CYBER READINESS
INSTITUTE

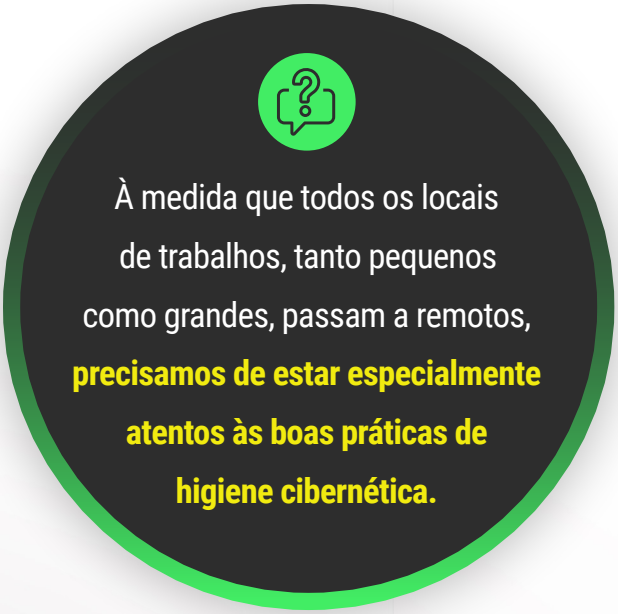
Proteger uma força de trabalho remota

Os próximos meses irão trazer desafios a quase toda a população mundial dado que as rotinas normais foram alteradas pelo coronavírus. As crianças e os professores irão colaborar de forma remota, os trabalhadores irão realizar o seu trabalho a partir de casa e os empresários irão gerir as suas empresas a partir da sala de estar, em vez da sala da administração.

Temos sorte pelo facto de as tecnologias avançadas de hoje permitirem que muitos de nós continuem a trabalhar com poucas perturbações. A disponibilidade de potência informática económica, o acesso aos serviços na nuvem e as ligações à Internet de alta velocidade tornam o teletrabalho uma alternativa viável que pode ajudar a abrandar esta crise sanitária mundial.

Mas à medida que mais pessoas se juntam à força de trabalho remota, é necessário estarmos cientes de que estamos expostos a outros riscos. À medida que todos os locais de trabalhos, tanto pequenos como grandes, passam a remotos, precisamos de estar especialmente atentos às boas práticas de higiene cibernética.

Eis alguns passos críticos que todos nós podemos seguir para proteger a nossa segurança online.



guide@cyberreadinessinstitute.org

As noções básicas

Palavras-passe

As palavras-passe continuam a ser a primeira linha de defesa no acesso a aplicações e dados essenciais. O trabalho remoto acrescenta a complexidade de depender da segurança da rede doméstica de todos os colaboradores.

- Certifique-se de que a palavra-passe do router doméstico não pode ser facilmente adivinhada e não inclua o seu endereço ou nomes pessoais.
- Sempre que possível ative a autenticação multifator (palavra-passe + um outro requisito, como uma mensagem de texto), incluindo o acesso a dados essenciais em aplicações na nuvem usadas para partilha de dados e documentos.

Patches

Os patches de segurança do sistema operativo devem ser aceites e permanecer atualizados.

- Exija aos colaboradores que tenham os seus sistemas operativos definidos para atualização automática.
- Relembre semanalmente os colaboradores para que aceitam todos os patches de segurança relevantes.

Phishing

Quanto mais de nós ficarem online nas próximas semanas, mais podemos esperar um aumento dos esquemas online, da engenharia social e das tentativas de phishing. Os hackers e os cibercriminosos irão seguramente utilizar as preocupações com a disseminação do vírus e o desejo insaciável de notícias para enganar as pessoas.

- Passe sempre com o rato sobre o nome do remetente do e-mail para determinar a verdadeira origem do mesmo e assegurar que o seu nome não é fraudulento.
- A maioria dos e-mails de ransomware individuais são falsos. Se puder, certifique-se de que um profissional de segurança verifica os e-mails antes de responder.
- Todas as empresas devem identificar um ponto de contacto no interior da empresa que os colaboradores poderão contactar se receberem um e-mail de phishing ou ransomware individual. Esta sensibilização e comunicação irá informar os colaboradores das táticas atuais dos agentes maliciosos.

Distanciamento social

O distanciamento social também funciona online.

- Limite a quantidade de dados pessoais que partilha nas redes sociais para reduzir o seu panorama de ameaça.
- Partilhe todos os dados através de aplicações seguras na nuvem. As pens USB não devem ser utilizadas para partilhar dados, visto que podem propagar malware.