Formação e sensibilização dos colaboradores

Está na altura de reunir os conhecimentos que adquiriu ao longo do Programa e partilhá-los com os seus colegas. Como Líder cibernético da sua organização, irá introduzir mudanças duradouras na sua organização e na cadeia de valor global em geral.

Nesta secção, incluímos recursos chave para o ajudar a comunicar as melhores práticas de preparação para o ciberespaço em toda a sua organização de forma a promover uma mudança significativa. Encontrará modelos de e-mail que poderá copiar e personalizar, e listas de verificação para partilhar para todos os membros da sua organização poderem ser responsabilizados, bem como ligações a recursos adicionais, tanto do CRI como de toda a comunidade de cibersegurança, que podem fornecer orientações adicionais para a sua equipa.

A implementação é a etapa mais importante do Programa de prontidão cibernética porque é o momento em que o conhecimento se transforma em ação. Para o ajudar neste processo, fornecemos os seguintes recursos para utilizar:

1. Modelos de e-mail: utilize estes modelos para apresentar aos seus colaboradores os 4 principais problemas de cibersegurança e outros conceitos chave.

2. Módulos de formação sobre os 4 principais problemas de cibersegurança: vídeos de formação breves sobre os 4 principais problemas de cibersegurança que podem ser facilmente distribuídos aos colaboradores

3. PowerPoints de formação: PowerPoints para as sessões de formação dos colaboradores

4. Materiais partilháveis: cartazes, campanhas nas redes sociais, guias, etc.

O CRI concluiu que uma abordagem de grande interação é a melhor forma de maximizar os resultados da formação. Comunique claramente com os colaboradores não só o valor para a empresa, mas também para eles próprios, que a conclusão da ciberformação trará os melhores resultados.

Tenha em conta a dimensão e o número de colaboradores da sua empresa quando decidir o melhor método de comunicação. Os debates presenciais, a comunicação por e-mail ou inclusivamente os Webinars agendados para acompanhar e auxiliar os colaboradores durante o processo de formação garantirão altas taxas de conclusão.

Documento de certificação de formação

O Cyber Readiness Institute exige que todos os colaboradores e contratantes recebam formação para obterem a Certificação de prontidão cibernética.

Ao assinar e devolver este Formulário de certificação, confirma que todos os colaboradores e contratantes receberam formação nas Políticas dos 4 principais problemas de cibersegurança do CRI e no seu papel no Plano de continuidade da atividade.

_____	_____
CEO	Líder cibernético
_____	_____
Data de assinatura	Data de assinatura

Recursos de formação

Modelos de e-mail: Os seguintes modelos de e-mail podem ser modificados e distribuídos a todos os colaboradores para os notificar sobre a sua nomeação para a função de Líder cibernético, as novas políticas cibernéticas da organização e os requisitos de formação futuros. É importante que o seu CEO envie o primeiro e-mail para os colaboradores compreenderem a importancia deste esforço.

1

Assunto: Mensagem da direção para os colaboradores sobre Prontidão cibernética

Olá, equipa,

Os ciberataques são ameaças muito reais e presentes para [Nome da empresa] e para as empresas que fornecemos. É de importância vital para o futuro da nossa atividade conseguirmos melhorar já a nossa prontidão cibernética. É por isso que estabelecemos uma parceria com o Cyber Readiness Institute para proteger os dados de [Nome da empresa], os dados dos nossos clientes e as suas informações pessoais para não serem expostos e usados para fins maliciosos.

Nomeei [Nome completo] como nosso(s) Líder(es) cibernético(s). A orientação da nossa equipa ao longo do Programa de prontidão cibernética será feita por [Ele/Ela/Eles], que adotará uma abordagem prática para aumentar a sensibilização para a cibersegurança ao focar-se no comportamento humano. Ao longo do Programa, vamos abordar as ciberameaças comuns à nossa empresa e desenvolver um Manual de prontidão cibernética para nos defendermos delas.

A realidade é que um simples clique numa ligação de e-mail suspeita pode permitir que um hacker aceda à nossa rede, acedendo assim aos dados da nossa empresa, aos dados dos nossos clientes e às suas informações pessoais. Estou empenhado em tornar a [Nome da empresa] mais resistente à cibersegurança ao prevenir os ataques e ao estar preparada quando ocorre um. Agradecemos que se tenha juntado no apoio a [Nome completo] para assegurar que [Nome da empresa] está preparada para o ciberespaço.

Muito obrigado,

[Assinatura do CEO]

2

Assunto: Novas políticas de sensibilização e formação em segurança

Olá, equipa!

[NOME ORGANIZAÇÃO] está a preparar-se para a Cibersegurança! O que significa para nós:

- Novas políticas para colaboradores: adicionámos algumas novas políticas e protocolos ao nosso manual que oferecem procedimentos e diretrizes para melhorar a segurança da [NOME DA ORGANIZAÇÃO]. Poderá analisar estas políticas aqui. [LIGAÇÃO]
- Líder cibernético designado: uma pessoa responsável por liderar o nosso percurso de prontidão cibernética.

Poderá estar a perguntar-se o que significa "Prontidão cibernética". "Prontidão cibernética" significa ser inteligente em relação aos hábitos tecnológicos e saber o que procurar para se manter seguro.

Os cibercriminosos sabem como a maioria de nós trabalha e exploram estes hábitos comuns para ultrapassar a sofisticada tecnologia de cibersegurança. De facto, alguns comportamentos estão na origem da maioria das falhas de cibersegurança e da forma como os hackers conseguiram entrar. Felizmente, quando sabemos o que fazer e o que não fazer em relação a estes 4 principais problemas de cibersegurança, a probabilidade destes métodos de ataque terem êxito diminui drasticamente.

- Palavras-passe+
- Atualizações de software
- Phishing
- Armazenamento e partilha de dados

Bloquear estas quatro áreas significa que os dados confidenciais relacionados com os clientes, fornecedores e colaboradores da [NOME DA ORGANIZAÇÃO] estão mais seguros. É por esta razão que vamos enviar alguns e-mails breves que darão alguma formação básica sobre as 4 principais problemas de cibersegurança e as coisas simples que todos podemos fazer para os evitar e prevenir.

Tenha em atenção que a adesão à política de cibersegurança e a formação são *obrigatórias*. Estes e-mails e pedidos devem demorar apenas 10 a 15 minutos a concluir, e solicitamos que responda ao seu superior hierárquico direto depois de concluir cada sessão de formação.

O primeiro e-mail de formação será enviado a [MM/DD]. Entretanto, leia as políticas atualizadas para saber mais sobre este esforço.

Em caso de dúvida sobre este assunto, contacte-nos!

[ASSINATURA DE E-MAIL]

3

Assunto: Problema cibernético principal n.º 1: Palavras-passe+

Olá, equipa!

É a nossa primeira sessão da série de formação Programa de prontidão cibernética!

Problema cibernético principal n.º 1: Palavras-passe+

A palavra-passe é uma porta de entrada para uma rede, um indivíduo ou uma organização. Utilizamos centenas de palavras-passe e dispositivos ligados na nossa vida profissional e pessoal, cada um deles uma porta de entrada para a nossa empresa. Uma palavra-passe fraca equivale a deixar a porta destrancada.

Cada uma das nossas palavras-passe é guardiã das informações e de sistemas importantes que nos são confiados, e pelos quais somos responsáveis. Não podemos deixar que sejam alvos fáceis.

Uma palavra-passe difícil de decifrar é a primeira linha de defesa contra hackers oportunistas. Criar uma palavra-passe forte demora apenas alguns segundos e é algo que todos os colaboradores da [NOME DA ORGANIZAÇÃO] terão de fazer para ajudar a manter os nossos dados tão seguros quanto possível.

Segue-se uma formação rápida sobre como criar palavras-passe fortes que poderá memorizar e utilizar facilmente:

[LIGAÇÃO]

Também atualizámos as políticas da nossa empresa em matéria de palavras-passe, que se aplicam a todos os colaboradores e contratantes da [ORGANIZAÇÃO].

Se tiver alguma dúvida sobre esta formação ou sobre como utilizar e gerir as suas palavras-passe, não hesite em contactar-me diretamente para falarmos sobre o assunto.

[ASSINATURA DE E-MAIL]

4

Assunto: Problema cibernético principal n.º 1: Atualizações de software

Olá, equipa!

Estamos na segunda sessão da nossa série de formação sobre o Programa de prontidão cibernética!

Problema cibernético principal n.º 2: Atualizações de software

É provável que esteja familiarizado com as notificações pop-up que informam que está disponível uma atualização de software para o seu computador, portátil, tablet ou dispositivo móvel. Apesar de poder ser tentador clicar em "Lembrar-me mais tarde", esta não é uma boa ideia. As atualizações de software reparam as falhas de segurança importantes e corrigem os erros críticos que foram identificados, pelo que devem ser instaladas imediatamente.

A não instalação destas atualizações deixa a porta aberta a vulnerabilidades de segurança conhecidas que os cibercriminosos podem e vão explorar para entrar e fazer um ataque. O infame ataque do ransomware WannaCry tirou partido de uma falha de segurança identificada no sistema operativo Windows que já tinha sido corrigida numa atualização dois meses antes. Apesar de o ataque só ter afetado quem não tinha instalado a atualização, em apenas 24 horas mais de 230.000 sistemas foram comprometidos e causaram danos globais de 4 mil milhões de dólares.

A instalação de atualizações pode eliminar estes pontos de acesso fácil e proteger contra ataques de malware e ransomware. Felizmente, as atualizações de software são fáceis de fazer.

A maioria dos sistemas operativos e do software pode ser configura para a "atualização automática", o que pode automatizar a instalação de atualizações e minimizar a interrupção do seu trabalho. Bastam alguns minutos para assegurar ou ativar a "atualização automática" de aplicações, sistemas e dispositivos, pelo que o deve fazer o mais rapidamente possível.

Tal como fizemos com as palavras-passe, também revimos as nossas políticas empresariais relacionadas com as atualizações de software. Estes padrões aplicam-se a todos os colaboradores e contratantes da [[ORG]].

O PDF em anexo da Lista de verificação de atualização de software fornece instruções passo a passo e ligações para facilitar a sua realização, que pode ler aqui [LIGAÇÃO].

Tenha em atenção que a adesão à política e o preenchimento da Lista de verificação de atualização de software em PDF é *obrigatória* para todos os colaboradores da [ORGANIZAÇÃO]. Esta lista de verificação deve demorar apenas 10 a 15 minutos e deve ser preenchida até [MM/DD]. Não se esqueça de informar o seu superior hierárquico depois de preencher esta lista de verificação.

Se tiver alguma dúvida sobre esta formação ou sobre como utilizar e gerir as atualizações de software, não hesite em contactar-me diretamente para falarmos sobre o assunto.

[ASSINATURA DE E-MAIL]

5

Assunto: Problema cibernético principal n.º 3: Phishing

Olá, equipa!

Está pronto para a terceira sessão da nossa série de formação no Programa de prontidão cibernética?

Problema cibernético principal n.º 3: Phishing

O phishing é um dos ciberataques mais generalizados. Qualquer pessoa com uma conta de e-mail ou um smartphone pode receber um e-mail ou uma mensagem de texto com phishing. Os ataques de phishing recorrem a mensagens enganosas para obter informações confidenciais ou o acesso a uma rede. Estas mensagens tentam enganar as pessoas para clicarem numa ligação, descarregarem um anexo na mensagem ou até fornecerem diretamente informações confidenciais, tais como dados bancários.

Muitos nós sabemos que o príncipe nigeriano que lhe envia um e-mail a pedir uma transferência bancária de 5000 dólares para a sua conta bancária é uma fraude. Mas os esquemas de phishing são muitas vezes sofisticados e difíceis de detetar, se não soubermos a que aspetos devemos estar atentos. Estas mensagens costumam ser oportunistas, assumindo fraudulentamente a forma de comunicações reais que podemos receber legitimamente.

De facto, 9 em cada 10 ciberataques começam com phishing, dada a eficácia com que os hackers o fazem. Embora os métodos que os hackers utilizam para lançar ataques de phishing estejam sempre a evoluir, a maioria das mensagens de phishing utiliza uma série de truques que pode aprender a detetar para não ser enganado.

Veja este breve vídeo para aprender alguns truques para detetar "phishing" nas suas mensagens. [LIGAÇÃO PARA O VÍDEO]

Além disso, veja mais alguns truques para detetar uma tentativa de phishing [AQUI].

Se tiver alguma dúvida sobre esta formação ou sobre como utilizar e gerir as atualizações de software, não hesite em contactar-me diretamente para falarmos sobre o assunto.

[ASSINATURA DE E-MAIL]

6

Assunto: Problema cibernético principal n.º 4: Suportes amovíveis e transferência segura de ficheiros

Olá, equipa!

Hoje vamos abordar a última questão central do ciberespaço na nossa série de formação no Programa de prontidão cibernética!

Problema cibernético principal n.º 4: Armazenamento e partilha de dados

As unidades USB são uma forma popular e fácil de armazenar e transportar ficheiros, mas também são alvos fáceis do software malicioso.

Os hackers podem infetar as unidades USB com software malicioso, tal como vírus, spyware e muitos outros, que podem causar danos irreversíveis. Alguém que encontre uma unidade USB "perdida" no parque de estacionamento pode ligá-la ao seu computador para ver o que contém e devolvê-la ao proprietário, sem conhecer o risco antes que seja tarde demais. As unidades USB não são o único tipo de dispositivo multimédia amovível, também se incluem:

- Discos óticos (discos Blu-Ray, DVDS e CD-ROMs)
- Cartões de memória (cartão Compact Flash, cartão Secure Digital e pen USB)
- Discos Zip/Disquetes
- Unidades flash USB
- Discos rígidos externos (DE, EIDE, SCSSI e SSD)
- Câmaras digitais
- Smartphones
- Outros dispositivos externos/acopláveis que contêm funcionalidades de suportes amovíveis

Atualizámos a nossa política da empresa relativa ao armazenamento e partilha de dados, que se aplicará a todos os colaboradores e contratantes da [ORGANIZAÇÃO]:

Se tiver alguma dúvida sobre esta formação ou sobre como utilizar e gerir as atualizações de software, não hesite em contactar-me diretamente para falarmos sobre o assunto.

Na próxima semana, iremos abordar o nosso novo Plano de resposta a incidentes, que nos ajudará a preparar e a responder aos eventos e problemas cibernéticos que poderão ocorrer.

[ASSINATURA DE E-MAIL]

7

Assunto: O nosso Plano de continuidade de atividade

Olá, equipa!

Vamos hoje abordar o nosso Plano de continuidade da atividade!

Isto servirá de roteiro para a nossa empresa como um todo e para cada pessoa determinar o que deve fazer e como agir quando ocorre um problema cibernético ou de segurança.

As práticas de higiene cibernética que aprendemos durante esta formação e as nossas novas políticas de prontidão cibernética contribuem muito para a redução do risco de uma falha da segurança. Mas mesmo com as melhores medidas implementadas, é importante assumir que provavelmente teremos de lidar com um incidente de segurança a dada altura.

O nosso Plano de continuidade da atividade permite-nos responder, resolver e aprender rapidamente com todos os problemas que surgem. Uma crise pode ser caótica e causar uma grande tensão, mas ter um plano passo a passo assegura que a nossa resposta a uma falha de segurança é estratégica e eficaz, em vez de reativa ou inútil.

Existem três elementos principais para a continuidade da atividade:

Preparar

- ✓ Certifique-se sempre de que tem cópias de segurança atualizadas e de que sincroniza as contas na cloud
- ✓ Esteja sempre alerta para situações suspeitas ou estranhas

Responder

- ✓ Contacte sempre o [LÍDER CIBERNÉTICO OU CONTACTO DE TI] se detetar algo estranho ou suspeito (o computador ficou bloqueado depois de abrir um ficheiro, etc.)
- ✓ Deixe imediatamente de utilizá-lo e desligue o dispositivo da rede

Recuperar

- ✓ Notifique todas as partes afetadas
- ✓ Reponha todas as palavras-passe e IDs
- ✓ Reinstale o software, as contas sincronizadas e as cópias de segurança dos dados, conforme necessário

Atualizámos o manual de procedimentos da nossa empresa com este Plano de continuidade da atividade. Este plano *deve ser consultado e usado* por todos os colaboradores e contratantes da [[ORGANIZAÇÃO]], e estará disponível aqui [LIGAÇÃO].

Se tiver alguma dúvida sobre o nosso Plano de continuidade da atividade, não hesite em contactar-me diretamente para o debater. Na próxima semana, faremos uma breve recapitulação do que aprendemos durante este programa e, em seguida, a [ORGANIZAÇÃO] receberá oficialmente a Certificação de prontidão cibernética!

[ASSINATURA DE E-MAIL]

8

Assunto: Recapitulação da prontidão cibernética

Olá, equipa!

Concluímos a série de formação no Programa de prontidão cibernética! Vamos analisar rapidamente o que aprendemos no nosso percurso para a Prontidão cibernética.

Vídeo sobre os 4 principais problemas de cibersegurança

Vídeo do Plano de continuidade da atividade

Como sempre, não hesite em contactar-me diretamente para debater qualquer questão.

[ASSINATURA DE E-MAIL]

Módulos de formação nos 4 principais problemas de cibersegurança:

- **Palavras-passe+**
- **Atualizações de software**
- **Sensibilização para o phishing**
- **Armazenamento e partilha seguros**
- **Plano de continuidade da atividade**

PowerPoint de formação

- **Modelo de formação do CRI**

Recursos de formação partilháveis:

- Cartazes de CRI: Procura uma forma de alegrar o escritório? Quer inspirar a sua equipa? Explore a nossa coleção de cartazes de Prontidão cibernética, arte nas redes sociais e infografias para transferir e partilhar
- Guias e sugestões do CRI: Uma série de guias para saber mais sobre a MFA, relações com fornecedores externos e muito mais.
- Cartão de sugestões para phishing da CISA: Consulte este recurso fácil de partilhar da CISA com exemplos e sugestões para os colaboradores: Phishing 508 compliant 508 compliant.pdf (cisa.gov)
- Vídeo de formação sobre phishing do Mastercard Trust Center: Partilhe este vídeo do Mastercard Trust Center para formar os colaboradores sobre as melhores práticas para evitar o phishing: https://youtu.be/CVJiZIjdOOE