Cyber Safety Cheat Sheet

Cybersecurity is a team effort. Here's how you can help reduce the risk of falling victim to the most common cyberattacks.

	✓	✗
PHISHING	• **Be suspicious** of unsolicited emails, especially those with urgent requests or grammatical errors. • **Hover over links** to see the real destination URL before clicking. • **Report suspicious emails** to your IT department.	• Click on links or open attachments in emails you weren't expecting. • Enter personal information or login credentials in response to an email. • Share confidential patient data via email unless absolutely necessary and following proper protocols.
RANSOMWARE	• **Install security & hardware updates** on all devices, including laptops & smartphones • **Be cautious** about opening attachments and clicking links. • **Report suspicious activity** to your IT department immediately.	• Open suspicious attachments or click on unknown links. • Pay a ransom if your system is infected - Contact IT immediately. • Download software from untrusted sources.
MALWARE	• **Only download software from trusted sources.** • **Keep your operating system and applications up to date** with the latest security patches. • **Beware** of free software and apps	• Open unknown or suspicious files. • Click on pop-up ads or download software from unsolicited emails. • Disable your antivirus software.
INSIDER THREATS	• **Limit access to sensitive data** only to those who need it for their job. • **Report any suspicious activit**y by colleagues, including unauthorized data access attempts. • **Be mindful of what information you share** both online and offline.	• Share your passwords or login credentials with anyone. • Access patient data outside of your job duties. • Take patient data outside the facility without proper authorization.
UNSECURED DEVICES & NETWORKS	• **Use strong passwords** and change them regularly. • **Beware of using public Wi-Fi** when accessing sensitive information. • **Report lost or stolen devices** immediately.	• Use weak passwords (e.g., birthdays, pet names). • Connect to unsecured Wi-Fi networks • Leave your computer unattended while logged in. • Leave sensitive data visible on your screen when you walk away.

Brought to you by: showd.me now i know www.showd.me