Cybersecurity Tip Sheet

Password Hygiene

- Use complex passwords with a mix of letters, numbers, and symbols.
- Avoid using the same password across multiple accounts.
- Change passwords regularly and avoid predictable patterns.
- Use a reputable password manager to store and generate passwords.

Phishing Awareness

- Be cautious of unsolicited emails asking for personal information.
- Verify the sender's email address before clicking on links or downloading attachments.
- Look for spelling errors and suspicious URLs in emails.
- Report phishing attempts to your IT department immediately.

Device Security

- Lock your devices when not in use.
- Use antivirus and anti-malware software and keep it updated.
- Avoid connecting to unsecured public Wi-Fi networks.
- Enable device encryption where possible.

Software Updates

- Install updates and patches as soon as they are released.
- Enable automatic updates for operating systems and applications.
- Regularly check for firmware updates on hardware devices.
- Uninstall unused or outdated software to reduce vulnerabilities.

Incident Reporting

- Report suspicious activity to your IT department immediately.
- Follow your organization's incident response protocol.
- Document the details of the incident including time, nature, and affected systems.
- Do not attempt to fix the issue yourself unless authorized.

Safe Browsing Practices

- Use secure and trusted websites (look for HTTPS).
- Avoid clicking on pop-ups or ads from unknown sources.
- Clear browser cache and cookies regularly.
- Use browser extensions that enhance security and privacy.

Cybersecurity is no longer a back-office concern—it's a frontline defense for patient safety, business continuity, and institutional trust. The Richmond University Medical Center

incident shows that even with robust systems, no organization is immune. But preparedness, rapid response, and continuous improvement can make all the difference.

The goal isn't to be invincible—it's to be resilient. Like outrunning a bear, you don't need to be the fastest, just faster than the next target. By layering defenses, training staff, and investing in infrastructure, you make your organization a harder target—one that attackers are more likely to skip.

Above all, remember: every click matters. Every password matters. Every moment of downtime impacts lives. Cybersecurity is everyone's responsibility—and together, we can protect what matters most.

Resources for cybersecurity best practices

Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA

Cybersecurity Framework | NIST

2025 Top 20 Must Read Resources to Stay Updated on Cybersecurity Threats and Trends - SecurityScorecard