

Cyber Safe at Home

Protect Your Family. Protect Your Workplace.



WHY IT MATTERS

Cybercriminals do not stop at the hospital door. A compromised personal account, home computer, or Wi-Fi network can expose sensitive information, enable identity theft, and create pathways into workplace systems.



COMMON THREATS



- Weak or reused passwords
- Phishing emails and text messages
- Unsecured mobile devices
- Poorly secured home Wi-Fi
- Fake shopping and delivery scams
- Stolen cloud account credentials

WHAT HAPPENS WHEN WE LET OUR GUARD DOWN?

Personal Impact:

- ⚠ Identity Theft
- ⚠ Financial loss
- ⚠ Stolen personal information
- ⚠ Account takeover



Healthcare Impact:

- Stolen work credentials
- Business email compromise
- Unauthorized access to healthcare systems
- Increased risk to patient care



5 ACTIONS YOU CAN TAKE TODAY

1 Use Strong, Unique Passwords.



- ✓ Use a password manager
- ✓ Never reuse passwords

2 Turn on Multi-Factor Authentication (MFA)



- ✓ Protect email first
- ✓ Protect banking and healthcare portals

3 Update Devices Regularly



- ✓ Enable automatic updates
- ✓ Replace unsupported devices

4 Secure Your Home Networks

- ✓ Change default router passwords
- ✓ Enable WPA3 or WPA2 encryption
- ✓ Separate guest devices when possible

5 Pause Before You Click



- ✓ Verify unexpected messages
- ✓ Be cautious with QR codes
- ✓ Report suspicious emails

Remember Cybersecurity starts at home. Every secure account, updated device, and cautious click makes healthcare safer for everyone

THINK. VERIFY. PROTECT.

Because today's cyber threats reach far beyond the workplace.