

Practicing Cyber-hygiene

As nurses



Practicing cyber-hygiene refers to taking steps to maintain cybersecurity and decrease the possibility of a data breach.

(Kim, 2018)

Hospitals are a major target of ransomware attacks.

Delayed patient care creates greater incentive to pay requested money.

(Zetter, 2016)



Prevention & Attention for Nurses



- Log out of workstations.
- Change passwords frequently.
- Create complex passwords.
- Do not share usernames and passwords.



- Do not leave portal devices unattended.
- Do not connect work devices to public networks or vice versa.
- Do not download extension from the internet that have not been approved.



- Verify emails and links are from known senders.
- Do not click on links from unknown emails.
- Report suspicious emails.

(Kamerer & McDermott, 2020)

Prevention & Attention for Nursing Managers



- Regular security awareness training and phishing campaigns
- Restrict staff technology privileges to only what is necessary for patient care
- Require logins at all workstations



- Be aware of staff burnout & fatigue
- Be consistent with norms and expectations related to network security
- Encourage accountability
- Teach staff to be discriminant "clickers"



- Disaster recovery plan
- Cybersecurity orientation and competency
- Informatics Nurse for specialized training
- Involvement in cybersecurity policy & procedure at local, state and federal levels

(Middaugh, D.J., 2021)