Cybersecurity During COVID-19

The COVID-19 pandemic has increased the threat of cybersecurity attacks as more healthcare personnel work remotely and offer telehealth services. The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert due to COVID-19 exploitation by cybercriminal groups. Ensure adequate security measures are in place to protect both the practice and patients.

COVID-19 Cyber Threat Exploitation

CISA and United Kingdom's National Cyber Security Centre (NCSC) are providing resources on how to defend against COVID-19-related cyber activity:

- Communication platform guidance for individuals and organizations
- Guidance for defending against password spraying attacks
- Phishing guidance for both organizations and individuals

Risk Management for Novel Coronavirus (COVID-19)

CISA's risk management guide includes:

- Actions for Infrastructure Protections
- Actions for your Supply Chain
- Cybersecurity for Organizations
- Cybersecurity Actions for Workforce and Consumers

Cybersecurity Assessments

CISA provides cybersecurity assessments to evaluate elements of a strong cybersecurity framework, including how to assess for risk and vulnerabilities.

Avoiding Social Engineering and Phishing Scams

Learn how to recognize and avoid phishing attacks with these security tips for email attachments and tips for spotting phishing emails.

Complimentary Antivirus Software

To support the efforts of OMS practices during the pandemic, Cytek is providing complimentary access to its Sophos antivirus software to AAOMS members while they are working from home.