o trabalho dos seus agentes fornecendo informações “essenciais para a missão” em excesso. Se você despejar muitos dados de uma só vez, eles podem ficar sobrecarregados e começar a dar cliques aleatórios nos informes apenas para esvaziar a fila. Em vez disso, identifique as duas ou três vulnerabilidades mais graves da sua organização e concentre seus esforços nelas. Nossos temas semanais da missão, como Phishing, Segurança da IA, Senhas e Relatórios, foram desenvolvidos para formar um agente com um perfil completo. Concentre-se na missão atual, alcance o objetivo e guarde as informações detalhadas para operações futuras.

Embora os recursos deste kit não devam, de forma alguma, substituir um programa abrangente de treinamento de conscientização em segurança, eles foram concebidos para serem facilmente compartilhados e implementados para terem um impacto profundo na sua equipe.

Detalhamento da missão

Abaixo, você encontrará o conteúdo organizado por semana, com sugestões de tópicos a serem apresentados e o texto associado para e-mails.

Com certeza, a essa altura você já deve ter algumas ideias ou estratégias em mente sobre como pretende trabalhar neste mês. Independentemente de como você estruturar sua campanha, sugerimos o envio de um e-mail introdutório no dia 1º de outubro ou até mesmo na última semana de setembro.

Aqui está um exemplo de texto:

Linha de assunto sugerida:
[INÍCIO DA MISSÃO] **Sua integração à Divisão de risco da força de trabalho**

MÊS DE CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA DE 2026 | INÍCIO DA MISSÃO

knowbe4

Divisão de risco da força de trabalho: Informe inicial

Bom dia, agentes!

No mundo da espionagem cibernética global, onde os riscos são altíssimos, você é o alvo principal e nossa linha de defesa mais forte.

Somente os agentes mais atentos e bem treinados conseguem enfrentar a onda de deepfakes gerados por IA, as sofisticadas técnicas de engenharia social e a guerra invisível travada nos bastidores das nossas redes.

O campo de batalha é perigoso, e você não deve enfrentá-lo sozinho. Felizmente, autorizamos uma série de sessões de inteligência para garantir que vocês estejam preparados para a missão que temos pela frente.

A MISSÃO:

Em outubro, vamos celebrar o Mês da conscientização em segurança cibernética e faremos a integração de todos os membros da nossa equipe à Divisão de risco da força de trabalho (WRD). Ao longo do mês, vocês receberão orientações de quatro especialistas, cada um representando um pilar fundamental da nossa cultura de segurança.

Prepare-se para uma operação de quatro semanas, na qual cada missão representa um novo nível de inteligência a ser dominado.

Não baixe a guarda neste mês e participe de **[insira atividades ou temas planejados aqui. Use as ideias contidas neste Guia do usuário como fonte de inspiração!]**

Se tiver alguma dúvida, entre em contato com **[insira a pessoa de contato]**.

Seu primeiro informe será enviado na segunda-feira. Fique a postos, agente, e boa sorte.

SEMANA 1

Phishing e engenharia social

Os espiões mais sofisticados não invadem os locais; eles conseguem acesso com sua habilidade de persuasão. Esta semana, o foco está nos sinais de alerta sutis da engenharia social que os filtros técnicos podem não detectar e em como identificá-los.

Aqui está um resumo dos recursos desta semana:

Módulo de treinamento: Ataque de smishing

Este módulo de sete minutos apresenta os perigos do smishing, ou phishing por mensagem de texto, e mostra como seus usuários podem impedir que se tornem mais uma vítima desse tipo de ataque cibernético.

Seus funcionários aprenderão:

- **Como os criminosos cibernéticos podem usar a engenharia social em mensagens de texto**
- **Como o smishing normalmente se apresenta**

ACESSAR RECURSO

Exercício de simulação: Como identificar ataques de phishing e whaling

Este exercício de simulação capacita os funcionários a identificar e responder a ataques sofisticados de phishing e whaling. Os participantes analisam um e-mail de simulação de fraude do CEO para distinguir entre indicadores falsos de confiança gerados por IA e sinais de alerta comportamentais reais. Concebido para que funcionários de todos os níveis pratiquem a aplicação do pensamento crítico e dos procedimentos oficiais da sua organização.

Dois recursos para download

- **Não morda a isca: Denuncie todas as tentativas de phishing:** lembrete em formato de pôster sobre os sinais comuns de um e-mail de phishing e o que fazer caso suspeite de algo
- **Sua função na segurança de internet:** recurso no estilo de infográfico que lembra aos usuários as táticas mais comuns de crimes cibernéticos e como evitá-las

RECURSOS DA SEMANA 1

Compartilhamento de conteúdo

Aqui está um exemplo de texto de e-mail elaborado pelo especialista Ghost para ser usado ao compartilhar o módulo de treinamento desta semana:

Linha de assunto sugerida:
[SEMANA 1 DA MISSÃO] **Como interceptar a ameaça de "smishing"**

knowbe4

Como interceptar a ameaça de "smishing"

MÊS DE CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA DE 2026 | SEMANA 1 DA MISSÃO

Bom dia, agentes!

Especialista com o codinome **Ghost** se apresentando.

Nossos dispositivos móveis são, no momento, os principais alvos de interferências externas. O inimigo não está mais só na sua caixa de entrada, mas também no seu bolso.

A MISSÃO:
Conclua o informe do "Ataque de smishing". Este módulo de treinamento apresenta os riscos do smishing, ou seja, o phishing por mensagem de texto, e mostra como você pode impedir de se tornar mais uma vítima desse tipo de ataque cibernético.

Você aprenderá:

- **Como os criminosos cibernéticos podem usar a engenharia social em mensagens de texto**
- **Como o smishing normalmente se apresenta**

Acesse aqui (https://training.knowbe4.com/modstore/view/af44ce18-ea58-47c9-a352-fb1f277ec903)

Se tiver alguma dúvida, envie um comunicado para **[insira a pessoa de contato]**.

Tome cuidado lá fora. Não perca os próximos informes deste mês.

Ghost, desligando.

SEMANA 2

IA e deepfakes

Mergulhe nos meandros sombrios da IA para ensinar aos usuários como agentes mal-intencionados usam ferramentas generativas para criar clones e roteiros perfeitos. Seus agentes devem recorrer ao seu recurso mais valioso, suas habilidades de pensamento crítico, para descobrir o que é real.

Aqui está um resumo dos recursos desta semana:

Módulo de vídeo: Um ataque de engenharia social com deepfake

Este módulo de vídeo de seis minutos apresenta membros do elenco da popular série de conscientização em segurança "The Inside Man", demonstrando como os criminosos cibernéticos estão usando a clonagem de voz por IA e a tecnologia de deepfake de vídeo para se passar por pessoas que você talvez conheça.

Seus funcionários aprenderão:

- **Como os criminosos cibernéticos podem usar deepfakes e engenharia social para comprometer as defesas de uma organização por meio de solicitações simples**
- **Sinais de alerta a serem observados para proteger você e sua organização contra ataques sofisticados de deepfake**

ACESSAR RECURSO

Módulo de treinamento: Como proteger a propriedade intelectual

Este módulo de treinamento de 10 minutos, disponível na biblioteca do KnowBe4 Compliance Plus, explica a importância da propriedade intelectual, ou PI.

Seus funcionários aprenderão:

- **O que é PI e por que ela é tão valiosa**
- **Como proteger a PI contra roubo, violação e divulgação acidental, inclusive por meio do uso de inteligência artificial**

ACESSAR RECURSO

Exercício de simulação: O desafio do prompt de IA

Este exercício de simulação prepara os funcionários para identificar os riscos decorrentes do uso de prompts inseguros no local de trabalho. Os participantes analisarão os prompts de IA para identificar quais são seguros e quais colocam os dados privados em risco. Concebido para que funcionários de todos os níveis pratiquem o pensamento crítico e sigam as políticas da sua organização.

Dois recursos para download/sinalização digital

- **Verdadeiro ou falso? Como identificar deepfakes:** lembrete em formato de pôster sobre o uso de dicas contextuais e do pensamento crítico para ajudar a identificar deepfakes que circulam pela internet
- **O phishing mais inteligente: Como a IA está transformando os golpes online:** recurso no estilo de infográfico que explica como a IA está tornando os golpes de phishing mais difíceis de detectar

RECURSOS DA SEMANA 2

Compartilhamento de conteúdo

Aqui está um exemplo de texto de e-mail elaborado pelo especialista Gadget para ser usado ao compartilhar nosso recurso em destaque sugerido para esta semana: o módulo “Um ataque de engenharia social com deepfake”.

Linha de assunto sugerida:
[SEMANA 2 DA MISSÃO] **Como desmascarar o deepfake**

MÊS DE CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA DE 2026 | SEMANA 2 DA MISSÃO

Bom dia, agentes!

Especialista **Gadget** se apresentando.

É frustrante ver os avanços da IA sendo usados para o mal. Os agentes mal-intencionados estão utilizando as mais recentes tecnologias de clonagem de voz com IA e deepfakes de vídeo para se passar por líderes e colegas. Qualquer pessoa que eles consigam imitar e que lhes proporcione o acesso e os dados necessários para cumprir suas próprias missões nefastas é um alvo legítimo.

A MISSÃO:

Conclua o informe em vídeo *Um ataque de engenharia social com deepfake*. Este módulo apresenta informações essenciais fornecidas pelos especialistas do “The Inside Man”, demonstrando como os criminosos cibernéticos estão usando a clonagem de voz por IA e a tecnologia de deepfake de vídeo para se passar por pessoas que você talvez conheça.

Você aprenderá:

- **Como os criminosos cibernéticos podem usar deepfakes e engenharia social para comprometer as defesas de uma organização por meio de solicitações simples**
- **Sinais de alerta a serem observados para proteger você e sua organização contra ataques sofisticados de deepfake**

Acesse aqui (https://training.knowbe4.com/modstore/view/0451be1f-0531-4724-a664-21f109be6308)

Se tiver alguma dúvida, entre em contato com **[insira a pessoa de contato]**.

Mantenha suas ferramentas afiadas e sua mente mais afiada ainda. Não perca os próximos informes deste mês.

Gadget, desligando.

SEMANA 3

Segurança de dados e senhas

Os dados confidenciais são como moeda corrente no mundo moderno; e os agentes mal-intencionados estão dispostos a fazer qualquer coisa para obtê-los. É importante garantir que seus agentes estejam cientes do valor dos dados que protegem e do que está em jogo caso um vazamento ocorra. Esta semana, vamos nos concentrar no uso de gerenciadores de senhas e na autenticação multifator (MFA) para garantir que, mesmo que um agente seja comprometido, os dados da agência permaneçam criptografados.

Aqui está um resumo dos recursos desta semana:

Módulo de treinamento para dispositivos móveis: Senhas fortes, contas seguras

Este módulo de cinco minutos, desenvolvido para uso em dispositivos móveis, explica a importância de senhas e frases secretas seguras na vida profissional e pessoal dos usuários.

Seus funcionários aprenderão:

- **Dicas sobre como criar senhas fortes e seguras e usar frases secretas com eficácia**
- **Como evitar erros comuns de segurança que deixam as contas vulneráveis**
- **Melhores práticas para proteger senhas e frases secretas**

ACESSAR RECURSO

Exercício de simulação: O jogo de adivinhar senhas

Este exercício de simulação permite que os funcionários assumam o papel de um hacker para tentar descobrir senhas fracas. Os participantes analisarão publicações nas redes sociais e tentarão adivinhar as senhas de seus autores apenas com base nas informações compartilhadas online. Este exercício demonstra como a combinação entre compartilhar informações em excesso na internet e práticas inadequadas de senhas facilita que agentes mal-intencionados invadam contas por meio de ataques de força bruta.

Dois recursos para download/sinalização digital

- **Senhas fortes garantem sua tranquilidade online:** recurso no estilo de pôster que destaca a importância das senhas fortes
- **Dados sigilosos: mantenha-os em segredo e protegidos:** documento em formato de infográfico que explica os princípios básicos para manter informações sigilosas seguras e por que isso é importante

RECURSOS DA SEMANA 3

Compartilhamento de conteúdo

Aqui está um exemplo de texto de e-mail *do* especialista Lock and Key para usar ao compartilhar o módulo de treinamento desta semana:

Linha de assunto sugerida:
[SEMANA 3 DA MISSÃO] **Como proteger o cofre**

Bom dia, agentes!

Especialista **Lock and Key** se apresentando a partir de... bem, essa é uma informação bem guardada.

A segurança de um segredo depende da força do seu cadeado. Voltaremos aos fundamentos básicos com um protocolo adequado de senhas. Apesar de parecerem informações muito básicas, elas não são menos importantes. Mesmo o cofre mais moderno será inútil se ficar aberto.

A MISSÃO:

Conclua o módulo de treinamento para dispositivos móveis "Senhas fortes, contas seguras".

Descubra por que as frases secretas são superiores às senhas e como eliminar os erros comuns que deixam nossa segurança vulnerável.

Você aprenderá:

- **Dicas sobre como criar senhas fortes e seguras e usar frases secretas com eficácia**
- **Como evitar erros comuns de segurança que deixam as contas vulneráveis**
- **Melhores práticas para proteger senhas e frases secretas**

Acesse aqui (https://training.knowbe4.com/modstore/view/c0ee0966-ff3a-4fc2-93bb-2a632811140b)

Se tiver alguma dúvida, envie uma mensagem criptografada para **[insira a pessoa de contato]**.

Como diz meu mago favorito: Guarde-a em segredo. Guarde-a em segurança.

LK

SEMANA 4

Denúncia de incidentes

Na Divisão de risco da força de trabalho, estar atento ao que acontece ao redor é uma parte essencial das operações. Nenhum agente consegue cumprir uma missão sozinho. Por isso, é fundamental que seus agentes saibam da importância de informar a equipe quando algo não parecer estar certo. Esta semana, vamos garantir que todos os agentes saibam exatamente como pedir reforços quando virem algo suspeito.

Aqui está um resumo dos recursos desta semana:

Audiocast sobre hábitos à prova de hackers: denúncias

Este audiocast de 15 minutos, dividido em módulos de 5 e 10 minutos, aborda a importância de denunciar ameaças à segurança.

Seus funcionários aprenderão:

- **Possíveis obstáculos à denúncia que podem surgir diante de uma ameaça à segurança**
- **Por que a denúncia é uma etapa tão crucial no combate ao crime cibernético**
- **Um processo de tomada de decisão que eles possam seguir para analisar situações e escolher ações seguras**

ACESSAR PARTE 1

ACESSAR PARTE 2

Jogo: Em busca da privacidade

Este jogo interativo de 15 minutos vai ajudar seus usuários a entender melhor as leis internacionais de proteção de dados por meio de uma aventura desafiadora ao redor do mundo, que vai aprimorar seus conhecimentos sobre conformidade.

Seus funcionários aprenderão:

- **A importância das regulamentações sobre privacidade de dados**
- **Diferentes abordagens regionais e internacionais em relação à privacidade de dados**

ACESSAR RECURSO

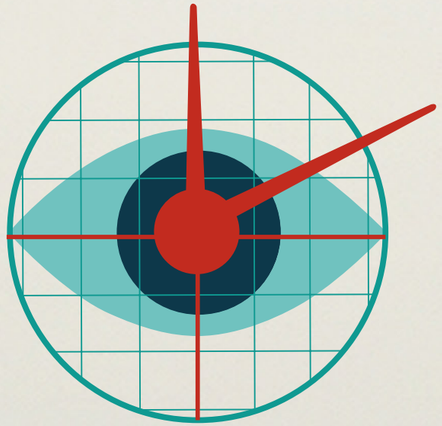
Exercício de simulação: Resposta a incidentes

Este plano de aula abrangente sobre resposta a incidentes orienta os funcionários da empresa por meio de exercícios de simulação de crises de segurança. O exercício é voltado a participantes de todos os níveis técnicos, com foco na identificação de funções, na tomada de decisões e na coordenação de equipes. As atividades incluem a priorização de listas de verificação de respostas e a realização de simulações realistas de cenários contendo situações complicadoras. Os participantes aprenderão sobre procedimentos estabelecidos de resposta a incidentes, comunicação entre equipes e adaptabilidade durante incidentes de segurança por meio de exercícios práticos e sessões estruturadas de análise dos resultados.

Dois recursos para download/sinalização digital

- **Uma única denúncia, proteção compartilhada:** recurso no estilo de pôster que destaca a importância de denunciar imediatamente e-mails suspeitos para proteger informações pessoais, colegas e dados de clientes
- **Phishing, segurança física e violações de dados... Nossa!:** recurso no estilo de infográfico que lembra aos usuários por que denunciar imediatamente problemas de segurança impede que pequenos problemas se transformem em incidentes graves

RECURSOS DA SEMANA 4



Compartilhamento de conteúdo

Aqui está um exemplo de texto de e-mail elaborado pelo especialista Scout para ser usado ao compartilhar o audiocast e o módulo de jogo desta semana:

Linha de assunto sugerida:
[SEMANA 4 DA MISSÃO] **Como manter a equipe informada**

knowbe4

Como manter a equipe informada

MÊS DE CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA DE 2026 | SEMANA 4 DA MISSÃO

Bom dia, agentes!

Scout se apresentando com um relatório final da situação e um informe.

Nossas missões só têm sucesso quando a WRD sabe o que está acontecendo em campo e no mundo real.

Denunciar incidentes não é dedurar ninguém. É compartilhar informações essenciais para que nossas equipes possam proteger o perímetro e manter os agentes mal-intencionados afastados.

Seu quarto e último informe é composto por duas partes:

A MISSÃO:

Para ouvir: Hábitos à prova de hackers: denúncias. Domine um processo crucial de tomada de decisão em segurança da informação para analisar ameaças em tempo real

Acesse a parte 1 (https://training.knowbe4.com/modstore/view/ad7bb017-916b-442f-b1e7-4f96bf6b202f)

Jogue: Em busca da privacidade. Viaje pelo mundo (virtualmente) e teste seus conhecimentos sobre as práticas globais de privacidade de dados para saber mais sobre o que está em jogo quando se trata de possíveis incidentes de violação

Acesse a parte 2 (https://training.knowbe4.com/modstore/view/a5ec90a8-956b-4675-8c63-c336812752e7)

Se tiver alguma dúvida, entre em contato com **[insira a pessoa de contato]**.

Scout desligando em nome de toda a equipe da WRD.

INFORME DA MISSÃO:

Mantendo os riscos da força de trabalho em evidência

A equipe de liderança da WRD espera que este dossiê de missão e os recursos fornecidos tenham ajudado você a capacitar sua equipe com as habilidades e ferramentas necessárias para combater todos os tipos de ameaças cibernéticas.

Estabelecer e manter uma sólida cultura de segurança é uma missão contínua. Uma verdadeira mudança de comportamento exige uma estratégia capaz de transformar sua maior superfície de ataque, sua força de trabalho, em sua maior linha de defesa, reduzindo assim os riscos associados aos seus colaboradores.

Considere esses recursos como um complemento a uma abordagem abrangente de treinamento e conscientização em segurança. Se você tiver interesse em saber como a KnowBe4 pode ajudar sua empresa a dar o próximo passo, entre em contato conosco.

Para ter acesso a mais recursos e informações para você e seus usuários durante todo o Mês da conscientização em segurança cibernética, não deixe de seguir e mencionar @KnowBe4 nas redes sociais. Use as hashtags #CyberAware e #CyberSecMonth para ficar por dentro de tudo o que acontece durante o Mês da conscientização em segurança cibernética.

knowbe4