CYBER READINESS
INSTITUTE

Hora de conversar

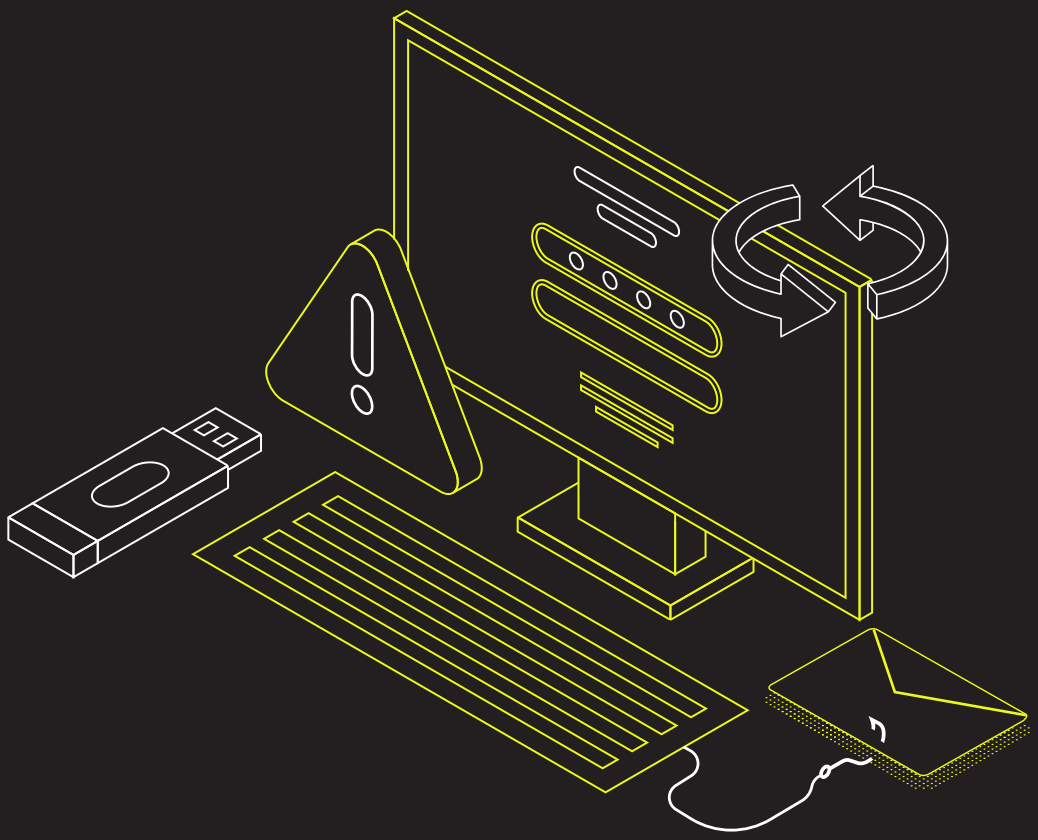
COMO FALAR
sobre prontidão com os seus funcionários

É hora de levar a preparação cibernética A SÉRIO.

A reputação da sua empresa depende disso.

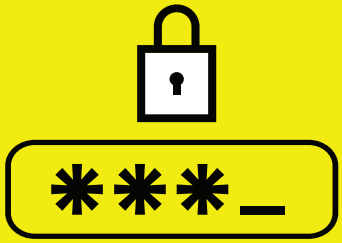
MAS COMO DEVE INICIAR
UMA CONVERSA SE NÃO FOR UM ESPECIALISTA CIBERNÉTICO?

Não precisa ser complexo ou intimidante. Consulte as perguntas e respostas neste documento para conversar com os seus funcionários sobre riscos cibernéticos, proteções e boas práticas de prontidão cibernética.



— 1 —

Palavras-passe

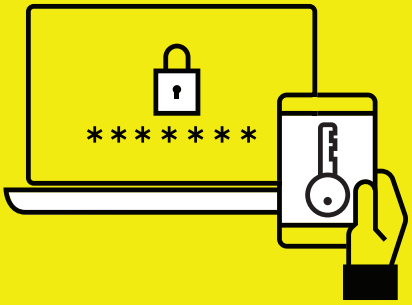


Qual é o tipo de palavra-passe mais forte?

As palavras-passe mais fortes são: frases de acesso, pensamentos aleatórios que formam uma frase. As frases de acesso devem ter, pelo menos, 15 carateres de comprimento.

Deve usar a mesma palavra-passe para fins comerciais e pessoais?

Não, não repita as palavras-passe sempre que possível.

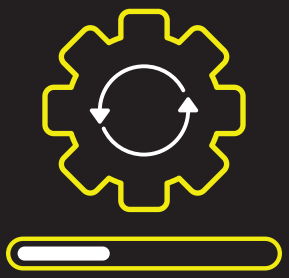


O que é autenticação de dois fatores?

A autenticação de dois fatores é uma forma de confirmar a sua identidade através da sua palavra-passe e também de outro método, como mensagem de texto ou e-mail. A autenticação de dois fatores é fácil de configurar e reduz significativamente as probabilidades de ser hackeado.

— 2 —

Atualizações



O que são atualizações?

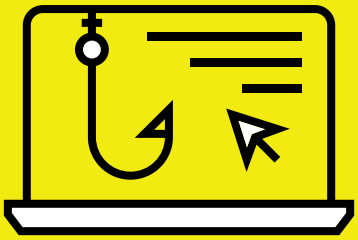
Simplificando, “atualizações” são novas versões de software e aplicações no seu telemóvel e computador. Estas atualizações corrigem problemas e aumentam a segurança. A instalação de atualizações é uma das medidas de prontidão cibernética mais fáceis e críticas que pode tomar.

Como pode garantir que os seus dispositivos estão atualizados?

Ative as notificações de atualização automática e não ignore as notificações de atualização. Lembre-se também de verificar se há atualizações em aplicações de terceiros.

— 3 —

Phishing



O que é phishing?

Phishing é um ataque cibernético enviado através de um e-mail falso. Os ataques de phishing tentam usar a sua conta para roubar dados pessoais ou assumir o controlo do seu computador. Estes ataques costumam ser difíceis de detetar.

Quais são os sinais comuns de uma tentativa de phishing?

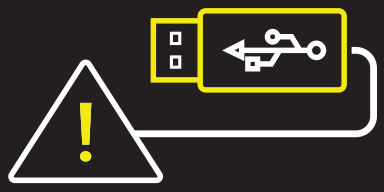
- Endereço de e-mail suspeito
- E-mails de estranhos que incluem anexos ou ligações
- Erros de ortografia ou frases quebradas
- E-mails suspeitos que pedem dados pessoais

Por que é necessário estar ciente dos riscos de phishing?

91 % de todos os ataques cibernéticos começam com um e-mail de phishing. 81 % das empresas que são alvo de um ataque de phishing perdem clientes.

— 4 —

USBs



Qual o problema com as pens USB?

Mais de ¼ de vírus por malware começam com uma pen USB infetada. Para além disso, 87% dos funcionários relatam a perda de uma pen USB e não informaram os seus empregadores.

De que forma pode limitar os ataques por USB?

Não use
pens USB, a menos que sejam aprovadas pelo seu líder cibernético

Nunca use
ou aceite uma pen USB de qualquer pessoa ou empresa externa

Se usadas,
as pens USB devem ser verificadas regularmente para detetar um possível malware

CYBER READINESS
INSTITUTE