# Training Bulletin Guidance—Ransomware

## Trainer Notes

This bulletin raises awareness about ransomware. In 2017, ransomware attacks spiked. Awareness and training are critical steps to preventing a ransomware attack on your business.

## Ransomware

Ransomware is a type of malware (malicious software) that 'kidnaps' your business data and holds it hostage until you pay a ransom.  Ransomware holds your data hostage by encrypting it and preventing access to it. If the ransom is paid, the decryption key is sent to you to decrypt and recover your data. If the ransom is not paid, your data remains encrypted and unusable. Or, with some ransomware, you must pay the ransom within a certain amount of time otherwise the ransomware deletes your data.

## Talking Points

- Remind employees that cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.
- Remind employees that malware attacks (like ransomware) are a real threat and every person and organization is a target.
- Employees can help prevent ransomware by understanding how to recognize phishing emails and knowing to alert your IT department if they receive one.

# CYBERSECURITY TRAINING BULLETIN

## Ransomware—Kidnapping Your Company Data

### What is Ransomware?

Ransomware is a type of malware (malicious software) that ‘kidnaps’ your business data and holds it hostage until you pay a ransom.  Ransomware holds your data hostage by encrypting it and preventing access to it. If the ransom is paid, the decryption key is sent to you to decrypt and ideally recover your data. If the ransom is not paid, your data remains encrypted and unusable.

### Ransomware in the News

In 2017, ransomware attacks spiked with several attacks making the mainstream news. For example, WannaCry and NotPetya were two ransomware variants that made major headlines last year. WannaCry alone affected more than 300,000 organizations worldwide. Ransomware attacks are growing and employees play a big part in protecting an organization against ransomware.

### How Does Ransomware Get on Your System?

Ransomware typically enters your network through outdated software, or, more commonly, when an employee responds to a phishing email by clicking on a link or opening an e-mail attachment containing malware.

## Best Practices

Here are some ways you can help to defend against ransomware attacks.

- Recognize phishing emails. Don’t open any attachments or click on any links in suspicious emails. Forward them to your IT department for verification. If you don’t know how to recognize a phishing email – ask your IT department for help.
- If infected, IMMEDIATELY disconnect your computer from all networks and call your IT department.
- Always regularly back up business critical data and store backups disconnected from your network. You don’t need to pay ransom if you have good backups!
- Keep all software on your computer up-to-date.