Comunicado de Prensa

Para Comunicación Inmediata
04/08/2020
Información de los casos del condado de Rowan: https://bit.ly/rowan-covid19-map

COVID 19 Información de contacto
Sitio Web:www.rowancountync.gov/covid-19
Correo Electrónica :covid-19@rowancountync.gov
Teléfono: 980-432-1800

Los parques del condado de Rowan cierran las pistas de tenis

El condado de Rowan cerrará sus canchas de tenis en el Parque Dan Nicholas y en el Parque Ellis a partir del 8 de abril de 2020 a las 5:00 PM por recomendación de la Asociación de Tenis de los Estados Unidos.

La Asociación de Tenis de EE.UU. (USTA) compartió, *"Aunque no hay estudios específicos sobre el tenis y COVID-19, los asesores médicos creen que existe la posibilidad de que el virus responsable de COVID-19 pueda ser transmitido a través de compartir y manejar en común pelotas de tenis, mangos de puertas, bancos, postes de red e incluso superficies de canchas.*

Como resultado de esto, la USTA pide que como jugadores de tenis tengamos paciencia al volver a las canchas y consideremos cómo nuestras decisiones no sólo nos afectarán a nosotros mismos, sino también cómo nuestras decisiones pueden impactar en nuestras comunidades más amplias. Mientras tanto, animamos a todos a mantenerse activos y sanos con el ejercicio en casa y variaciones creativas de "tenis en casa"." Las ideas para "tenis en casa" se pueden encontrar en el sitio web de Net Generation USTA.

Concienciación sobre seguridad cibernética durante COVID-19

Las agencias de seguridad nacional están viendo un uso creciente de los temas relacionados con COVID-19 por parte de actores cibernéticos malintencionados. Al mismo tiempo, el aumento del teletrabajo ha incrementado el uso de servicios potencialmente vulnerables, como las redes privadas virtuales (VPN), lo que amplifica las amenazas para los individuos y las organizaciones como:

- Phishing (suplantación de identidad), utilizando el tema del coronavirus o COVID-19 como señuelo,
- Distribución de malware (software malicioso), usando señuelos temáticos del coronavirus o COVID-19,
- El registro de nuevos nombres de dominio que contengan palabras relacionadas con el coronavirus o COVID-19, y
- Ataques contra la infraestructura de acceso remoto y teletrabajo de reciente y a menudo rápida implantación.

Phishing
Las estafas de phishing consisten en correos electrónicos fraudulentos que afirman ser de empresas de renombre para atraer a los individuos a revelar información personal. Los organismos de seguridad nacional han observado un gran volumen de campañas de phishing con líneas de asunto como:

- Actualizaciones de Coronavirus 2020,
- Actualizaciones de Coronavirus,
- 2019-nCov: Nuevos casos confirmados en su ciudad, y
- 2019-nCov: Brote de virus de la coronación en su ciudad (Emergencia).

Estos correos electrónicos o mensajes de texto contienen una llamada a la acción, animando a la víctima a visitar un sitio web que actores cibernéticos malintencionados utilizan para robar datos valiosos, como nombres de usuario y contraseñas, información de tarjetas de crédito y otros datos personales.

Robo de credenciales
Ha habido un aumento en el phishing relacionado con COVID-19 para robar credenciales de usuario. Si el usuario hace clic en el hipervínculo, aparece una página web de inicio de sesión falsa que incluye un formulario de introducción de contraseña. Si la víctima introduce su contraseña en la página falsificada, los atacantes podrán acceder a las cuentas en línea de la víctima, como su buzón de correo electrónico. Este acceso puede utilizarse para adquirir información personal o sensible, o para enviar correos electrónicos de phishing utilizando la libreta de direcciones de la víctima.

Vulnerabilidad del teletrabajo
Muchos ciudadanos están trabajando a distancia durante este tiempo. Los ciberdelincuentes malintencionados se aprovechan de una variedad de vulnerabilidades conocidas públicamente en las VPN y otras herramientas y software de trabajo remoto. Los atacantes han podido secuestrar teleconferencias y aulas en línea que se han establecido sin controles de seguridad (por ejemplo, contraseñas) o con versiones sin parches del software de la plataforma de comunicaciones. La exigencia de contraseñas y la estrecha vigilancia de las listas de participantes pueden ayudar a reducir las posibilidades de ataque.

Cómo proteger sus datos
La guía de correo electrónico sospechoso del Centro Nacional de Seguridad Cibernética (NCSE) explica qué hacer si ya ha hecho clic en un correo electrónico, archivo adjunto o enlace potencialmente malicioso. Proporciona consejos sobre a quién contactar si su cuenta o dispositivo ha sido comprometido y algunas de las medidas de mitigación que puede tomar, como cambiar sus contraseñas. También ofrece los principales consejos del NCSC para detectar un correo electrónico de phishing:

- Autoridad - ¿El remitente afirma ser de alguien oficial (por ejemplo, su banco o su médico, un abogado, un organismo gubernamental)? Los criminales a menudo

pretenden ser personas u organizaciones importantes para engañarte para que hagas lo que ellos quieren.

- Urgencia - ¿Le dicen que tiene un tiempo limitado para responder (por ejemplo, en 24 horas o inmediatamente)? Los delincuentes suelen amenazarle con multas u otras consecuencias negativas.
- Emoción - ¿El mensaje te hace sentir pánico, miedo, esperanza o curiosidad? Los delincuentes suelen utilizar un lenguaje amenazador, hacer falsas reclamaciones de apoyo o intentar burlarse de usted para que quiera saber más.
- Escasez - ¿El mensaje ofrece algo que escasea (por ejemplo, entradas para un concierto, dinero o una cura para enfermedades)? El miedo a perder un buen negocio u oportunidad puede hacer que respondas rápidamente.

###

El registro público de este comunicado de prensa está disponible en www.rowancountync.gov/COVID-19