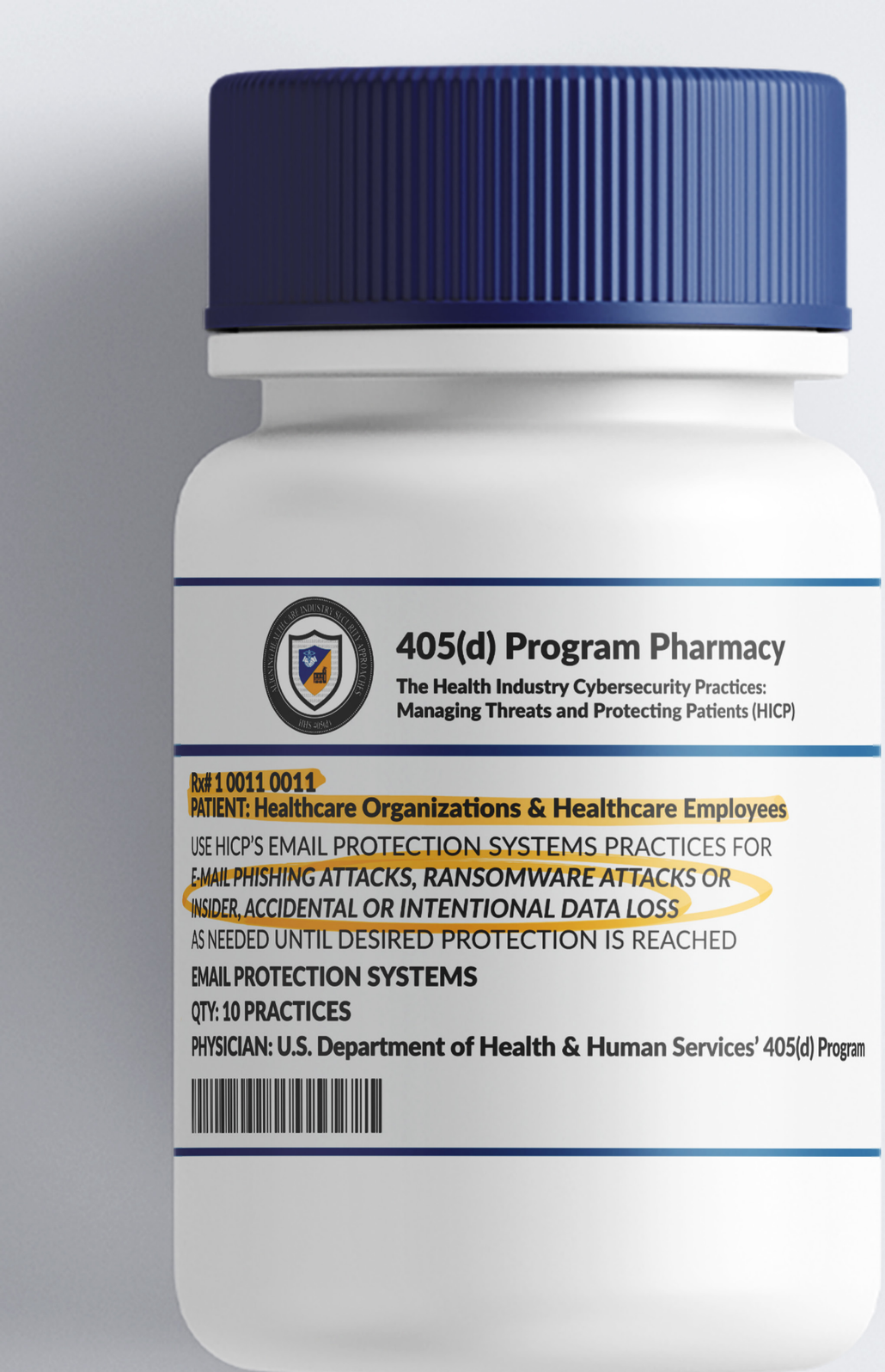

PRESCRIPTION:

Email Protection Systems

The two most common phishing methods occur by email access: 1) Credential theft is where attackers leverage e-mails to conduct credential harvesting attacks on the organization. 2) Malware dropper attacks are used when attackers deliver malware through emails, which can compromise endpoints. An organization's cybersecurity practices must address these two attack vectors. Because both attack types leverage e-mail, e-mail systems should be the focus for additional security controls.

Protect yourself and your patients by following the course of treatment below:

For Small Organizations:

- Instill basic e-mail protection controls such as standard antispam and antivirus (AV) filtering controls, which should be implemented in any e-mail system.
- Acquire Multifactor Authentication (MFA) for remote e-mail access, which is the process of verifying a user's identity using more than one credential, thus adding an extra layer of defense against email attacks.
- Implement education and awareness activities such as trainings, phishing simulations, and awareness campaigns to assist employees and partners in protecting your organization against phishing attacks.

For Medium/Large Organizations:

In addition to instituting the tips for Small Organizations be sure to incorporate the following

- Institute basic email controls including real-time black hole lists, distributed checksum clearinghouses (DCCs), and spam/virus checks on outbound messages.
- Utilize advanced and next generation tooling to combat phishing and malware. These tools use threat analytics and real-time response capabilities to provide protection against phishing attacks and malware.
- Perform analytical education by reviewing who in your organization is being targeted most and create cyber security education specifically for that group.

For more Email Protection Systems practices, please visit www405d.hhs.gov to download a copy of the HICP technical volume for your organization. Check out the available resources 405(d) has to offer by visiting our social media pages @ask405d on Facebook, Twitter, and Instagram!