



Media Release

For Immediate Release

04/08/2020

Rowan County Case Information:
<https://bit.ly/rowan-covid19-map>

COVID-19 information contacts

Website: www.rowancountync.gov/covid-19

Email: covid-19@rowancountync.gov

Phone: 980-432-1800

Rowan County Parks Closes Tennis Courts

Rowan County will close its tennis courts at Dan Nicholas Park and Ellis Park beginning April 8, 2020 at 5:00 PM after recommendation from US Tennis Association.

US Tennis Association (USTA) shared, *"Although there are no specific studies on tennis and COVID-19, medical advisors believe there is the possibility that the virus responsible for COVID-19 could be transmitted through common sharing and handling of tennis balls, gate handles, benches, net posts and even court surfaces.*

As a result of this, the USTA asks that as tennis players we need to be patient in our return to the courts and consider how our decisions will not only affect ourselves, but how our decisions can impact our broader communities. In the meantime, we encourage everyone to stay active and healthy with at-home exercise and creative "tennis-at-home" variations." Ideas for "tennis-at-home" can be found on [Net Generation USTA's website](#).

Cybersecurity Awareness During COVID-19

National security agencies are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying threats to individuals and organizations such as:

- Phishing, using the subject of coronavirus or COVID-19 as a lure,
- Malware distribution, using coronavirus- or COVID-19- themed lures,
- Registration of new domain names containing wording related to coronavirus or COVID-19, and
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

Phishing

Phishing scams involve fraudulent emails claiming to be from reputable companies to entice individuals to reveal personal information. National security agencies have observed a large volume of phishing campaigns with subject lines like:

- 2020 Coronavirus Updates,
- Coronavirus Updates,



- 2019-nCov: New confirmed cases in your City, and
- 2019-nCov: Coronavirus outbreak in your city (Emergency).

These emails or text messages contain a call to action, encouraging the victim to visit a website that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information, and other personal information.

Credential Theft

There has been an increase in COVID-19-related phishing to steal user credentials. If the user clicks on the hyperlink, a spoofed login webpage appears that includes a password entry form. If the victim enters their password on the spoofed page, the attackers will be able to access the victim's online accounts, such as their email inbox. This access can then be used to acquire personal or sensitive information, or to send phishing emails using the victim's address book.

Teleworking Vulnerability

Many citizens are working remotely during this time. Malicious cybercriminals are taking advantage by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. Attackers have been able to hijack teleconferences and online classrooms that have been set up without security controls (e.g., passwords) or with unpatched versions of the communications platform software. Requiring passwords and closely monitoring participant lists can help reduce chances of attack.

How to Protect Your Data

The National Cyber Security Centre's (NCSE) [suspicious email guidance](#) explains what to do if you've already clicked on a potentially malicious email, attachment, or link. It provides advice on who to contact if your account or device has been compromised and some of the mitigation steps you can take, such as changing your passwords. It also offers NCSC's top tips for spotting a phishing email:

- **Authority** – Is the sender claiming to be from someone official (e.g., your bank or doctor, a lawyer, a government agency)? Criminals often pretend to be important people or organizations to trick you into doing what they want.
- **Urgency** – Are you told you have a limited time to respond (e.g., in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** – Does the message make you panic, fearful, hopeful, or curious? Criminals often use threatening language, make false claims of support, or attempt to tease you into wanting to find out more.
- **Scarcity** – Is the message offering something in short supply (e.g., concert tickets, money, or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

###