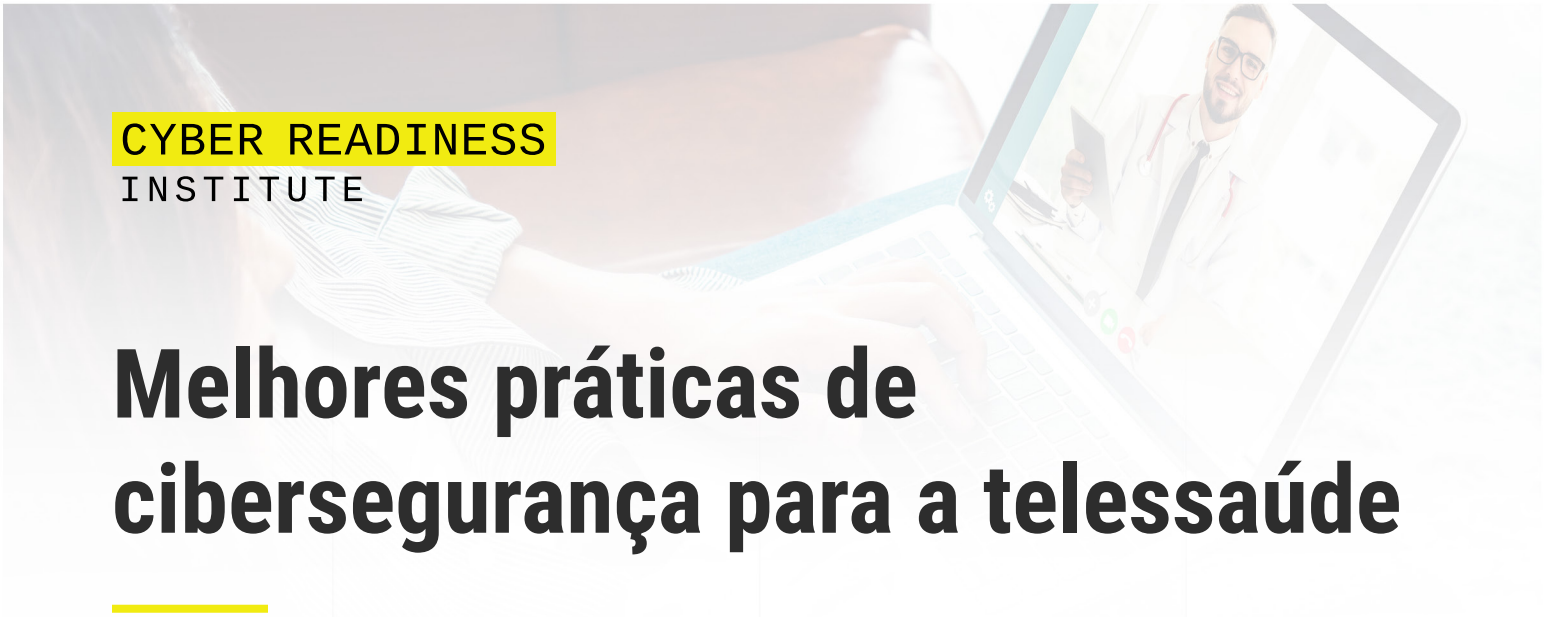
CYBER READINESS
INSTITUTE



Melhores práticas de cibersegurança para a telessaúde

O panorama dos cuidados de saúde está diferente, agora que passaram oito meses. A telessaúde está mais prevalecente do que nunca e existem novas políticas a compreender e implementar na sua prática. Não obstante todas estas mudanças, uma questão permanece: existe uma grande quantidade de informações pessoalmente identificáveis, sensíveis e confidenciais integradas no nosso sistema de cuidados de saúde.

As perguntas de acesso e a segurança foram sempre importantes, especialmente quando as práticas começaram a passar aos registos clínicos eletrónicos. Com a telessaúde cada vez mais popular, nunca foi tão importante garantir que o seu espaço de saúde compreende e implementa comportamentos básicos de higiene cibernética para proteger dados de pacientes e empresas. Criar uma cultura de preparação cibernética no seu espaço, além de reduzir o risco de ataques informáticos, também o prepara e equipa melhor com as ferramentas certas, se e quando sofrer um ataque. Ao focar-se no comportamento humano e indicar uma pessoa de contacto, ou um "Líder cibernético", no seu espaço, o Cyber Readiness Institute encoraja-o a focar-se na educação e sensibilização como primeira linha de defesa e oportunidade de resiliência.

Os hackers aproveitam-se da lacunas na segurança da telessaúde para fazer ataques direcionados a clínicas vulneráveis. Estudos apuraram que, entre março e abril deste ano, os alertas de segurança enviados para departamentos de tecnologias da informação em 148 sistemas anfitrião das mais populares aplicações de telessaúde aumentaram 30 % a nível global face ao mesmo período do ano anterior.

Com a popularidade crescente da telessaúde, registou-se um aumento correspondente em ataques direcionados, incluindo um aumento de 117 % em alertas de segurança causado exclusivamente por problemas de malware.

Em termos de telessaúde, ter uma base forte nos aspetos essenciais, como palavras-passe, atualizações de software, phishing e uso de USB, será enormemente benéfico na adaptação ao seu espaço ao novo "ambiente de telessaúde".

guide@cyberreadinessinstitute.com

Boas práticas

Familiarize-se com a telessaúde, porque veio para ficar

- Reconheça que a conveniência da telessaúde a torna atrativa para os pacientes
- Saiba como as emergências de saúde pública declaradas mudam os protocolos de telessaúde (por exemplo, em reembolsos, licenças entre estados ou regulamentos HIPAA)

Seja proativo em vez de reativo

- Crie um plano de resposta a incidentes, pratique-o e divulgue-o junto dos colaboradores e colegas [Aceda a **BeCyberReady.com** para saber como criar um plano de resposta a incidentes]

Seja consistente com a sua plataforma de telessaúde selecionada em todo o espaço

- Saiba quais as plataformas de telessaúde com conformidade HIPAA
- Priorize as suas necessidades e dúvidas, bem como as dos pacientes, na avaliação de opções
- Garanta uniformização e transparência

Conheça os aspetos básicos da higiene cibernética

- Palavras-passe: Ative a autenticação multifator e use frases de acesso com 15 ou mais carateres
- Atualizações de software: Ative as atualizações automáticas
- Phishing: Realize testes de phishing de rotina e mostre aos colaboradores como são as tentativas de phishing
- USB: Use partilhas de ficheiros online em vez de USB

Esteja ciente, alerta e pronto para a cibernética.

Sobre o CRI

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para a partilha de recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). Explore os blocos de construção de uma boa segurança cibernética com o nosso Kit de iniciação ou crie uma cultura de preparação cibernética na sua empresa com o Programa de preparação cibernética online. Os nossos recursos de teletrabalho e guias de local de trabalho híbrido oferecem sugestões oportunas para lidar com a evolução dos desafios cibernéticos da atualidade. Para saber mais, visite www.BeCyberReady.com.