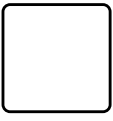


# Cybersecurity Checklist for Dental Teams

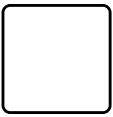
Protect Patient Data Like You Protect Their Smiles



## Use Strong, Unique Passwords

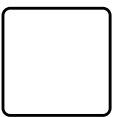
- Combine upper/lowercase, numbers, and symbols
- Avoid using across accounts
- No sticky notes, please 🙄

**Pro Tip: Use a password manager**



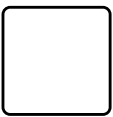
## Turn on Multi-Factor Authentication (MFA)

- Adds an extra layer of protection
- Enable it for email, PM software, and cloud tools



## Think Before You Click

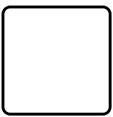
- Hover over links first
- Double-check sender addresses
- Don't open surprise attachments
- When in doubt, verify with a call



## Log Off When You Walk Off

- Hit Windows+L every time you walk away
- Set auto-lock timers
- Protect screens from wandering eyes

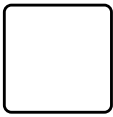
**Visual hacks are a REAL thing with an 88% success rate (70% going unnoticed and 52% of screens are at risk).**



## Handle Devices with Care

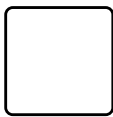
- Avoid using unknown USB drives
- Use only company-approved storage devices
- Ask IT before adding any new tech or hardware to the system

**46% of compromised systems are personal devices (non-managed) with business logins.**



## Don't Delay Software Updates

- Updates patch security gaps and fixes bugs
- Keep antivirus and operating system up-to-date
- Schedule updates regularly...don't snooze them



## Know Who to Call for Help

- Report suspicious activity ASAP
- Follow your practice's incident response plan
- Save Pact-One's number in your contacts (just in case)!

## Cybersecurity is a Team Effort

Every click, login, and lock screen counts.

**Want expert training or help securing your network?**

Contact us to speak with a dental IT pro.

Pact-One Solutions | [pact-one.com](https://pact-one.com) | 866-722-8663

