BEWARE OF INFECTION

Ransomware

Ransomware is a type of **malware** (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the attacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the attacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. It is important to note that payment does not guarantee release of your data.

QUICK TIPS TO AVOID INFECTION

Ransomware attacks often originate via a phishing email. Be sure you know how to identify these phishing emails! Stay alert when any email asks you to enter your credentials.

Do not power off or shut down the computer or server, in case a volatile random-access memory (RAM) image needs to be collected for forensics and incident response investigations.

Notify IT or your practice manager immediately if you believe you have been infected.

Ensure firewalls are in place.

Participate in all organization sponsored training.

KNOW THE RISK

The average cost of a ransomware attack — not including the cost of the ransom itself — was

$4.54M

Source: Cost of Data Breach Report 2022

PROTECT YOUR ORGANIZATION

Prevention is the best medicine.

Check out the Prescription Series Posters to learn how you can prevent Ransomware attacks.

Presented in Technical Volumes 1 and 2 of HICP, the ten Cybersecurity Practices range from personnel training and awareness to the development and implementation of new processes, the acquisition and customization of new technology, and, ultimately, to fostering a consistent, robust, and continually updated approach to cybersecurity.

HHS 405(d)
Aligning Health Care Industry Security Approaches

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov or our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*