GUIA

CYBERSECURITY AWARENESS TRAINING

Guia de início rápido

Este guia irá guiá-lo através de cenários básicos para acelerar o seu processo de integração. Inicie sessão no portal de administração do Cybersecurity Awareness Training da ESET e utilize os links para aceder às secções relevantes do guia do utilizador. Não se esqueça de consultar o final deste documento para ver as descrições dos cursos.

Progress. Protected.

Saiba mais sobre:

ADICIONAR E REGISTAR UTILIZADORES

O primeiro passo é importar os colaboradores (a quem chamamos de "alvos") que serão inscritos e que participarão na formação. O ESET Cybersecurity Awareness Training fica disponível de imediato, permitindo inscrever os colaboradores logo após a ativação da conta.

REALIZAR CAMPANHAS DE PHISHING

Uma campanha de phishing é uma excelente ferramenta para avaliar o nível de sensibilização dos seus colaboradores em matéria de cibersegurança. Saiba como configurar e lançar a sua primeira campanha.

GERAR RELATÓRIOS

As várias opções oferecem uma visão geral clara do progresso dos seus colaboradores, do desempenho nas campanhas de phishing e do número de colaboradores que ainda não concluíram a formação.

INSCRIÇÃO AUTOMÁTICA EM GRUPOS

Pode configurar a inscrição automática, para que todos os novos colaboradores recebam formação assim que ingressarem na empresa.

PREPARAR MICROCURSOS POR E-MAIL

Pode configurar Campanhas de Treino por E-Mail — pontuais ou programadas — para garantir que os seus colaboradores permaneçam informados. Além disso, a equipa de investigação global da ESET no WeLiveSecurity™ produz uma grande variedade de materiais para criar vídeos de nível avançado.

IMPLEMENTAR COMPLEMENTO DE DENÚNCIA DE PHISHING

Permita aos seus colaboradores denunciar phishing. O suplemento KillPhish™ permite aos utilizadores denunciar phishing rapidamente e fornece informações avançadas sobre a classificação de risco.

GERIR UTILIZADORES

As empresas evoluem à medida que novos colaboradores se juntam à equipa e outros seguem novos caminhos. Com o Cybersecurity Awareness Training da ESET, pode ativar ou desativar destinatários sempre que necessário, ou mesmo adicionar novos administradores para gerir a formação.

GUIA DO CURSO DA BIBLIOTECA DE CONTEÚDOS

Encontrará um conjunto de módulos de formação na sua consola. Analise o conteúdo de cada um para decidir qual é o mais adequado para si.

FLUXOGRAMA DO CURSO

Ainda não sabe por qual módulo de formação começar? O guia "Ajude-me a escolher" irá ajudar a encontrar o curso certo.

O que gostaria de fazer hoje?

ADICIONAR UTILIZADORES E INSCREVÊ-LOS NA FORMAÇÃO

1. Criar grupos e adicionar alvos (utilizadores)

Os utilizadores que serão inscritos na formação e participarão em testes de phishing (campanhas) são designados por **Alvos**. Deverá criar um **Grupo** (ou vários) e, em seguida, adicionar ou sincronizar os alvos. Pode adicionar manualmente, através de um ficheiro CSV, ou sincronizá-los com o Microsoft 365, o Active Directory, o LDAP e outras plataformas.

GUIA DO UTILIZADOR + VÍDEO
Criar grupos e importar alvos

2. Inscrever numa formação

Existem duas opções para uma formação inicial: **Curso gamificado Cybersecurity Awareness Training da ESET** e **Formação All-in-one Security Training**. Ambas abordam todas as informações básicas de que a maioria das pessoas necessita para se protegerem melhor a si próprias e às suas organizações, e emitem um certificado após a aprovação no questionário, o que satisfaz os requisitos de seguros e conformidade.

+ DICAS

Pode subscrever cursos adicionais gratuitamente em **Escola > Biblioteca de Conteúdos / Loja.** Depois de se inscrever, também pode atribuir esses cursos aos alunos. Veja aqui todas as descrições dos cursos.

Pode alterar as definições da sua escola antes da inscrição, caso queira realizar alguma destas ações:

- Mudar o método de início de sessão de nome de utilizador/palavra-passe para **Token**. Assim, os seus formandos não precisam de credenciais de acesso para aceder ao treino. Em vez disso, qualquer inscrição ou e-mail de lembrete terá um link único que faz login diretamente no portal.
- Ative lembretes de curso automáticos, que serão emitidos semanalmente até o curso ser concluído.

GUIA DO UTILIZADOR
Inscreva alvos num curso

GUIA DO UTILIZADOR
Definições da Escola

REALIZAR UMA CAMPANHA DE PHISHING

1. Configurar uma lista segura

A lista segura permite que os e-mails simulados pela ESET contornem o seu filtro de e-mail. Para que as simulações funcionem corretamente, os nossos IPs devem ser incluídos na lista de permissões do seu filtro de spam. Alguns sistemas podem exigir a inclusão na lista segura por cabeçalhos. Consulte o guia Noções Básicas de Listas Seguras abaixo:

GUIA DO UTILIZADOR + VÍDEO
Noções Básicas de Listas Seguras

Encontrará instruções para várias plataformas na barra lateral após clicar na ligação acima. Se utilizar o Microsoft 365 para o e-mail, os domínios dos modelos de phishing que selecionar também devem ser adicionados ao Microsoft Defender (até 20 de cada vez). Siga o guia no link abaixo:

GUIA DO UTILIZADOR + VÍDEO
Microsoft Defender Advanced Delivery

2. Criar Campanha

Antes de criar a sua primeira campanha simulada de phishing, talvez queira autorizar o seu domínio (ou pode ignorar isto e fazê-lo por campanha). Se ainda não adicionou os seus públicos-alvo/grupos, siga o Passo 1 à esquerda.

Depois de criar o seu primeiro grupo e autorizar o(s) domínio(s) de destino, pode criar a sua primeira campanha. Também pode explorar, personalizar e adicionar templates de phishing primeiro.

Recomendamos ativar a opção **Inscrição Automática de alvos que falharam**, o que significa que, se algum dos seus alvos clicar num link, transferir um anexo ou responder ao e-mail de teste de phishing, será automaticamente inscrito num curso para aprender a ter mais cuidado no futuro. Os cursos intitulados TEST FAIL são cursos de reciclagem de 5 minutos destinados a este fim. Veja descrições aqui.

GUIA DO UTILIZADOR + VÍDEO
Criar uma Campanha

GERAR RELATÓRIOS SOBRE CAMPANHAS DE PHISHING E/OU O ESTADO DOS CURSOS

1. Escolha o seu relatório

Vá a **Relatórios > Gerador de Relatórios** e selecione o tipo de relatório que deseja.

- Se está a reportar uma campanha de phishing, escolha **Por Campanha > Sumário de Relatório**.
- Se pretende ver o estado de uma formação (quem se inscreveu, quem está a frequentar ou quem já concluiu), selecione **Por Curso > Relatório de Inscrições em Cursos**.
- Pode encontrar descrições adicionais dos relatórios disponíveis abaixo.

USER GUIDE
Report Generator

2. Para filtrar por grupos ou tipos de alvos, clique no menu suspenso Filtros

Escolha os filtros de seleção (tais como campos baseados na localização, funções, etc.) e/ou selecione o(s) grupo(s) a incluir neste relatório.

3. Guarde as definições do relatório personalizado (opcional)

Ative o botão deslizante para **Guardar Opções Personalizadas**, e atribua um nome ao seu relatório personalizado. Se o fizer, este aparecerá no menu suspenso **Selecionar Relatório** no futuro.

4. Clique em Submeter

Poderá ver os detalhes do seu relatório. Em seguida, pode clicar em **Guardar PDF** ou **Enviar PDF por E-mail** no canto superior direito.

+ DICAS

Pode criar relatórios a partir de outras fontes:

- Relatórios de cursos específicos, acedendo a **Escola > Gerir Conteúdo**, e, em seguida, clicar em **Ver** ao lado de qualquer curso que tenha atribuído. Pode guardar como **CSV**, **Excel**, ou **PDF**.
- Os relatórios de testes de phishing também podem ser criados a partir de **Testes/Campanhas > Gerir Testes** (ou Campanhas) e, em seguida, clique em **Ver** no lado direito. Desça até à secção Detalhes e clique em **CSV** ou **Excel** para criar um relatório a partir daí.

INSCREVER AUTOMATICAMENTE GRUPOS NA FORMAÇÃO

1. Criar novo evento

Pode configurar um grupo para uma inscrição automática num ou em vários cursos de formação, de modo a que, sempre que alguém for adicionado ao grupo (manualmente ou através de sincronização automática), o novo membro seja automaticamente inscrito. Vá até Administração > Definições > Definições de Conta, e, em seguida, clique em **EVENTOS** na parte superior. Depois, clique no botão **Criar** no canto superior direito.

2. Crie um Evento de Inscrição Automática

Digite o seu nome e, em seguida, selecione **Adicionar Alvo a um Grupo** em **Evento**. Em seguida, clique no menu suspenso em **Selecionar** para escolher o(s) grupo(s) que pretende configurar para a inscrição automática. Clique em **Seguinte**.

Em **Ação**, selecione se pretende escolher um curso ou um programa. Selecione o curso ou programa no qual gostaria de ser inscrito automaticamente para os destinatários adicionados ao grupo.

Selecione **Verificação de Inscrição** em **Condições** e, em seguida, clique em **Seguinte** (ou em **Adicionar Ação** se pretender adicionar mais cursos).

Verifique os parâmetros e, se estiverem corretos, clique em **Concluir**. Qualquer pessoa adicionada a este grupo a partir de agora será automaticamente inscrita no(s) curso(s) que especificou aqui.

CONSULTAR AS CERTIFICAÇÕES DOS MEUS FORMANDOS

Vá a Escola > Certificados > Certificados de Estudantes. Pode **Ver**, **Fazer Download** ou **Imprimir** a partir do menu suspenso à direita.

Também pode utilizar a função **Criar Certificado** para qualquer curso exclusivo que tenha carregado no portal. Clique abaixo para saber mais:

GUIA DO UTILIZADOR
Certificados

ENVIAR MINICURSOS DE APRENDIZAGEM POR E-MAIL

Tal como a criação de uma campanha de phishing, pode configurar **Campanhas de Formação por E-mail** para serem enviadas uma única vez ou de forma programada. Estes e-mails abordam temas de cibersegurança que estão inteiramente incluídos no próprio e-mail, para que a sua organização se mantenha informada e vigilante.

Também publicamos semanalmente ou quinzenalmente vídeos curtos e de nível avançado sobre temas recentes no mundo da cibersegurança, todos produzidos pela nossa equipa de investigação global em WeLiveSecurity™.

A. Configurar uma lista segura

A lista segura permite que os e-mails simulados pela ESET contornem o seu filtro de e-mail. Para que as simulações funcionem corretamente, os nossos IPs devem ser incluídos na lista de permissões do seu filtro de spam. Alguns sistemas podem exigir a inclusão na lista segura por cabeçalhos. Consulte o guia Noções Básicas de Listas Seguras abaixo:

GUIA DE UTILIZADOR + VÍDEO
Noções Básicas de Listas Seguras

Encontrará instruções para várias plataformas na barra lateral após clicar na ligação acima. Se utilizar o Microsoft 365 para e-mail, o domínio de e-mail de formação (trainingemails.com) deve ser adicionado ao Microsoft Defender. Siga o guia no link abaixo:

GUIA DE UTILIZADOR + VÍDEO
Microsoft Defender Advanced Delivery

B. Configurar uma campanha de formação

Inicie uma campanha de formação da mesma forma que iniciaria uma campanha de phishing, acedendo a Testes / Campanhas > Criar Campanha. Depois clique em **Iniciar** abaixo de **Campanha de Treino**. Também pode explorar, personalizar e adicionar templates de phishing primeiro. Clique em **E-mails de Treino** abaixo de **Tipo de Template** para filtrar apenas os e-mails de formação.

Pode escolher novos modelos quando criar uma campanha, mas se visitar a biblioteca de modelos, pode ver ou personalizar detalhes, se assim desejar (ou criar o seu próprio modelo).

Veja mais informações no Guia de Utilizador:

GUIA DE UTILIZADOR + VÍDEO
Criar uma campanha

INSTALAR UM PLUG-IN PARA QUE OS UTILIZADORES DENUNCIEM PHISHING

A. Oferecem um plug-in gratuito para isto?

Oferecemos três plug-ins gratuitos diferentes. Veja aqui as diferenças:

GUIA DE UTILIZADOR
Plug-ins de denúncia de phishing

B. O que é e como funciona o KillPhish™?

Permita que os utilizadores analisem e denunciem ameaças de e-mail com o plug-in incluído para o Outlook, o KillPhish™.

O KillPhish™ é um suplemento avançado de proteção contra ameaças de e-mail para o Microsoft 365. Analisa ameaças conhecidas em Windows, Mac/iOS e Android para o Outlook Desktop, Web e Mobile. Permite denunciar phishing e outros tipos de ameaças. O perfil de risco de cada caixa de e-mail é único, e o KillPhish™ pode ajudar a identificar sinais de ameaças à segurança.

Atribui uma "pontuação" no Outlook que indica o nível de risco provável de um e-mail, com base em agentes maliciosos conhecidos, registos SPF, endereços IP, domínios, palavras-chave e outros fatores. Permite também que os utilizadores cliquem num botão Denunciar em e-mails suspeitos. Estes dados são incluídos no Net Reporter Score, disponível na CyberCentral da ESET, que pode utilizar para avaliar a evolução ao longo do tempo, juntamente com outros dados recolhidos no âmbito das suas campanhas de phishing.

C. Com que dispositivos/plataformas é compatível?

O KillPhish™ funciona em caixas de e-mail do Microsoft Office 365. Funciona no Outlook para computador, na aplicação web do Outlook (OWA) e na aplicação do Outlook para dispositivos móveis.

D. Como implemento isto?

Siga as instruções no Guia de Utilizador abaixo:

GUIA DE UTILIZADOR
Suplemento Microsoft (KillPhish)

E. E se não usarmos o Outlook?

Existe também uma versão simplificada do KillPhish™ para o Google Workspace:

GUIA DE UTILIZADOR
KillPhish Lite

ADICIONAR MAIS ALVOS QUANDO JÁ NÃO HÁ LUGARES DISPONÍVEIS

A. Desativar ou eliminar alvos

Se algumas pessoas já não fazem parte da sua organização, pode eliminá-las ou desativá-las para libertar licenças (até 20% por ano). Se quiser sincronizar utilizadores, isso é feito automaticamente (por exemplo, com o Microsoft Graph para o Microsoft 365 ou o AD).

Se quiser gerir manualmente, vá a Alvos/Grupos > Gerir Alvos, e depois, clique no botão triangular do menu suspenso à direita do alvo e, depois, clique em **Eliminar** ou **Desativar**. Se os desativar, pode reativá-los mais tarde, caso tenha um lugar disponível.

Para eliminar ou desativar vários de uma só vez, vá até Alvos/Grupos > Gerir Grupos e clique no botão triangular de menu suspenso situado à direita do grupo com os alvos que pretende editar.

Selecione todos os alvos a editar clicando na caixa de seleção à esquerda; em seguida, desça até ao final da página e clique em **Eliminar** ou **Desativar**.

B. Adquira licenças/amplie a sua licença

Pode adquirir licenças adicionais ou ampliar a sua licença a qualquer momento até três meses antes do prazo de validade. Consulte a secção à direita para obter instruções.

ADICIONAR UTILIZADORES ADMINISTRADORES AO PORTAL

Pode adicionar um número ilimitado de utilizadores administradores à sua conta. Estes são os utilizadores com acesso à plataforma de administração para adicionar utilizadores, atribuir formações, realizar campanhas de phishing, ver relatórios, etc.

Existem dois tipos de utilizador no portal de administração: Administrador e Utilizador. Um Utilizador não consegue ver o separador Administração no portal, mas tem acesso a todas as outras funções da plataforma de administração.

Para adicionar uma conta de administrador, vá até Administração > Gerir Utilizadores de Portal, e clique em **Criar** no canto superior direito. Em **Tipo**, clique em **Utilizador** para acesso limitado e **Admin** para acesso total, e adicione o e-mail e o nome deles.

Clique em **Guardar**.

+ NOTA

Estes utilizadores não vão participar na formação e fazer campanhas de phishing. Esses são os alvos e serão adicionados em Alvos/Grupos.

AINDA TENHO DÚVIDAS. PRECISO DE AJUDA!

Como posso adicionar utilizadores/licenças ou renovar a minha conta?

Se o total de licenças for inferior a 100, siga estes passos. Para mais de 100 licenças, contacte o seu integrador ou envie um e-mail para comercial@eset.pt, caso não tenha um.

1. Inicie sessão no Portal de Administração.
2. Ao lado do nome da sua empresa, copie o **Utilizador** alfanumérico (começa com ECAT ou ECA2).
3. Aceda à página de Gestão de Subscrições da ESET, cole o Utilizador mencionado no passo 2 e clique em **FAZER LOGIN AGORA**.
4. Vá até **Gestão de Subscrições** no canto superior esquerdo. Em **Detalhes da Licença**, clique em **Alargar Licença**. Depois digite ou clique no + para obter o novo total de **Dispositivos** (utilizadores/alvos).
5. Selecione a data de validade atual para aumentar o número de licenças, ou a segunda data de validade para renovar e aumentar o número de licenças.
   - Se quiser alargar, pagará a diferença entre as licenças existentes e adicionais. Se faltarem menos de 90 dias para o vencimento, o pedido é processado como renovação. Se renovar agora, as licenças adicionais são adicionadas imediatamente e prolongadas até ao final do período de validade da sua licença (até 20% adicionais).
   - Se quiser renovar, introduza o novo total de licenças, caso seja diferente. A sua conta será válida por mais um ano a partir da data original, ou por um ano a partir de hoje, caso a conta já tenha expirado.
6. Clique em **ATUALIZAR AGORA**, e depois em then **CONTINUAR PARA A ENCOMENDA**.
7. Verifique os seus dados (pode ser necessário introduzir o e-mail associado à sua conta) e, em seguida, clique em **CONTINUAR PARA O PAGAMENTO**.
8. Introduza os seus dados de pagamento para processar a encomenda.
9. Os lugares adicionais ou a renovação serão processados no prazo de quatro horas úteis.

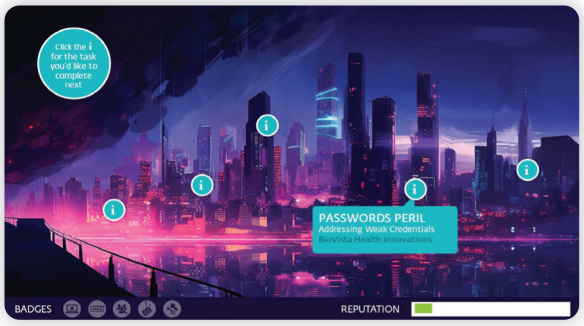
GUIA DA BIBLIOTECA DE CONTEÚDOS

Os cursos de formação abrangentes, bem como outros cursos, já estão na sua conta. Pode inscrever-se gratuitamente em cursos adicionais acedendo a Escola > Biblioteca de Conteúdos. Leia as descrições abaixo para saber qual é a opção mais adequada para a sua organização. Veja também os Fluxogramas de Cursos para obter ajuda adicional na escolha.

Formação abrangente

80-90 MINUTOS

Ambas as opções incluem as melhores práticas para se proteger a si e à sua organização contra as ciberameaças e os cibercrimes atuais. Ambas cumprem os requisitos da grande maioria das normas de seguros e conformidade. Os cursos retomarão a partir do ponto em que o participante ficou, caso não consiga concluí-los numa única sessão.



OPÇÃO 1: SECURITY AWARENESS TRAINING GAMIFICADO DA ESET

Esta formação gamificada e interativa permite ao formando escolher a ordem dos tópicos e inclui uma pontuação de reputação, 5 minijogos para reforçar o processo de aprendizagem, 5 cenários e um questionário de 15 perguntas. A história e o formato foram totalmente atualizados, e o conteúdo de vídeo incluído é totalmente novo ou foi atualizado com as informações mais recentes. Se a sua organização concluiu a versão anterior (gamificada) da formação, esta é recomendada para o ano seguinte, especialmente se os seus requisitos de seguros ou conformidade exigirem que a formação seja diferente todos os anos.

PROTEÇÃO DE DADOS PESSOAIS IDENTIFICÁVEIS (PII)

PARA ORGANIZAÇÕES QUE TRATAM DE PII

10 MINUTOS

- Introdução aos PII
- O que são Dados Pessoais Identificáveis (PII)?
- Por que é importante proteger os PII?
- Como proteger os PII

OPÇÃO 2: ALL-IN-ONE CYBERSECURITY TRAINING

Este formato linear é uma versão simplificada da formação. Tem uma estrutura de blog, com animações, cenários e interações. O conteúdo de vídeo foi adicionado ou realizado com a atualização dos conselhos mais recentes de especialistas. Ambas as opções abordam os seguintes tópicos:

SEGURANÇA NA INTERNET

- Redes Públicas de Wi-Fi
- Manter a Segurança Durante o Trabalho Remoto
- Inteligência Artificial (IA)
- Filtro de Conteúdos Online
- Navegação Mais Segura
- VPNs

PALAVRAS-PASSE

- Utilizar Palavras-passe ou Frases-passe Seguras
- Boas Práticas de Palavras-passe
- Gestão de Palavras-passe
- Autenticação Multifatorial

MALWARE

- Tipos de Malware
- Alvos de Malware
- Segurança de Dispositivos Móveis
- Como o Malware Chega Até Si

AMEAÇAS PERSONALIZADAS

- Engenharia Social
- Ameaças Internas

E-MAIL

- Phishing
- Anexos de E-mail
- Spam

Minicursos

30-50 MINUTOS

CURSO ESSENCIAL SECURITY AWARENESS TRAINING

30 MIN, INCLUI CERTIFICADO BÁSICO

Esta formação foi feita para organizações com tempo de formação limitado ou que apenas precisam de abordar os conceitos básicos. Inclui apenas o vídeo animado e uma pergunta de conhecimentos sobre os tópicos descritos abaixo, além de um questionário de 5 perguntas no final.

Este é um **programa de cursos**, ou seja, trata-se de um grupo de minicursos. Cada curso será atribuído aos seus utilizadores, que poderão acompanhar o seu progresso à medida que avançam e serão orientados ao longo de cada um deles. Inclui:

- Phishing
- Engenharia Social
- Ameaças Internas
- Malware
- Navegação Mais Segura
- Palavras-passe Fortes

CURSO RÁPIDO SECURITY AWARENESS TRAINING

50 MIN, INCLUI CERTIFICADO RÁPIDO

Este curso é uma versão resumida do Curso All-in-one Cybersecurity Training. Embora uma narrativa completa possa ajudar a cativar os formandos e a aumentar a retenção de conhecimentos, para as organizações que não dispõem de 90 minutos para dedicar à formação e não precisam de abordar todos os tópicos, este curso é uma excelente opção. Inclui:

- Phishing
- Anexos de E-mail
- Engenharia Social
- Ameaças Internas
- Malware
- Navegação Segura
- Palavras-passe Fortes
- Boas Práticas de Palavras-passe
- Autenticação Multifatorial

Cursos de reciclagem

3-8 MINUTOS

TESTE DE PHISHING FALHADO

Os minicursos de Teste de Phishing Falhado são ideais para utilizar na criação de uma campanha de phishing para a inscrição automática em cursos. Assim, quando um alvo (aluno) clicar num link, descarregar um anexo ou realizar uma ação semelhante num teste de phishing, aprenderá imediatamente a evitar esse erro numa tentativa real de phishing.

- **TESTE DE PHISHING FALHADO—Phishing**
  Recomendado para alvos que clicam num link ou respondem a um e-mail de teste de phishing
- **TESTE DE PHISHING FALHADO—Engenharia Social**
  Recomendado para alvos que introduzem informações em testes de phishing que incluem uma página inicial (como uma página de login simulada)

VÍDEOS CURTOS

Os Vídeos Curtos (15 opções, vídeos e um teste de conhecimentos) também fazem parte dos cursos de formação abrangentes e não precisam de ser atribuídos aos utilizadores no âmbito da sua inscrição normal, caso os inscreva num dos cursos de formação abrangentes.

MINICURSOS

Estes Minicursos (6 opções) são cursos curtos, em formato de blog, e podem ser atribuídos sempre que desejar atualizar um determinado grupo ou todos os funcionários sobre um tema específico. Acedendo a **Escola** > Biblioteca de Conteúdos / Loja, pode subscrevê-los gratuitamente. Pesquise **Minicursos** no topo, e depois pode **Pré-visualizar** ou **Subscrever** (gratuitamente) no que se quer inscrever.

MINIJOGOS

JOGOS QUE PODEM SER ATRIBUÍDOS PARA MANTER FUNCIONÁRIOS EM FORMA

Estes 5 minijogos estão no Curso Gamificado de Security Awareness Training. Podem ser atribuídos como revisão de determinados tópicos ou como complemento a qualquer curso de formação não gamificado, como uma forma divertida de reforçar um tópico e ajudar a cimentar os conhecimentos.

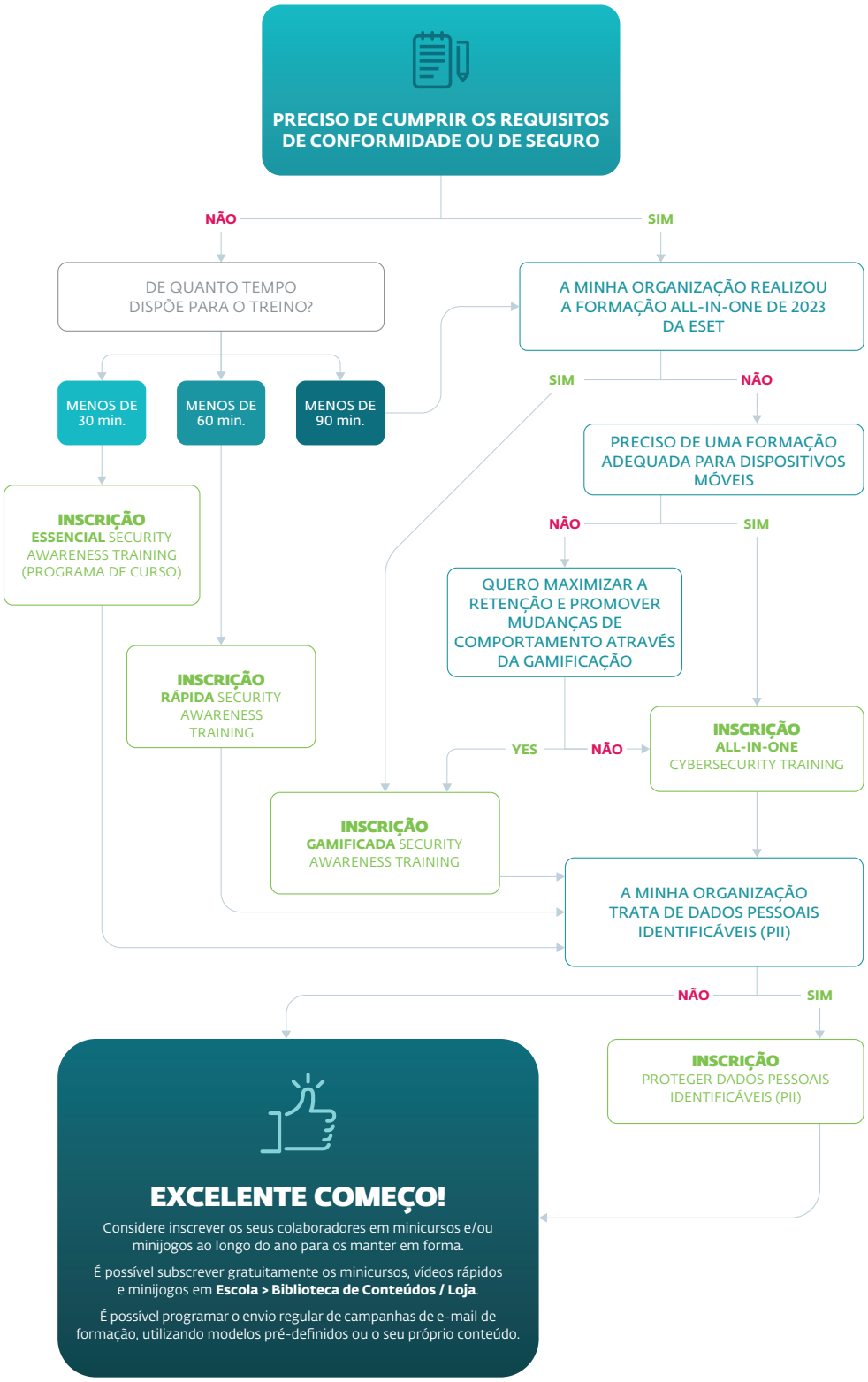
Pode subscrevê-los gratuitamente acedendo a **Escola** > Biblioteca de Conteúdos / Loja. Pesquise **Minijogos** no topo, e depois pode **Pré-visualizar** ou **Subscrever** (gratuitamente) no que se quer inscrever.

Os jogos incluem:

- Lance-se na Defesa Contra a Engenharia Social
- Escolha Palavras-passe Fortes e Proteja os seus Dados
- Proteja a Atlântida de Ataques de Phishing
- Detetive de Dados de IoT e Trabalho Remoto
- Proteja a sua Cidade contra Ataques de Malware

FLUXOGRAMA DE CURSOS

AJUDE-ME A ESCOLHER O(S) CURSO(S) A ATRIBUIR



eset Digital Security
Progress. Protected.