Ch: 8 Prevent Malware and Security Threats

- Detect, Remove, and Prevent Malware
- Troubleshoot Common Workstation Security Issues

Topic A: Detect, Remove, and Prevent Malware

Computer Viruses and Worms

this is important stuff

Virus: Code designed to infect computer files when it is activated.

Worm: A type of virus that spreads through memory and network connections rather than infecting files.

Virus types: Macro: these viruses affect Office documents

Boot sector: these attack the boot sector information, the partition table,and sometimes the file system

Firmware: these are targeted against the firmware of a specific component, such as the drive controller

Program: these are sequences of code that insert themselves into another executable program.

Script: these are to automate OS functions and add interactivity to web pages.

Computer Viruses and Worms

Worm: A type of virus that spreads through memory and network connections rather than infecting files.

Worms:

- Self-contained
- Typically target a network application vulnerability
- Rapidly consume network bandwidth

Trojan Horses and Spyware

Trojan Horse: A malicious software program hidden within an innocuous-seeming piece of software.

Spyware: Software that records information about a PC and its user.

Rootkit: A class of malware that modifies system files, often at the kernel level, to conceal its presence.

Ransomware: A type of malware that tries to extort money from the victim by appearing to lock their computer or by encrypting their files, for instance.

Trojan Horses and Spyware

Trojans: Used by the Greeks tocapture Troy

- Often function as a back door to applications
- Backdoor allows attacker access to the computer
  - Upload files
  - Install software
  - Turn the system into a botnet
  - Launch DoS attacks
  - Send mass-mail spam
- Used to conceal the attacker's actions

Trojan Horses and Spyware

Spyware:

Often installed without user's knowledge

Keyloggers attempt to steal information by recording keystrokes

Trojans and Spyware

- Rootkits:
  - Masquerade as a dll
  - Doesn't reveal its presence
  - General function:
    - Replace key system files and utilities
    - Provide backdoor for rootkit handler
    - Evade anti-virus software
  - May be deployed as part of DRM (Digital Rights Management)

Trojans and Spyware

- Ransomware:
  - Attempt to extort money from the victim
  - May block access to the PC or encrypt files
  - Allows access to OS but not to your personal data!

Sources of Malware Infection

- Unsavory websites
- Unpatched browser
- No anti-virus software
- Links in unsolicited email
- Compromised PC on the same network
- Executing file of unknown origin
- Zero-day exploit

Antivirus Software

- **Antivirus software:** Software capable of detecting and removing virus infections and other types of malware.
- **Heuristic:** Monitoring technique that allows dynamic pattern matching based on past experience rather than relying on pre-loaded signatures.

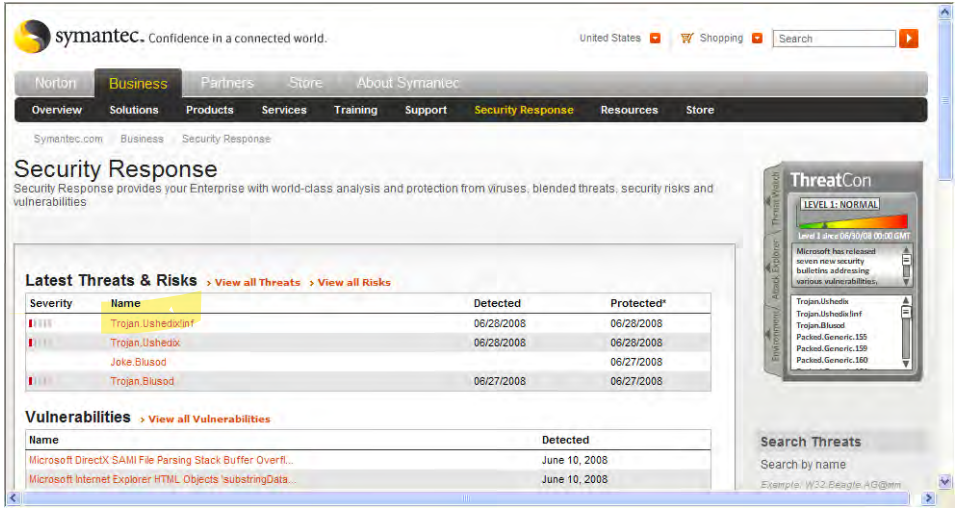
Can run:	User can:	Updates must be installed
• When a file is accessed • At boot time	• Disinfect file • Quarantine file • Delete file	

Best Practices for Malware Removal

this is test question

Identify and research	Identify and research malware symptoms.
Quarantine	Quarantine infected systems.
Disable	Disable System Restore (in Windows).
Remediate	Remediate infected systems: • Scan and use removal techniques (Safe Mode, Pre-installation environment).
Schedule	Schedule scans and run updates.
Enable	Enable System Restore and create restore point (in Windows).
Educate	Educate end user.

Malware Research



Quarantine and Remediation of Infected Systems

very important stuff

Disconnect

- Disconnect network link

Move

- Move infected system to secure work area

Disable

- Disable System Restore and automated backup systems

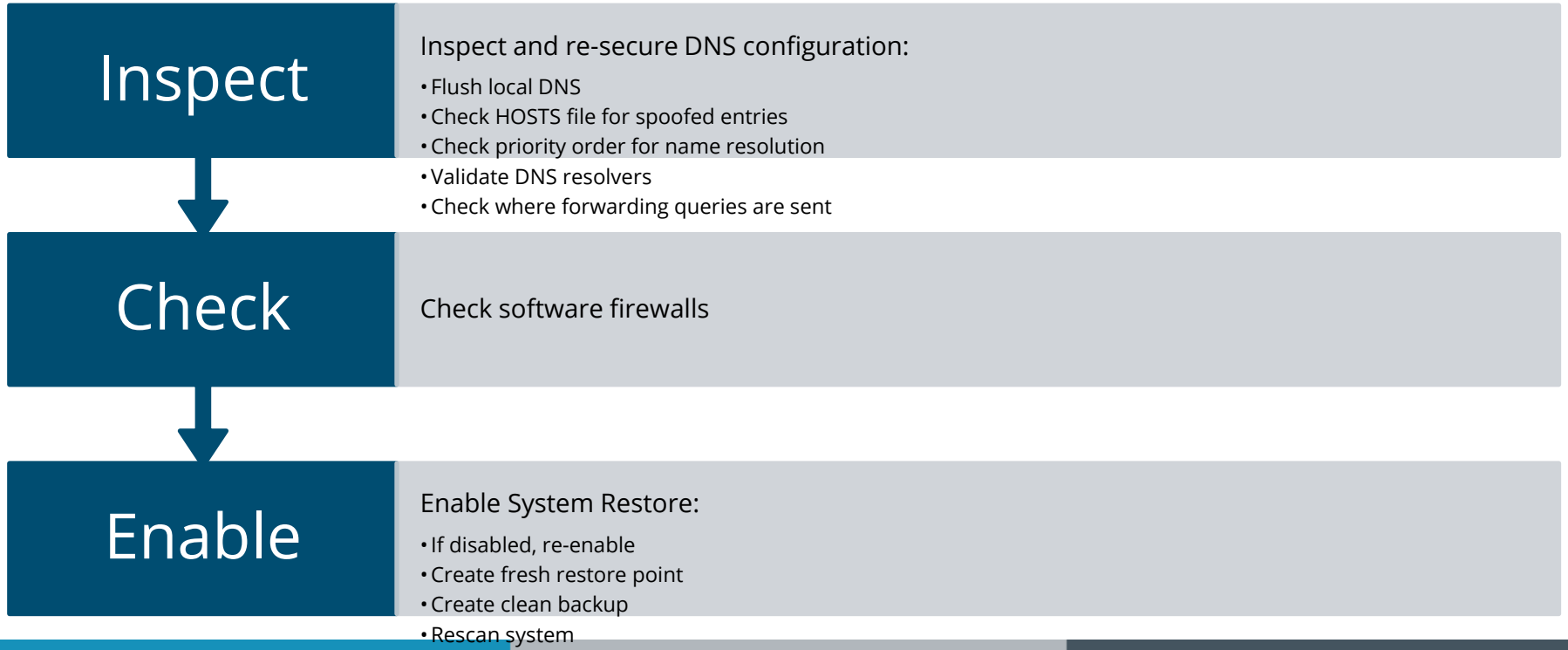
Scan

- Scan any removal media that was attached

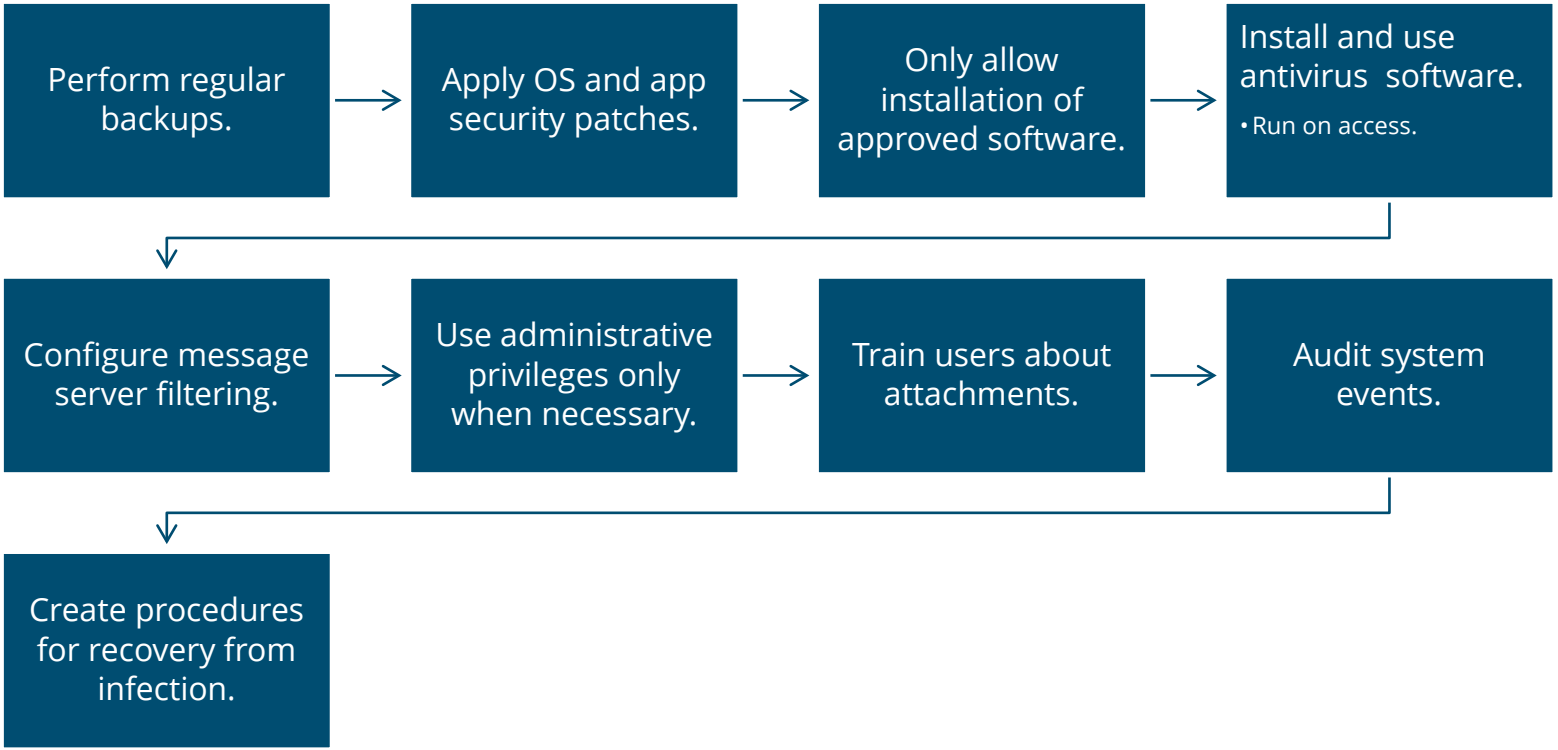
Use

- Use antivirus software on the infected system

Malware Infection Prevention



Guidelines for Reducing Malware Effects



Discussing Detecting, Removing, and Preventing Malware Infections

- **What are the principal characteristics of Trojan malware?**

- **ANSWER:**
  - A Trojan is malware disguised as legitimate software. Most Trojans establish a backdoor so that use of the computer can be subverted by a remote handler.

Discussing Detecting, Removing, and Preventing Malware Infections

- **What general class of malware is crypto-malware an example of?**

- **ANSWER:**
  - Crypto-malware is a type of ransomware. The malware encrypts files on the target and then demands a ransom be paid to release the key that can decrypt them again.

Discussing Detecting, Removing, and Preventing Malware Infections

- **Why might you need to use a virus encyclopedia?**

- **ANSWER:**
  - Typically, if a virus cannot be removed automatically, you might want to find a manual removal method.

  - You might also want to identify the consequences of infection—whether the virus might have stolen passwords, and so on.

Discussing Detecting, Removing, and Preventing Malware Infections

- **Why must antivirus software be kept up-to-date regularly?**

- **ANSWER:**
  - While there are certain heuristic techniques, a scanner is most effective when it can detect viruses that it recognizes.

  - The virus update contains details about new or changed virus threats. If the update is not made, it is quite unlikely that these viruses will be detected if they infect your system.

Discussing Detecting, Removing, and Preventing Malware Infections

- **What type of file scan offers best protection for ordinary users?**

- **ANSWER:**
  - On-access scans. These might reduce performance somewhat but very few users would remember to scan each file they use manually before opening.

Discussing Detecting, Removing, and Preventing Malware Infections

- **What would be the purpose of quarantining an infected file, rather than deleting it?**

- **ANSWER:**
  - If antivirus software cannot clean a file, you may still want to investigate alternative methods of recovering data from the file.

  - Quarantine means the antivirus software blocks access without actually removing the file from the file system.

Discussing Detecting, Removing, and Preventing Malware Infections

- **Why is DNS configuration a step in the malware remediation process?**

- **ANSWER:**
  - Compromising domain name resolution is a very effective means of redirecting users to malicious websites.
  - Following malware infection, it is important to ensure that DNS is being performed by valid servers.

Discussing Detecting, Removing, and Preventing Malware Infections

- **What sort of training should you give to end users to reduce the risk of infections?**

- **ANSWER:**
  - Not to disable security applications and to be wary of emailed links, file attachments, removable media, and websites from unproven sources.

Topic B: Troubleshoot Common Workstation Security Issues

Common Symptoms of Malware Infection

Performance symptoms:

- Fails to boot or locks up
- Strange messages or graphics on screen
- System or network performance is very slow

Application crashes and service problems:

- Security-related applications stop working
- Applications and plug-ins stop working or crash frequently

File system errors and anomalies:

- File system or individual files are corrupted or deleted
- Date stamps and file sizes change
- Permissions change
- New executables appear in system folders

Examine event logs for audit failures and crash events

Web Browser Security Issues

Redirection: When the user tries to open a web page but is sent to another page (which may or may not look like the page the user was attempting to access).

- Browsers are often targeted with adware and spyware:
  - Pop-ups
  - Additional toolbars
  - Home page changes suddenly
  - Search provider changes suddenly
  - Slow performance
  - Excessive crashes

- Trojans, rootkits, and botnets
  - Firewall shows unfamiliar processes or ports trying to connect to the Internet
  - Scan of other hosts for weaknesses
  - Attempts to launch DoS attacks

Web Browser Security Issues

- Virus alert hoaxes and rogue antivirus:
  - Hoax virus alerts sent as pranks
  - Asks user to forward message to everyone
  - Contains steps to “remove” the virus
    - Actually, causes damage instead
  - Rogue antivirus used to disguise trojans
    - Fake security alerts
    - Cold calling users and claiming to represent Microsoft support

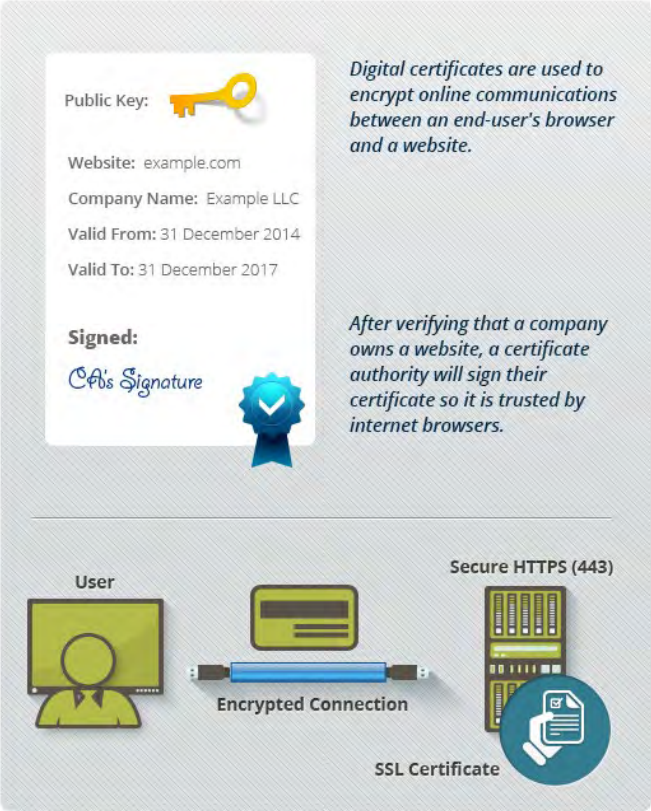
Digital Certificate Issues

Digital certificate: An X.509 digital certificate is issued by a CA as a guarantee that a public key it has issued to an organization to encrypt messages sent to it genuinely belongs to that organization.

Certificate Authority (CA): A server that can issue digital certificates and the associated public/private key pairs.

- Digital certificate:
  - Wrapper for public/private key pair
  - Vouched for by a CA
- When compromised, a CA installs its own root certificate on the computer:
  - Validates the CA signature on messages
  - Stolen certificates exploited due to weaknesses in the key used in the certificate

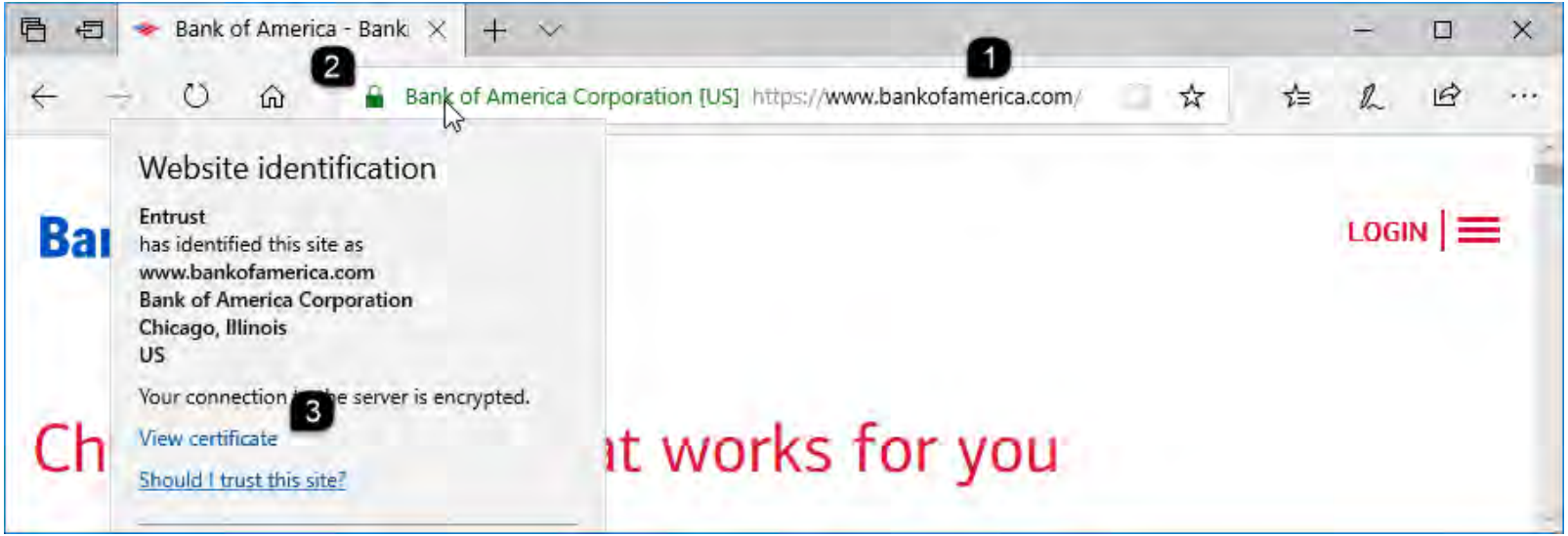
Digital Certificate Issues



- Browser displays certificate information in the address bar:
  - Valid, trusted certificates show a padlock icon
  - Highly trusted certificates show a green address bar
  - Untrusted, invalid certificates show a maroon address bar

Digital Certificate Issues

1. Check the domain in the address bar.
2. Only enter information using a trusted certificate.
3. Select the padlock to view certificate holder and information about the CA that issued the certificate and view the certificate itself.



Email Issues

Spam: Junk messages sent over email.

Zombie PC: A PC infected with unauthorized software that directs the PC to launch a DDoS attack.

Keep spam filters up-to-date to protect against latest spam techniques.

Messages filtered as spam posted to Junk email folder.

- Check to see if any legitimate messages were sent to Junk.

Users can blacklist spammers and whitelist safe senders.

Email frequently used vector for malware.

Spam may be symptom of malware infection.

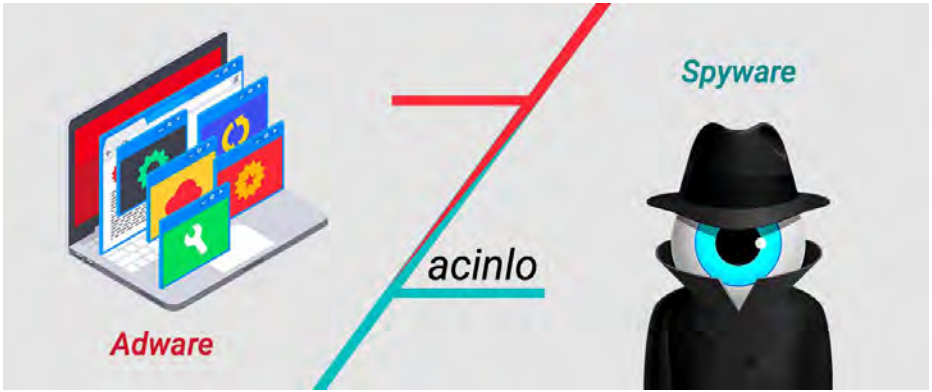
- **Zombie PC.**
- User receives bounces, non-deliverable messages, automated replies from unknown recipients regarding spam that was sent.

Guidelines for Troubleshooting Common Workstation Security Issues

Symptoms of malware infection might include:

- Performance issues such as failure to boot, lock ups, slow performance, or strange messages or images on screen.
- Frequent application crashes and service problems.
- Changes to system files or changes to file permissions.
- Event log entries showing a high number of audit failures or application and service crash events.

Guidelines for Troubleshooting Common Workstation Security Issues



- Web browsers are frequent targets for malware delivery.
  - May be adware or spyware.
  - Might redirect users to a site that imitates the site the user attempted to access.
  - As compromised PC attempts to communicate with handler, unfamiliar processes or ports show up in firewall log files.
  - Hoax virus alerts requesting users to forward the message, or messages including steps to remove the virus with the steps doing the actual damage.
  - Rogue antivirus disguises Trojans.

Guidelines for Troubleshooting Common Workstation Security Issues

- Check for compromised CAs.
  - Verify the padlock icon is shown in browsers for secure sites and that the address bar is not **maroon**, which would indicate an untrusted, insecure site.
- Email issues include:
  - Check the Junk email folder to ensure legitimate emails are not improperly flagged.
  - Make sure users understand the potential issues in running email file attachments.

Discussing Troubleshooting Common Workstation Security Issues

- **Early in the day, a user called the help desk saying that his computer is running slowly and freezing up. Shortly after this user called, other help desk technicians who overheard your call also received calls from users who report similar symptoms. Is this likely to be a malware infection? If so, what type of malware would you suspect?**

- **ANSWER:**
  - It is certainly possible. Software updates are often applied when a computer is started in the morning so that is another potential cause but you should investigate and log a warning so that all support staff are alerted.

  - It is very difficult to categorize malware when the only symptom is performance issues. You might say a virus or worm as the malware is non-stealthy. However, it is equally possible that performance issues could be a result of a badly written Trojan or a Trojan/backdoor application might be using resources maliciously (for DDoS, Bitcoin mining, spam, and so on).

Discussing Troubleshooting Common Workstation Security Issues

- **Why might a PC infected with malware display no obvious symptoms?**

- **ANSWER:**
  - If the malware is used with the intent to steal information or record behavior, it will not try to make its presence obvious.
  - A rootkit may be very hard to detect even when a rigorous investigation is made.

Discussing Troubleshooting Common Workstation Security Issues

- **You receive a support call from a user who is "stuck" on a web page. She is trying to use the Back button to return to her search results, but the page just displays again with a pop-up message. Is her computer infected with malware?**

- **ANSWER:**
  - If it only occurs on certain sites, it is probably part of the site design.
  - A script running on the site can prevent use of the Back button. It could also be a sign of adware or spyware though, so it would be safest to scan the computer using up to date anti-malware software.

Discussing Troubleshooting Common Workstation Security Issues

- **Another user calls to say he is trying to sign on to his online banking service, but the browser reports that the certificate is invalid. Should the bank update its certificate, or do you suspect another cause?**

- **ANSWER:**
  - It would be highly unlikely for a commercial bank to allow its website certificates to run out of date or otherwise be misconfigured.
  - You should strongly suspect redirection by malware or a phishing/pharming scam.

Discussing Troubleshooting Common Workstation Security Issues

- **Your company's static IP address has been placed on a number of anti-spam blacklists. Could this be the result of external fraud or do you need to investigate your internal systems for malware?**

- **ANSWER:**
  - It would be very unusual for someone to be able to insert your IP address into multiple blacklists. You should suspect that malware is being used to send spam from your network.