Welcome to Las Vegas!

As this weekend has commenced and thousands travel in for the big game, cyber threats are lurking. One of the best defenses against a hack is to adopt good cyber hygiene.

Verizon Business has six tips that can help you better defend yourself from a cyber breach attempt and help keep your work intact:

1. **Keep your technology with you at all times.** Don’t leave any computers, phones, tablets or USB drives unattended.

2. **Update your software**. Keep all software, operating systems and applications up to date with the latest security patches as soon as they’re available.

3. **Use multi-factor authentication.** This extra step keeps threat actors out and can save you and your organization from a major issue.

4. **Don’t fall victim to social engineering.** If a message looks suspicious, it’s often is a phishing attempt. Don’t click on any links and report the message as spam.

5. **Don’t share sensitive information over public WiFi.** Instead, consider using a personal hotspot or 5G network service when working or sharing any sensitive data.

6. **Follow your organization’s incident response plan.** In case you fall victim to a breach, make sure you know the steps of your organization’s incident response plan and follow them accordingly.

Learn more about how you can help better secure your data and help address cyber attacks against your organization with the QR code.

verizon business

¡Bienvenidos a Las Vegas!

A medida que comienza este fin de semana y miles de personas viajan para asistir al gran partido, las amenazas cibernéticas acechan. Una de las mejores defensas contra un hackeo es adoptar una buena higiene cibernética.

Verizon Business tiene seis consejos que pueden ayudarte a defenderte mejor de un intento de vulneración cibernética y a mantener tu trabajo intacto:

1. **Mantenga los dispositivos con usted en todo momento.** No deje sin vigilancia las computadoras, los teléfonos, las tabletas o las unidades USB.

2. **Actualice su software.** Mantenga todo el software, los sistemas operativos y las aplicaciones actualizados con los últimos parches de seguridad tan pronto como estén disponibles.

3. **Utilice autenticación de múltiples factores.** Este paso adicional mantiene alejados a los actores de amenazas y puede salvarlo a usted y a su organización de un problema importante.

4. **No sea víctima de la ingeniería social.** Si un mensaje parece sospechoso, a menudo se trata de un intento de phishing. No haga clic en ningún enlace y reporte el mensaje como spam.

5. **No comparta información confidencial a través de redes Wifi públicas.** En su lugar, considere utilizar un punto de acceso personal o un servicio de red 5G cuando trabaje o comparta datos confidenciales.

6. **Siga el plan de respuesta a incidentes de su organización.** En caso de que sea víctima de una filtración, asegúrese de conocer los pasos del plan de respuesta a incidentes de su organización y sígalos en consecuencia.

Obtenga más información sobre cómo puede ayudar a proteger mejor sus datos y ayudar a abordar los ataques cibernéticos contra su organización con el código QR.

verizon business