CYBER READINESS
INSTITUTE

Mantener seguros a educadores y estudiantes

Los educadores y estudiantes de nuestra nación se encuentran en un territorio inexplorado, ya que el aprendizaje remoto se convierte en la norma para los sistemas escolares de todo el país. El aprendizaje remoto presenta enormes oportunidades que no podríamos haber imaginado hace 30 o 40 años.

Para los profesores, implica que su misión puede continuar. Para los estudiantes (y los padres), supone que el aula no tiene límites y puede existir un sentido ajustado de normalidad en estos tiempos de incertidumbre.

Tenemos la suerte de que las tecnologías avanzadas de hoy en día permitirán a profesores y estudiantes seguir trabajando juntos. También significa que debemos tomar precauciones para garantizar que todos estemos protegidos.

Existen algunas medidas sencillas que los profesores pueden adoptar para proteger su seguridad en línea y la de sus estudiantes.

Aspectos básicos

Contraseñas/frases de contraseña

Las contraseñas/frases de contraseña siguen siendo la mejor manera de bloquear aplicaciones y datos personales. La enseñanza a distancia también significa que todos debemos centrarnos en proteger nuestras redes domésticas.

- Asegúrese de que la contraseña/frase de contraseña de su rúter doméstico (las frases de contraseña son más seguras que las contraseñas) no se pueda adivinar con facilidad y no incluya su dirección o nombres personales.
- Habilite la autenticación de múltiples factores (contraseña/frase de contraseña + otro requisito, como un mensaje de texto) para acceder a datos esenciales en aplicaciones en la nube, lo cual es importante para compartir datos y documentos con sus estudiantes.

guide@cyberreadinessinstitute.com

Parches

Los parches de seguridad del sistema operativo deben aceptarse y mantenerse actualizados.

- Asegúrese de que sus sistemas operativos estén configurados para actualizarse de forma automática.
- Acepte todos los parches de seguridad pertinentes semanalmente.

Phishing

- Cuantos más de nosotros estemos en línea durante las próximas semanas, más podremos esperar un aumento de las estafas en línea, la ingeniería social y los ataques de phishing. Los piratas informáticos y los delincuentes seguramente aprovecharán la preocupación sobre la propagación del virus y el deseo insaciable de noticias para engañar a la gente.
- Utilice líneas de asunto coherentes con sus alumnos para que puedan validar con más facilidad que los correos electrónicos son suyos.
- Coloque siempre el ratón sobre el nombre del remitente del correo electrónico para determinar el verdadero origen del remitente.
- Recuerde a sus alumnos que presten mucha atención al nombre y al correo electrónico del remitente.

Utilización del USB

Puesto que todo el mundo trabaja de forma remota, nos sentimos tentados a utilizar unidades USB o multimedia extraíbles para transferir información, desde un ordenador de la escuela a uno doméstico.

- Pregunte a su escuela o distrito por su suscripción a un proveedor de almacenamiento de datos basado en la nube para poder acceder a los documentos y compartirlos con sus alumnos de forma segura.
- No utilice unidades USB. Suelen estar infectados de malware que puede dañar su ordenador.

Aplicaciones de vídeo y chat

- Es posible que no tenga la opción de elegir la plataforma de vídeo que utiliza porque las escuelas participan en grandes contratos con proveedores. Cuando sea posible, solicite una plataforma/aplicación de comunicaciones cifradas y seguras.
- Recuerde a sus alumnos —y a usted mismo— que deben bloquear el vídeo y el audio desactivando estas funciones cuando no estén en uso. También puede bloquear la cámara de vídeo con un trozo de cinta adhesiva gruesa.
- Asegúrese de conocer a la persona que está tratando de chatear por vídeo con usted.

Cómo ponérselo fácil a sus estudiantes

Enseñe a sus alumnos el “ABC” de una buena higiene cibernética:

A – Autentique sus cuentas mediante el uso de frases de contraseña seguras.

B – Tenga cuidado con los intentos de phishing y ayude a los estudiantes a verificar que usted es el remitente del correo electrónico.

C – Advierta a los alumnos que utilicen la aplicación de vídeo solo si VEN que el nombre que aparece llamando en la pantalla es el suyo.