Being Cybersmart

The Do’s and Don’ts to Consider Regarding Your Online Presence

By Chad Schiffman

Being cybersmart in the healthcare industry starts with establishing a security culture and making sure everyone who works for a healthcare organization understands their responsibility to make privacy and security a priority. All employees should understand and follow policies that are in place for protecting health information and other sensitive data.

What about protecting your online presence?

As more and more of our day-to-day activities happen online, so does the risk of a cyberattack. Yet, individuals and organizations are often unaware of their online presence, including how their information is being used, collected and shared.

The U.S. Department of Homeland Security STOP.THINK.CONNECT.™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Using this campaign for staying safe and private online as a guide, the next page offers cybersmart do’s and don’ts to consider.
Do treat personal information like money. In other words, value and protect your personal information and information about your organization. Information such as your purchase history or location has value to bad actors.

Do make sure you are aware of and comfortable with your privacy and security settings on websites and apps. Be sure to look closely at each device, application or browser as they have different features and methods for collecting information and limiting what is shared with others.

Do make sure your computer, mobile devices, software and apps are up to date to protect from a compromise to your data due to viruses, malware, etc.

Do separate business and personal activities performed online. It’s much safer to have separate logins, maintain separate accounts, etc. for performing business and personal activities.

Don’t post anything about yourself or your practice without considering what it reveals, who might see it and how it could be perceived — both now and in the future. What you post now may impact your online presence in the future.

Don’t just rely on your username and a simple password. Instead, make sure you have a strong password that meets best practice requirements and consider additional authentication tools such as biometrics, security keys or a unique one-time code sent to your mobile device.

Don’t post anything about anyone without their permission, especially photos or videos. Have patients sign a consent form that allows you to use their likeness in both print and digital marketing.

A final thought
The threat of a cyberattack is real, and your cybersecurity efforts are more important than ever before. Looking at what your online presence is, including how your information is being used, collected or shared online should be a priority. These types of efforts are simple yet effective ways to be cybersmart in a digital world.