# Doctors: Protect your home devices from COVID-19 cyber scams

APR 17, 2020

**Andis Robeznieks**
Senior News Writer

**What's the news:** A cybersecurity resource, developed jointly by the AMA and American Hospital Association (AHA), gives guidance on protecting remote workplaces as many physicians are working from home to care for patients during the COVID-19 pandemic.

The resource, "Working from home during the COVID-19 pandemic," tells physicians about immediate steps they can take to quickly strengthen home or hospital-based computers, networks and medical devices from the rise in COVID-19-themed security threats and attacks. The resource includes checklists, sources, tips and advice on bolstering protections to keep pace with deceptive cyberattacks that could disrupt patient care or threaten medical records.

"For physicians helping patients from their homes and using personal computers and mobile devices, the AMA and AHA have moved quickly to provide a resource with important steps to help keep a home office resilient to viruses, malware and hackers," said AMA President Patrice A. Harris, MD, MA.

**Why it's important:** Cybersecurity is a patient-safety issue.

Telemedicine technology has given physicians and care teams the power to do much of what they could accomplish in a medical office while ensuring care to those who need it. Telemedicine also offers patients convenience and safety by supporting physical-distancing measures. But vigilance is required as cybercriminals find health data an enticing target and measures need to be taken to protect it.

The FBI reports that its Internet Crime Complaint Center has already received more than 1,200 complaints related to COVID-19 scams. These include phishing campaigns against first responders, deploying ransomware at medical facilities and launching "Distributed Denial of Service," or DDoS, attacks that disrupt online service by overwhelming a system with traffic from multiple sources.

In one scheme, cybercriminals sought to trick online readers into clicking on a link that appeared to be

a map showing the distribution of COVID-19 cases but was actually a website that infects visitors with an information-stealing program.

“Based on recent trends, the FBI assesses these same groups will target businesses and individuals working from home via telework software vulnerabilities, education technology platforms, and new business email compromise schemes,” an FBI warning states.

**To learn more:** Physicians who believe they are the victim of an internet scam or cybercrime—or those who want to report suspicious activity—can visit the FBI Internet Crime Complaint Center.

The cybersecurity guide is the latest addition to a growing inventory of essential tools and resources the AMA has produced as the COVID-19 pandemic and its impact evolves. Clinical information, guides, updates on AMA advocacy and guidance on medical ethics can be found at the AMA COVID-19 Resource Center.