CYBERSECURITY

Steps to Protect Your Dental Practice

Take a multi-tiered approach to security.

Simply having a backup is not enough. Use a reputable cloud provider to implement a recoverability plan.

Communicate cybersecurity awareness to your staff members.

Regularly communicate with your staff the importance of security and how to be cyber-safe. Include security in new employee onboarding.

Implement a strong password policy for your office.

Implement a password policy and train your staff on intentional and diligent password management:

- Eliminate duplicate password usage.
- Create complex passwords.
- Do not text, email, or share passwords.
- Change passwords regularly.

Use a password manager with two-factor authentication.

Choose a reputable password manager like Keeper, LastPass, 1Password, or Dashlane.

Always use two-factor authentication when available.

Use two-factor authentication whenever possible, especially with financial institutions.

Avoid using memory sticks/USB drives unless you purchased them.

Malware can be placed on a stick planted by a cybercriminal and you'll never know it until it is too late.

Do not click on links in emails and messages.

Go directly to the sites of interest instead.

Do not share personal information to people that contact you.

If someone asks you for personal information by phone, email, web or other means, don't share! You should always be the one to initiate the contact.

Keep your technology systems updated.

Keep your technology systems patched and updated with the most current security software.

Incorporate a business-only technology use policy.

Use your technology in the office only for the office. Make it a policy not to allow online shopping from any of your practice's computer.

curve DENTAL®

For more resources, visit curvedental.com.

07.2021