CYBER READINESS
INSTITUTE

A Manter Docentes e Alunos Seguros

Os docentes e alunos do nosso país estão em território desconhecido à medida que a aprendizagem remota passa a ser a norma do sistema educativo em todo o país. A aprendizagem remota oferece oportunidades tremendas que não poderíamos ter imaginado há 30-40 anos atrás.

Para os docentes significa que a sua missão pode continuar. Para os alunos (e pais), significa que a sala de aula não tem limites e que um sentido ajustado de normalidade pode existir nestes tempos incertos.

Temos sorte pelo facto das tecnologias avançadas de hoje permitirem que docentes e alunos continuem a trabalhar juntos. Também significa que precisamos de tomar precauções para garantir que todos estejamos protegidos.

Existem alguns passos fáceis que os docentes podem seguir para salvaguardar a sua segurança online e a dos seus alunos.

O básico

Palavras-passe / frases de acesso

As palavras-passe / frases de acesso continuam a ser a melhor maneira de bloquear dados pessoais e aplicações. O ensino remoto também significa que todos precisamos de nos concentrar em proteger as nossas redes domésticas.

- Certifique-se de que a palavra-passe / frase de acesso do seu router doméstico não é facilmente adivinhada e não inclua o seu endereço ou nomes pessoais (as frases de acesso são mais seguras do que palavras-passe).
- Permita a autenticação multifator (palavra-passe / frases de acesso + outro requisito, como uma mensagem de texto) para acesso a dados críticos em aplicações na nuvem, o que é importante para a partilha de dados e documentos com os seus alunos.

guide@cyberreadinessinstitute.com

Patches

Os patches de segurança do sistema operativo devem ser aceites e manter-se atualizados.

- Certifique-se de que os seus sistemas operativos estão configurados para atualização automática.
- Aceite todos os patches de segurança relevantes semanalmente.

Phishing

- Quanto mais ficarmos online nas próximas semanas, mais podemos esperar um aumento das burlas online, engenharia social e ataques de phishing. Hackers e criminosos certamente usarão as preocupações com a disseminação do vírus e o desejo insaciável de notícias para enganar as pessoas.
- Use linhas de assunto consistentes com os seus alunos para que eles possam validar mais facilmente que os e-mails são seus.
- Passe sempre o rato sobre o nome do remetente do e-mail para determinar a verdadeira origem do mesmo.
- Chame a atenção dos seus alunos para prestarem atenção ao nome e ao e-mail do remetente.

Uso de USB

Com todos em trabalho remoto, somos tentados a usar USBs ou dispositivos de armazenamento removíveis para transferir informações - de um computador escolar para um computador doméstico.

- Consulte a sua escola ou agrupamento quanto à subscrição a um fornecedor de armazenamento de dados na nuvem para poder aceder a documentos e partilhá-los com os seus alunos de maneira segura.
- Não use USBs. Frequentemente, estão infetados com malware que pode danificar o seu computador.

Aplicações de vídeo e de conversas

- Pode não ter a opção de escolher a plataforma de vídeo que usa porque as escolas têm grandes contratos com fornecedores. Quando possível, solicite uma plataforma / aplicação de comunicação encriptada e segura.
- Chame a atenção dos seus alunos para bloquearem o vídeo e o áudio, desativando essas funções quando não as utilizarem. Também pode tapar a câmara de vídeo com um pedaço de fita adesiva ou um diapositivo.
- Confirme se conhece a pessoa que está a tentar falar consigo.

Como facilitar as coisas para os seus alunos

Ensine aos seus alunos o "ABC" da boa higiene cibernética:

A – Autentique as suas contas com frases de acesso fortes.

B – Cuidado com as tentativas de phishing e ajude os alunos a verificar se é o remetente do e-mail.

C – Avise os alunos para usarem a aplicação de vídeo só quando VIREM o seu nome no ecrã.