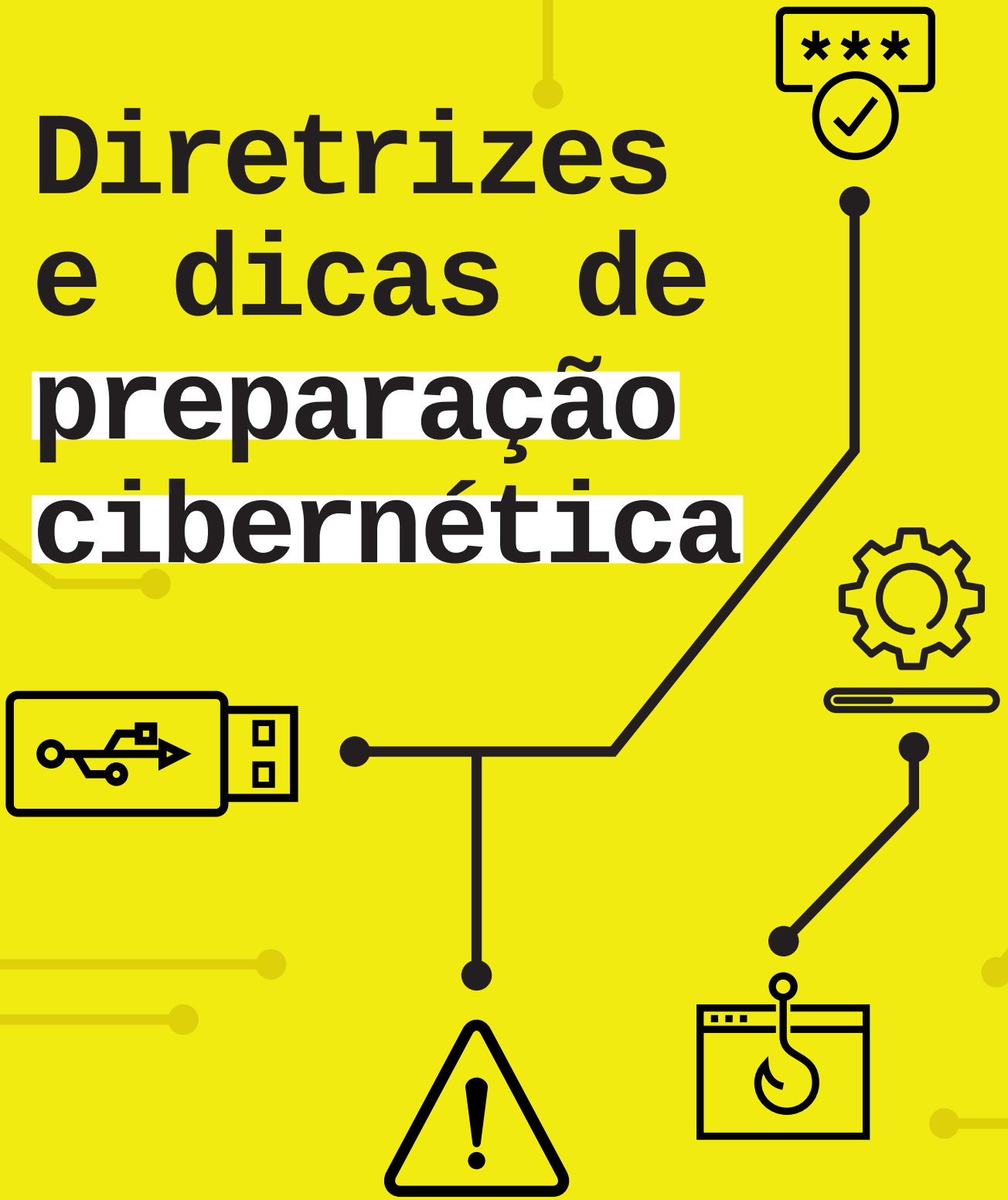
CYBER READINESS
INSTITUTE

# Diretrizes e dicas de preparação cibernética



A maioria das empresas tem diretrizes que todos os funcionários devem seguir sobre responsabilidades básicas, como chegar pontualmente ao trabalho, o que vestir no escritório ou como solicitar férias. Diretrizes sobre prontidão cibernética básica também devem ser incluídas. Afinal, a segurança dos seus dados e sistemas tem um grande impacto nos seus negócios e clientes. Recomendamos que use as dicas e diretrizes seguintes para ajudar a informar os seus funcionários e responsabilizar todos os membros da equipa para criar uma cultura de prontidão cibernética.

# Palavraspasse

**Palavras-passe fortes são essenciais para proteger os seus sistemas e contas.** Quer esteja a aceder a e-mails de trabalho, a recuperar ficheiros de um disco rígido partilhado ou a iniciar sessão em qualquer serviço online, a *frase de acesso* que usa é importante. Pode inclusivamente adicionar outra camada de segurança com autenticação de dois fatores. Esse tipo de autenticação exige que insira um código exclusivo que é enviado para o seu dispositivo móvel para cada novo inicio de sessão. A autenticação de dois fatores cria um vínculo de segurança importante entre a palavra-passe e a pessoa.

Encorajamo-lo a usar estas diretrizes para os seus funcionários:

1. Use uma frase de acesso longa com, pelo menos, 15 caracteres.Por exemplo, escolha uma frase do seu programa de TV, filme ou música favorita.

2. Nunca use a mesma frase de acesso para contas pessoais e de trabalho, e não partilhe os seus nomes de utilizador e palavras-passe com ninguém, incluindo membros da equipa.

3. Use a autenticação de dois fatores sempre que estiver disponível.

# ATualizações de software

**É fundamental manter todos os softwares e sistemas operacionais atualizados.** Cada atualização lançada pelo fornecedor do software pode incluir correções e patches importantes que protegem o software e os sistemas contra ataques. Muitas empresas designam uma pessoa para gerir as atualizações de todos os computadores da empresa, o que é preferível. Como alternativa, pode exigir que cada funcionário gira as suas próprias atualizações. De qualquer forma, as atualizações regulares são extremamente importantes.

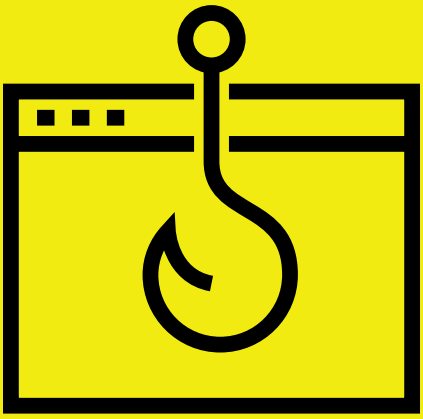
Recomendamos as seguintes diretrizes para atualizações:

1. Ligue o recurso de atualização automática em todos os dispositivos e software sempre que for oferecido.

2. Atualize regularmente todos os sistemas operativos, software e aplicações para computadores, telemóveis e tablets assim que receber uma notificação a indicar que está pronta uma atualização.

3. Verifique regularmente para garantir que todas as atualizações estão instaladas e nenhuma notificação foi perdida.

# Phishing



**Phishing é um dos problemas cibernéticos mais comuns e mais perigosos da atualidade.** Frequentemente, um e-mail de phishing pode parecer uma mensagem real e segura. Mas abri-lo pode resultar no descarregamento de vírus de software ou permitir que invasores acedam aos seus dados. Todos recebem e-mails de phishing. É por isso que é importante saber o que procurar. Sensibilizar é a melhor defesa contra phishing.

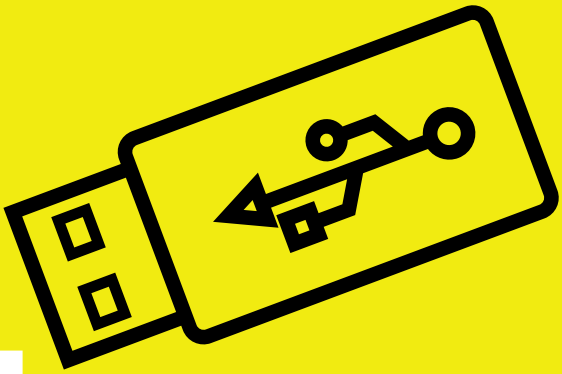
Aqui estão algumas dicas que irão ajudar:

1. Verifique o endereço de e-mail do remetente e qualquer outra informação de identificação, como logótipo da empresa, endereço e detalhes de contacto para quaisquer inconsistências ou sinais de que pode ser falso.

2. Se não estiver familiarizado com o remetente do e-mail, não clique em nenhuma ligação nem descarregue nenhum anexo do e-mail.

3. Não forneça nenhuma informação pessoal em resposta.

# USBs e unidades de armazenamento removíveis



**Pens USB são úteis para partilhar ficheiros entre computadores, mas também podem ser usadas para transmitir vírus e malware.** Não há como saber onde a pen esteve ou quem pode tê-la comprometido. A melhor maneira de evitar riscos com pens USB e outras unidades de armazenamento removíveis é evitar usá-las. No entanto, instituir uma proibição total de pens USB pode ser um desafio.

Portanto, recomendamos que todos os funcionários sigam as diretrizes abaixo:

1. Apresente alternativas a pens USB fáceis de usar, tais como serviços de partilha de ficheiros na cloud para evitar as pens USB.

2. Nunca aceite ou use um USB de um terceiro não verificado.

3. Mais importante ainda, use o bom senso. Se não sabe de onde veio a pen, não a ligue.

# Resposta a incidentes

A prontidão cibernética envolve tomar as medidas corretas para reduzir o risco, mas também estar preparado quando um incidente ocorre. Ter um plano de resposta a incidentes é uma etapa crítica para se tornar preparado para ataques cibernéticos. Pense nisso como uma simulação de incêndio: se acontecer uma emergência, é importante ter um plano em que todos sabem o seu papel.

Encontrará mais informações sobre a resposta a incidentes no Programa de Prontidão Cibernética, mas deve focar-se, no mínimo, em três áreas:

1. **Prepare-se:** Certifique-se de que todos os colaboradores criam cópias de segurança regulares do respetivo trabalho e dos dados.

2. **Atue:** Se ocorrer um ataque ou problema, desligue imediatamente o dispositivo afetado da rede da empresa. Todos os colaboradores devem ser obrigados a realizar este passo.

3. **Recupere:** Restaure os dados perdidos a partir de uma cópia de segurança, notifique todas as partes afetadas e reponha o ID e a palavra-passe do dispositivo comprometido.

PRONTO PARA LEVAR AS SUAS COMPETÊNCIAS A UM NOVO NÍVEL?

# EXPLORE O PROGRAMA DE PRONTIDÃO CIBERNÉTICA

O Programa de Prontidão Cibernética é um recurso online gratuito que descreve os passos a dar para avaliar e melhorar a sua prontidão cibernética. É fácil de usar e rastrear o seu progresso. Pode trabalhar ao seu próprio ritmo. Depois de concluído, receberá um Certificado de Prontidão Cibernética para apresentar aos clientes e fornecedores que tomou medidas para criar uma cultura de prontidão cibernética em toda a sua empresa.

Saiba mais:

BeCyberReady.com