CYBER READINESS
INSTITUTE

Staying Healthy and Cyber Secure with Telehealth

The COVID-19 pandemic has spurred a dramatic increase in telehealth and accompanying that surge, has been an equally dramatic increase in cyber attacks, according to a new report from cybersecurity ratings firm Security Scorecard and dark web research company DarkOwl.

Individuals and families are grappling with social distancing, stay-at-home guidelines, remote schooling, and other pandemic-related recommendations. At the same time, the need to see a healthcare provider has taken on increased importance, difficulty, and new meaning. With these conditions, the popularity of telehealth use has jumped but individuals and patients need to assess their readiness to remain secure, cybersecure. This task may seem daunting but there are some basic actions people can take for themselves and with their healthcare providers to retain the convenience and benefits of telehealth while increasing their cybersecurity.

Patients are consumers of telehealth and should approach telehealth with a strong awareness of cyber readiness fundamentals. As a patient, you need to be aware that you are sharing important confidential information, which needs to be protected, with your healthcare provider. Engaging in this type of online interaction with your healthcare provider creates a shared responsibility for reducing vulnerabilities to you, your family, and your healthcare provider's network. Hackers are targeting patient usage of telehealth as a gateway to compromise doctors' offices, insurance companies, and even your personal and business data. Like most human interactions, your use of telehealth is only as secure as the weakest link, and each link needs to be as informed as possible about vulnerabilities and threats. **The following actions will help you prepare to use telehealth for staying healthy and more cybersecure.**

Things to do

Be Aware, and Prepare

Familiarize yourself with telehealth and its benefits for you and your family:

- According to recent research done by the Cyber Readiness Institute (CRI), 45% of people surveyed who have used telehealth during the pandemic will continue to do so "once things return to normal." So, telehealth is here to stay.
- According to the same CRI research, individuals using telehealth in 2020 have improved their cybersecurity by changing passwords, updating their software, deleting suspicious emails, and adding virus protection.
- Use a different password for your telehealth log-in than you do for your other personal or work access. Ideally, it should be a passphrase of 15 characters or more.
- Review the CRI Starter Kit at **www.BeCyberReady.com** to strengthen your awareness of basic cybersecurity behaviors, AND examine how you are protecting your own cybersecurity.
- Ask your healthcare insurance provider about telehealth coverage.
- Prepare for a conversation with your healthcare provider about telehealth.

Be Proactive

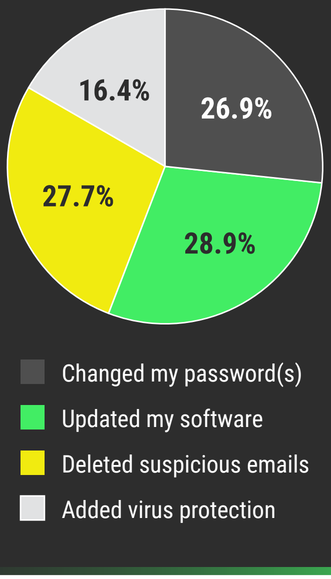
Discuss telehealth security with your healthcare provider:

- "Do you have a staff member who is responsible for addressing all telehealth issues?"
- "Do you conduct cybersecurity training with your staff?"

Understand your healthcare provider's use of telehealth and how it might affect you:

- "Is my telehealth appointment covered by my insurance and are there any deductibles and co-pays?"
- "Do you use a private internet connection when conducting my telehealth visit?"
- "Do you have cyber insurance coverage for your practice?"
- "Is the telehealth system you use HIPAA compliant?"

#Cybersecurity Poll: If you used telehealth this year, have you done any of the following options to improve your cybersecurity? If so, select what was most important to you.



About CRI

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit www.BeCyberReady.com.