

GUIA

Como planejar seu calendário de serviço de Conscientização e Treinamento em Cibersegurança

Como o cenário de ameaças muda rapidamente e torna-se cada vez mais mal-intencionado, há a necessidade de avançar os programas de serviço de Conscientização e Treinamento em Cibersegurança para garantir que acompanhem as ameaças atuais. Criar um ciclo contínuo de aprendizado ajuda a incorporar uma cultura de conscientização cibernética na empresa e a fazer com que todos atuem para proteger contra as ameaças.

A importância do aprendizado contínuo

É essencial que o treinamento seja continuado e adequado. Hermann Ebbinghaus, psicólogo alemão, foi pioneiro em estudos experimentais voltados à memória, que foram conduzidos durante o final do século XIX, levando-o à descoberta da “[Curva do esquecimento](#)”. Conforme observado por Ebbinghaus, se uma nova informação não for aplicada, nós esqueceremos cerca de 75% dela em apenas seis dias.¹

Embora possa ser interessante criar um grande módulo de treinamento que atenda às obrigatoriedades de conformidade e disponibilizar anualmente tal módulo aos funcionários, o consequente desafio é que a conscientização em Cibersegurança não estará à frente das operações diárias.

Consolidar uma cultura que recompense comportamentos positivos, os quais sejam esperados pela empresa, não precisa ser algo complexo e difícil de colocar em prática. Basta um pouco de planejamento e criatividade, além de algumas verificações ao longo do ano, para que você empregue a conscientização organizacional sobre segurança cibernética durante o ano todo.

Este documento tem o propósito de gerar ideias, ajudando você a elaborar o calendário do seu programa de conscientização e formação em Cibersegurança.

Essa etapa, ou seja, a elaboração do seu calendário, ocorre depois de ter definido as metas e estratégia do seu programa. Precisa de ajuda com a primeira etapa? Consulte [Guia sobre como definir as metas e planejar seu serviço de Conscientização e Treinamento em Cibersegurança](#).

Conscientização e Treinamento em Cibersegurança alinhadas à integração do funcionário

Quando uma nova contratação é integrada à empresa, é importante incluir o treinamento de conscientização em Cibersegurança no processo de integração.

Apresentar aos novos funcionários os elementos básicos de um bom comportamento de Cibersegurança desde o primeiro dia ajuda a mostrar a eles que, para a empresa, a segurança e a proteção dos dados, redes e usuários são fundamentais.

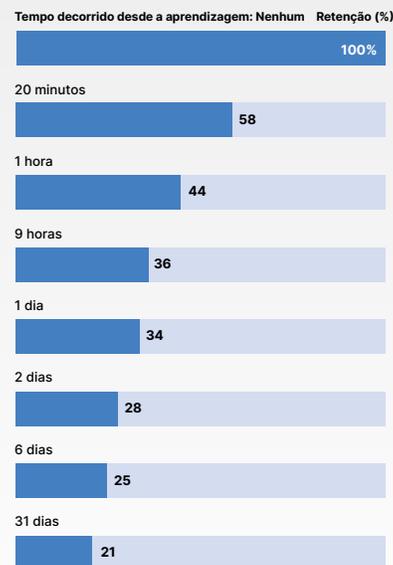
Comece com um módulo de formação introdutório que ensinará aos aprendizes o conceito da conscientização e formação em segurança da informação e mostre o que pode ser feito para proteger informações pessoais e sobre a empresa.

Feito isso, escolha módulos complementares específicos que abordem áreas importantes para a empresa. Se você sabe, por exemplo, que o ataque de phishing é um problema específico enfrentado pela sua empresa, selecione os módulos sobre phishing, engenharia social e segurança de e-mail; você pode combiná-los ao módulo introdutório ou introduzi-los durante determinado período da integração.

Depois, teste seus usuários com exercícios de simulação de phishing. Assim, usuários que possam acabar caindo em um ataque de phishing simulado poderão ser redirecionados a micromódulos extras, para lembrar dos ensinamentos importantes.

A curva do esquecimento

Se uma nova informação não for aplicada, nós esqueceremos cerca de 75% dela em apenas seis dias.



Fonte: Hermann Ebbinghaus

Integração de amostra

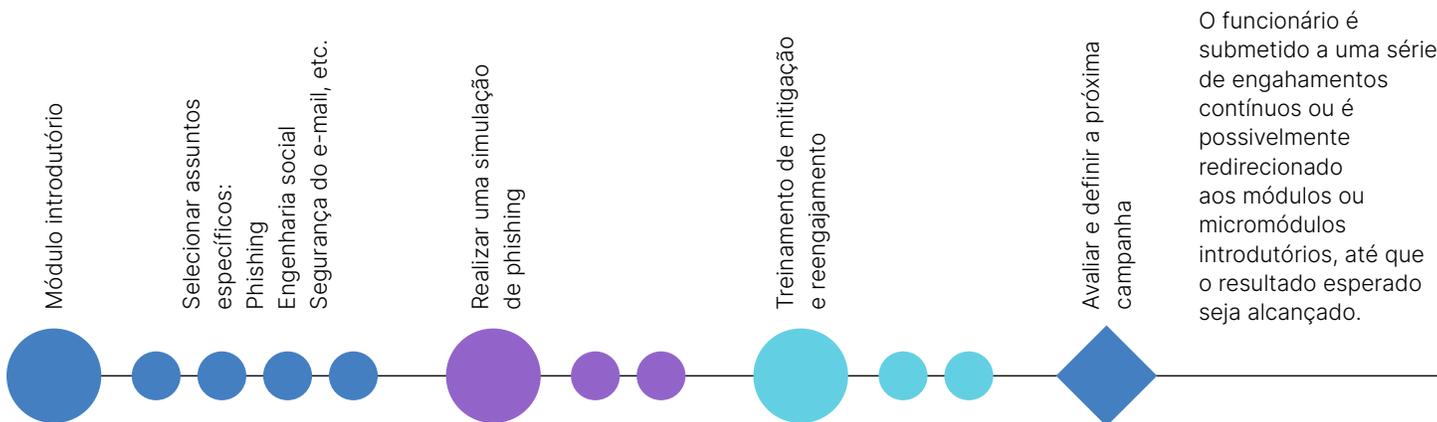


Figura 1: O tempo entre os módulos de formação pode ser de dias ou semanas, dependendo do seu processo de integração.

Crie uma cultura de Cibersegurança com participação contínua

Recomenda-se verificar os funcionários ao longo do ano e promover breves oportunidades de aprendizado que ajudem a impulsionar uma cultura de conscientização em Cibersegurança. O envio mensal de novos conteúdos ajuda a manter o interesse e a participação dos funcionários. É importante que o treinamento seja devidamente direcionado à função certa e que possa ser facilmente assimilado, entendido e implementado. Não sobrecarregue seus funcionários com grandes blocos de treinamento de uma só vez.

Confira abaixo uma campanha de exemplo que pode ser dividida em um único ou em vários assuntos, criando um tema para cada mês. Inclua, além disso, simulações correspondentes de phishing, de técnica de tailgating na porta do escritório, verificações sem aviso prévio se a mesa está limpa ou não, além de outros tipos de teste, que podem ser combinados com a divulgação de recursos de comunicação que ajudam a reforçar os principais ensinamentos.

O exemplo a seguir ocorre durante um período de três meses; a ideia, porém, é que temas diferentes continuem ao longo do ano. Este é um panorama de três meses de um programa que dura o ano todo. A frequência mensal é um exagero para sua empresa? Crie o mesmo modelo, mas opte por uma frequência trimestral, ao invés de mensal.

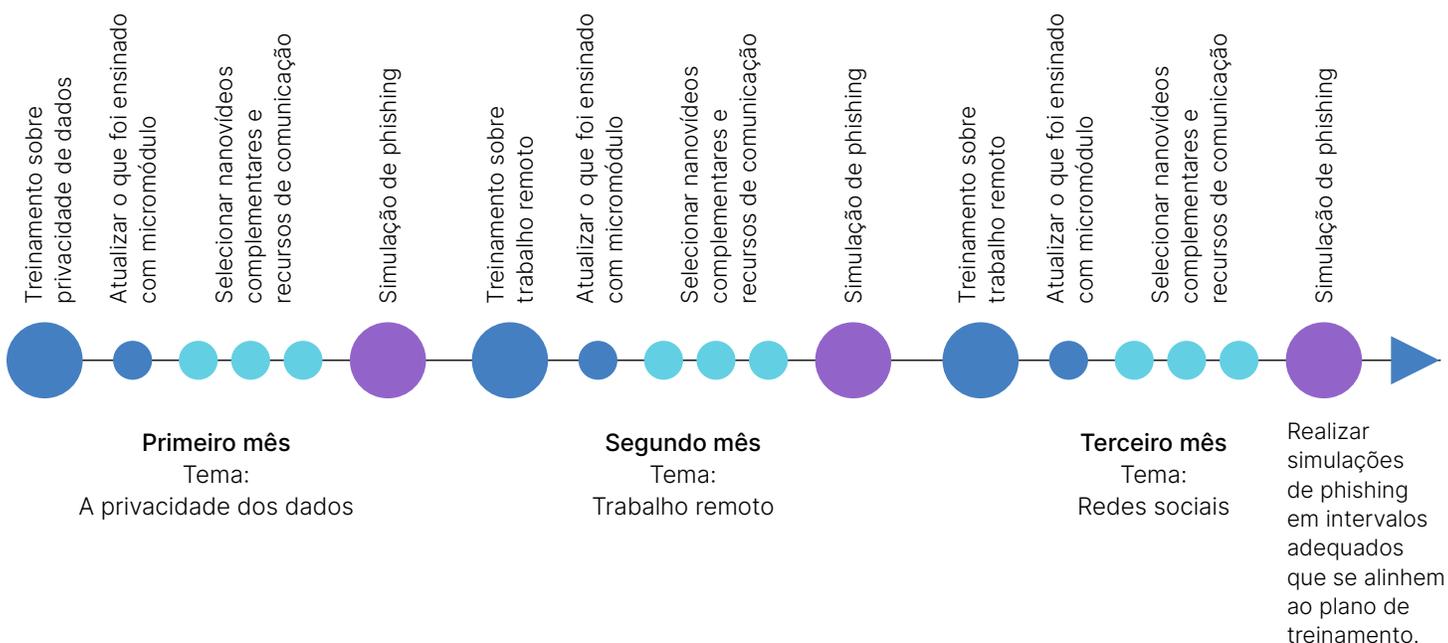


Figura 2: Resumo de três meses de um programa com a duração de um ano.

Adapte sua formação e conscientização de acordo com diferentes períodos festivos e eventos regionais e globais

Uma excelente maneira de reforçar os principais ensinamentos é associar sua formação e conscientização aos assuntos do setor ou aos períodos festivos. Além disso, seus funcionários podem ler sobre esses assuntos em outras publicações ou nas redes sociais, o que ajuda a reforçar a importância da segurança cibernética.

Confira alguns períodos festivos ou considerações importantes nos quais pode basear sua campanha:

Outubro é o Mês de Conscientização em Segurança Cibernética

O Mês de Conscientização em Segurança Cibernética é uma campanha internacionalmente conhecida, realizada todos os meses de outubro para ajudar o público a aprender mais sobre a importância da segurança cibernética.

O National Institute of Standards and Technology destaca algumas [dicas, temas e recursos úteis](#) para usar durante esse mês.

A Black Friday e os períodos festivos

A Black Friday e a Cyber Monday dão início à temporada de compras nos Estados Unidos. Aliás, 30% de todas as vendas do varejo ocorrem entre a Black Friday e o Natal. Desde a criação da Cyber Monday, as lojas físicas e de comércio eletrônico buscam gerar uma parcela significativa da sua receita anual durante esse fim de semana de compras.

Conforme observado pelo FortiGuard Labs, há uma quantidade cada vez maior de golpes envolvendo sites falsos que parecem sites legítimos de comércio eletrônico. Eles podem até parecer seguros, mas, se você não estiver prestando atenção, podem acabar desviando seu pagamento (e até mesmo suas informações de pagamento) durante uma compra que, para você, era legítima. Sites falsos de comércio eletrônico estão rapidamente se tornando a principal ameaça aos consumidores e eles abrangem uma variedade enorme de produtos para ludibriar possíveis clientes.

Realize campanhas até esse período para orientar seus funcionários sobre essa ameaça e como é fácil cair no golpe desses sites. [Leia mais](#) no blog da Fortinet.

Dia da Privacidade de Dados/Dia da Proteção de Dados

O Dia da Privacidade de Dados, ou Dia da Proteção de Dados, como é conhecido na Europa, é celebrado no dia 28 de janeiro. O objetivo dessa data é conscientizar e promover práticas recomendadas voltadas à privacidade e à proteção de dados.

Este é um excelente momento para focar seu treinamento na segurança e privacidade de dados. Gostaria de conferir mais recursos sobre o assunto? Muitas regiões e governos possuem campanhas nacionais específicas que podem ser implementadas pelas empresas.

Temporada de declaração do imposto de renda

Há muitos cibercriminosos por aí, loucos para aproveitar o estresse e as incertezas que cercam a temporada de declaração do imposto de renda. Eles empregam ataques de [phishing](#), campanhas de e-mail ou até mesmo por chamadas telefônicas, se passando por alguém da Receita Federal ou de algum órgão responsável pela fiscalização. Esses criminosos podem extrair informações pessoais a partir dos dados roubados, incluindo números da Previdência Social, o que os torna legítimos, mesmo que não sejam realmente.

Além das campanhas de phishing implementadas através de um modelo “[atirar para todos os lados](#)”, que envia milhares de e-mails na esperança de que, ao menos, uma pessoa caia na armadilha, outro tipo de ataque que também está em alta é o spear phishing.

Até a temporada de declaração do imposto de renda, realize campanhas para garantir que seus funcionários não acabem se distraíndo e caindo em um ataque de spear phishing mais sofisticado. Esse tipo de ataque é muito mais difícil de se identificar, já que ocorre na forma de e-mails direcionados e personalizados que muitas vezes dão a impressão de que foram enviados por alguém que conhece o destinatário.

Outros:

- Eleitoral
- Férias
- Emergências de saúde pública, como a COVID-19 ou vacinas
- Estados de emergência, como inundações, incêndios florestais, etc.

Simulação de phishing

A simulação de phishing é uma ferramenta importante para reforçar a conscientização e a formação em cibersegurança com foco em ameaças baseadas em e-mail, como phishing, spear phishing, falsa identidade, comprometimento de e-mail comercial e ataques de ransomware baseados em e-mail.

Ela deve ser uma atividade contínua (pelo menos, quinzenalmente) em toda a sua base de funcionários e usuários, embora os assuntos e a frequência possam variar. Além disso, a simulação ou teste de phishing deve incorporar conteúdos de aprendizagem e formação que se aplicam no momento do clique de um e-mail de teste.

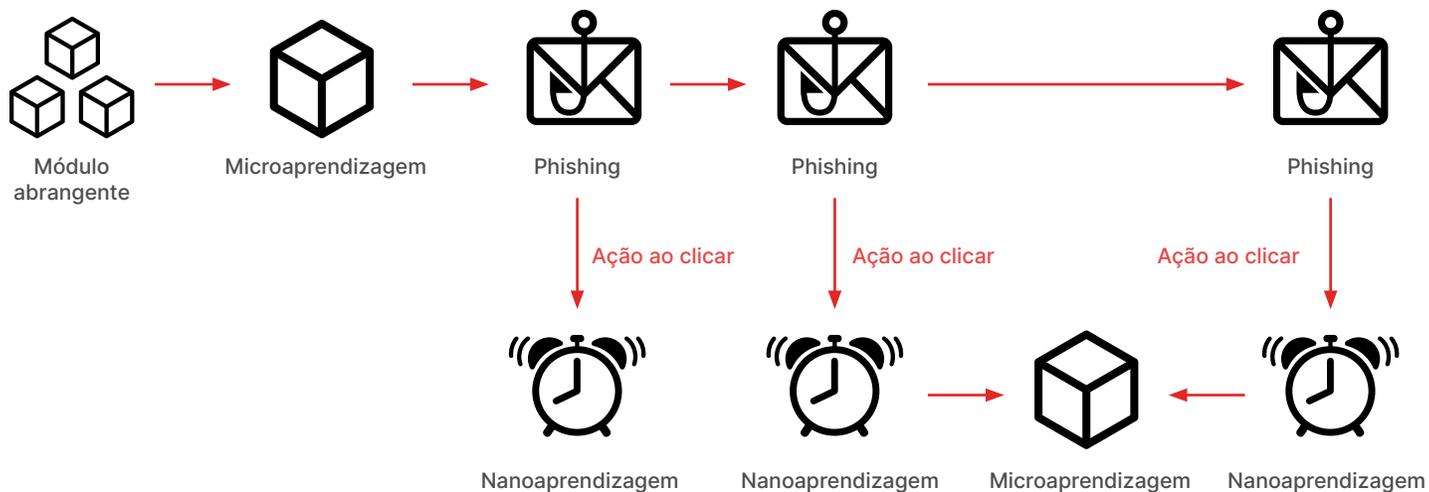


Figura 3: Como criar uma “campanha” de phishing.

Ao definir um programa de simulação de phishing, sua abordagem não deve ser, necessariamente, testar todos os funcionários em relação aos mesmos e-mails de phishing; você deve assumir uma abordagem mais inteligente que leve em consideração algumas posições estratégicas, como:

- Há grupos ou departamentos de funcionários ou usuários que devem passar por testes menos/mais frequentes ou voltados a diferentes assuntos ou táticas?
- Quais as táticas mais importantes a serem testadas para reforçar a vigilância? Se sua empresa recebe, por exemplo, e-mails supostamente do CEO pedindo uma ação por parte dos funcionários, teste tanto eles quanto os usuários em e-mails de teste parecidos.
- Realize testes que incorporem links e anexos suspeitos simulados, tanto juntos quanto de forma separada.
- Considere assuntos de phishing que estejam associados a atividades que somente os funcionários estariam cientes, aparentemente, como comunicados sobre mudanças na folha de pagamento ou nos recursos humanos, redefinições de senhas, avisos de indisponibilidade do treinamento, newsletters internas, etc. Criminosos inteligentes criarão e-mails que vão tentar imitar esses comunicados internos, portanto, é importante testar seus funcionários e usuários em relação a isso.
- Crie uma campanha de conscientização e teste de phishing específica para funcionários ou quem costuma clicar em e-mails de teste de phishing.

Ao final das campanhas de teste de phishing, lembre-se de conferir o desempenho e outras métricas para ver como sua empresa está se saindo. Ao fazer isso, analise várias posições estratégicas, como o desempenho das suas campanhas, o desempenho de grupos individuais entre as campanhas, com quais táticas os funcionários e usuários estão tendo dificuldades para identificar e quais pessoas estão clicando várias vezes em testes e precisam de mais treinamento e reforço.

Lembre-se do treinamento de mitigação

O treinamento de mitigação deve ser positivo, e não punitivo.

Como parte do ciclo contínuo da conscientização e treinamento, verifique com seus funcionários se o que eles estão aprendendo está ajudando ou mudando seus comportamentos. As verificações podem ser assinaladas por várias ações:

- Baixo desempenho em questionários e avaliações
- Clique acidental em e-mails de simulação de phishing
- Violação de dados ou privacidade
- Baixo desempenho em outros tipos de testes, tais como verificações aleatórias nas mesa, simulações de tailgating, etc.

Se os funcionários apresentarem baixo desempenho em algum desses pontos, microvídeos ou nanovídeos são ótimos recursos para enviar lembretes direcionados sobre o que fazer em cada situação. É importante que o treinamento de mitigação não seja apresentado como o ensino de uma lição, o que pode soar negativamente como um reforço. Ao invés disso, o treinamento deve ser motivador, estimulando o engajamento dos funcionários. A meta é reeducar e reforçar os principais ensinamentos, e não aplicar uma punição.

“Mesmo entre obstáculos temporais coercivos, procure oportunidades para visitar, revisar e reafirmar.”²

Sobre o Serviço de Conscientização e Treinamento em Cibersegurança da Fortinet

O Serviço de Conscientização e Treinamento em Cibersegurança da Fortinet promove uma conscientização tempestiva sobre as atuais ameaças à segurança cibernética e ajuda funcionários da empresa a terem a consciência cibernética e a conseguirem identificar e parar com os ataques. Voltado a atender às demandas de PMEs e empresas, o serviço oferece uma proposta completa que inclui uma interface administrativa intuitiva de criação de campanha, monitoramento e geração de relatórios, módulos de aprendizado do usuário final, micromódulos ou nanomódulos de reforço e recursos de conscientização.

¹ Steve Glaveski, [Where Companies Go Wrong with Learning and Development](#), Harvard Business Review, 2 de outubro de 2019.

Saiba mais

² Robert F. Bruner, [Repetition is the First Principle of All Learning](#), ResearchGate, agosto de 2001.