

September Newsletter

How to Protect Your Dental Network, Like a Pro

Your dental network is essential for your practice. By understanding the different layers of security and implementing them in your practice, you can protect your network from unauthorized access, data breaches, and other cyber threats.



Here are some of the layers of security you need to know about:

Wi-Fi security:

Have separate passwords for patients and staff. This makes it easier to track who has access to what. If you have a single password it can be difficult to track who has accessed patient data. This can make it more difficult to investigate security breaches.

Monitoring and Patching:

Monitoring your network for suspicious activity can help you detect and respond to cyberattacks quickly. Patching critical updates will keep your network secure.

Endpoint detection and response (EDR):

EDR software can help you detect and respond to malware infections on your endpoints. EDR software can also help you investigate and remediate security incidents.

Firewall:

A firewall is like a bouncer at a club. It controls who can come and go in your network.

Backups:

Backups are essential for protecting your data in case of a cyberattack or other disaster. Make sure to regularly backup your data to an off-site location.

Antivirus software:

Antivirus software can help protect your devices from malware infections. Make sure to keep your antivirus software up to date and to scan your devices regularly.

Training:

Training your staff on cybersecurity best practices can help them protect your network from cyberattacks. Make sure your staff knows how to create strong passwords, avoid clicking on phishing links, and report suspicious activity.

By adding these layers, you can protect your dental network from unauthorized access, data breaches, and other cyber threats. This will help you keep your patients' data safe and secure, and it will also help you keep your network running smoothly and efficiently.