LEVEL THREE

You've reached the next level in your cyber quest, but watch out—**Dr. Enkryptor** has entered the game! This notorious villain deals in **ransomware**, locking up valuable data and holding it hostage for big payouts. Cybercriminals use it to strong-arm organizations out of millions and cripple top-tier cybersecurity and IT teams.

YOUR MISSION:

Your mission this week is to stay sharp and power up your knowledge so you can **defend the digital realm by mastering Ransomware Defense**. Complete the exercises and move one step closer to becoming a Cyber Superhero!

YOU'LL LEARN:

- The real-world impact of ransomware
- Warnings an infection is in progress
- Proactive defenses to keep your systems (and sanity) safe

To start SCAN or CLICK the QR codes

VILLAIN: Dr. Enkryptor

ATTRIBUTES: Threatening, Sneaky

RANSOMWARE ATTACK MODES:

- Installing malware on your device/network
- Locking you out of your systems
- Encrypting your data and then demanding a ransom payment

Ransomware Quick Tips

- Back up your files to a secondary, secure location
- To add another layer of protection by only using secure networks
- Be sure to always keep your security software up to date
- Never pay a ransom to cybercriminals

IMPORTANT: If you believe you've been a victim of a ransomware attack, disconnect any devices from your network and contact the Enterprise Cybersecurity team immediately.

Identify Cyber Threats ◆ *Stop, Look, and Think*

IN-PERSON

USB - uses a thumb drive to install malware

Tailgating - bypasses security by following authorized users

DIGITAL

Phishing - emails target an organization

Spear Phishing - targets a specific person/role

PHONE/MOBILE

Smishing - text based, SMS phishing

Vishing- over-the-phone, voice based phishing