Cybersecurity Tips for Cardinal Employers

At Cardinal Services, cybersecurity is a shared responsibility. While we continue to strengthen our internal protections, we encourage all clients to adopt the following best practices to safeguard sensitive data and systems.

1. Enable and Enforce Multi-Factor Authentication (MFA)

Multi-factor authentication is one of the most effective ways to prevent unauthorized access.

- Require MFA for all systems, including email, payroll, and HR platforms
- Encourage employees to use authenticator apps instead of SMS when possible
- Reinforce that passwords alone are not sufficient protection

Important Update:

Cardinal is actively rolling out Prism One ID, which will provide a streamlined and secure login experience with enhanced MFA protections across PrismHR access points.

2. Use Strong, Unique Passwords

Weak or reused passwords remain a leading cause of security breaches.

- Require passwords to be long, complex, and unique for each system
- Avoid using personal information (names, birthdays, company name)
- Consider a password manager to securely store credentials

3. Be Vigilant Against Phishing and Email Threats

Cybercriminals often target employees through deceptive emails.

- Verify unexpected requests for sensitive information or payments
- Check sender addresses closely, even if the name appears familiar
- Do not click on suspicious links or open unknown attachments
- When in doubt, confirm requests through a secondary method

4. Secure Your Devices

Every device that touches your systems can introduce risk.

- Keep operating systems and applications updated
- Install only approved software
- Ensure endpoint protection is active and not disabled
- Lock devices when not in use

5. Separate Business and Personal Use
Mixing personal and business activity increases exposure.

- Avoid using personal devices for work systems unless authorized
- Never share company credentials with others
- Use secure networks when accessing company data

6. Protect Remote Access
Remote work requires additional safeguards.

- Always use secure VPN access when required
- Avoid public Wi-Fi when accessing sensitive systems
- If public Wi-Fi must be used, avoid logging into critical platforms

7. Limit Access to Sensitive Information
Not every employee needs access to all data.

- Follow the principle of least privilege
- Regularly review user access rights
- Remove access promptly when roles change or employment ends

8. Report Suspicious Activity Immediately
Early detection can prevent larger incidents.

- Report unusual emails, login alerts, or system behavior
- Notify your internal contact or Cardinal support team promptly
- Do not assume someone else has already reported it

9. Keep Software and Systems Updated
Outdated systems are a common entry point for attackers.

- Enable automatic updates where possible
- Patch systems regularly
- Replace unsupported or end-of-life software

10. Understand Your Role in Security
Technology alone cannot prevent all risks.

- Provide regular cybersecurity awareness training for employees
- Encourage a culture where reporting concerns is supported
- Reinforce that security is a daily responsibility

Cardinal's Commitment
Cardinal Services continues to invest in advanced security controls, including 24/7 monitoring, cloud-based protections, and enhanced authentication systems like Prism One ID. These efforts are designed to protect both our organization and our clients.

Strong cybersecurity requires partnership. By following these best practices, you help ensure the safety and integrity of your data and systems.