Online scammers target doctors amid COVID-19. How to stay safe.

APR 24, 2020

Tanya Albert Henry
Contributing News Writer

COVID-19 has required many physicians to see patients via telehealth and communicate with co-workers through email instead of face-to-face, making it fertile new ground for con artists who target their prey online.

Scammers have specifically targeted physicians and other health professionals during the pandemic and with the threat not going away any time soon, physicians must be extra vigilant, experts say. The FBI recently issued a warning that they have fielded more than 1,200 complaints to its internet crime complaint center specifically related to COVID-19.

The AMA and the American Hospital Association (AHA) compiled a comprehensive cybersecurity resource—"Working from home during the COVID-19 pandemic"—to guide physicians on protecting remote workplaces.

And for a limited time, AMA members receive even greater savings—40% off—on identity-theft protection from Aura, Identity Guard through AMA Member Benefits PLUS.

The service continuously scours information in the darkest corners of the web and alerts you to, among other things, high-risk transactions that indicate identity theft, such as account takeovers; a presence of your social security number, credit card numbers, financial account numbers, health insurance numbers and other vulnerable information on the dark web. All plans also include $1 million for stolen funds reimbursement.

The best defense for scams, though, is vigilance and a healthy dose of critical thinking and skepticism, says Sharma Upadhyayula, head of product engineering and operations at Aura, Identity Guard.

"A lot can be prevented by simple basic things we oftentimes ignore because of convenience, such as creating strong password, setting up different passwords for different accounts and running virus

scans on a daily basis," he said. "Take the time to do these things. It can save a lot of heartburn."

Stay up to speed on the AMA's COVID-19 advocacy efforts and track the fast-moving pandemic with the AMA's COVID-19 resource center, which offers a library of the most up-to-date resources from JAMA Network™, the Centers for Disease Control and Prevention, and the World Health Organization.

Here are some hoaxes that are prevalent now and tips on how physicians can protect themselves and their patients.

Phishing scams

These are one of the most common traps that physicians may encounter, Upadhyayula said. Scammers send emails that they often try to disguise as coming from a legitimate source. For example, the email may look like it is coming from the Centers for Disease Control and Prevention, a payroll service or the help desk saying they are doing a security or software update. It may even look like it comes from a colleague you know, but is really a fake account a scammer created using information found on social media.

The email tries to lure you into clicking on a link that will take you to a site that may download malware onto the device you are using, or it may take you to a fake screen where you are asked to enter sensitive information such as account names or numbers and passwords.

Advice: Often you get these emails when you are not expecting them, Upadhyayula said, so go directly to the source and verify it's a legitimate email. If it appears to be from a colleague or a help desk, ask them if they sent an email. If it looks like it is from the CDC, a bank or other source, go directly to that source's website to look for the information or pick up the phone to call someone there. Physicians also can use their cursor to hover over the web address they are being asked to go to or the email address the email came from to see if it looks legitimate.

Data security and privacy

Unsecured networks, public networks and computers without antivirus programs are prone to hacking, so physicians who are using home computers to see patients via telehealth during the COVID-19 pandemic need to be conscious of the connections they are using.

Advice: In addition to using virtual private network (VPN), make sure computers and other personal devices you use have all available software updates and patches. Upadhyayula said hackers often

exploit devices that are not current. Use strong and unique passwords; using a password manager to make it easier for you. Make sure videoconferences are always password protected so hackers can't get in.

What if I've been compromised?

If you've entered account credentials such as your log in and password into a fake website, go into your accounts and change your passwords, including any accounts where you use the same log in information you entered, Upadhyayula said.

If you've downloaded something unsafe, tell your IT department or telehealth provider. If you have antivirus software, run a scan or you can shut your device down until you've talked to someone about it.

Upadhyayula said "telehealth is becoming more and more of a target for hackers. They like data from which they can profit and physicians usually have a good data set with patient information that hackers can use to profit from."