13.13.3 Security Troubleshooting Facts

As a PC technician, there are a variety of security issues that you must deal with each day. Several common workstation security issues and practices are discussed here.

The key to troubleshooting security issues is to do everything you can to prevent them from occurring in the first place. Consider the following preventative measures:

Preventative Measure	Description
Implement Malware Prevention	Do the following: - Install anti-malware on all systems to search for malware, viruses, worms, trojans, and rootkits. - Enable automatic definition updates on your anti-malware software. - Configure frequent quick malware scans along with less frequent full system scans. - Implement anti-spam measures. This can be done using anti-spam software on each individual workstation. However, it's usually advantageous to implement an anti-spam appliance that filters email messages for your entire organization.
Implement Browser Security	Do the following: - Disable pop-ups on all web browsers. Pop-ups can covertly install malware or redirect users to malicious websites. Enable pop-ups only for legitimate sites that require them. - Override automatic cookie handling. Configure your browser to prompt you before allowing cookies. - Disable third-party browser extensions. - Disable sounds in web pages.
Configure Automatic Updates	Enable automatic updates for all operating systems.
Maintain Awareness	Stay current by subscribing to security alerts offered by many security software vendors.
Educate Users	Educate users about current security threats and how to respond to them. For example, teach them to: - Use strong passwords. This includes email account passwords as well as workstation account passwords. - Distrust anything coming from the web: Don't click anything just because the site says you must do so. - View email with suspicion. A reputable company in the modern world will not send an email asking users to respond with personal information. Any message that does is using phishing to gather personal information. - Recognize social engineering attempts and respond appropriately.

As a PC technician, there are many key security threats that you need to be aware of:

Issue	Description
Spam	Spam may or may not be malicious in nature. However, it wastes time, network bandwidth, and storage space as many organizations are required by law in the United States to retain all email communications for a period of time. The best way to combat spam is to implement an anti-spam appliance that is placed between your network and the internet. The appliance scans all emails as they enter the organization and quarantines anything deemed to be spam.
Phishing Emails	*Phishing* is the process used by attackers to acquire sensitive information such as passwords, credit card numbers, and usernames by masquerading as a trustworthy entity. Phishing emails are drafted such that they appear to have come from a legitimate organization, such as banking, social media, or e-commerce websites. They convince the user to click a link that takes them to a malicious website (that looks exactly like the legitimate website) where they are tricked into revealing sensitive

	information. To detect phishing email, train users to recognize their key characteristics: - The source address of the message may not match the domain of the company it claims to be coming from. - The message tries to create a sense of urgency. For example, it may warn that your bank account will be frozen, that your credit card has been stolen, or that you will be subject to arrest if you don't follow the instructions in the message. - The hyperlinks in the message go to websites that are not associated with the organization the message claims to be coming from. If you hover your mouse over a link (without clicking it) you can see where the link actually leads. If it isn't pointing to the organization's URL, there's a pretty good chance the message is an exploit.
Hijacked Emails	To hijack an email account, attackers use password hints set up by the user to try to gain access to the user's email account. Users should not use personal information such as their birthplace or mother's maiden name. This information is relatively easy to obtain using social media. Once an account has been hijacked, the attacker can use it to propagate spam or malware to every contact in the user's address book.
Pharming	*Pharming* redirects one website's traffic to another, bogus, website that is designed to look like the real website. Once there, the attacker tricks the user into supplying personal information, such as bank account and PIN numbers. Pharming works by resolving legitimate URLs to the IP address of malicious websites. This is typically done using one of the following techniques: - Changing the hosts file on a user's computer - Poisoning a DNS server - Exploiting DHCP servers to deliver the IP address of malicious DNS servers in DHCP leases.
Rogue Antivirus	Rogue antivirus exploits usually employ a pop-up in a browser that tells the user the computer is infected with a virus and that the user must click a link to clean it. Sometimes this exploit is used to trick users into paying for worthless software they don't need. However, it also is frequently used to deploy malware on the victim's computer.
Cookies	*Cookies* are data files placed on a client system by a web server for retrieval at a later time. Cookies are primarily used to track the client. By default, cookies can be retrieved only by the server that set them. The cookies themselves are fairly benign; however, cookies can be exploited by an attacker to steal a client's session parameters. This allows the attacker to impersonate the client system and hijack the session, potentially exposing sensitive information.
Browser History	The browser history and its cache contain information that an attacker can exploit. If an attacker can gain access to the cache or the browser history, they can learn things about the user such as: - The email service they use - The bank where they keep their accounts - Where they shop An attacker can exploit this information to conduct other attacks, such as stealing cookies or sending phishing emails.

As a PC technician, you should be familiar with the symptoms of a malware infection. Look for the following:

- Slow computer performance
- Internet connectivity issues
- Operating system lock ups
- Windows update failures
- Renamed system files
- Disappearing files
- Changed file permissions
- Access denied errors

You should frequently check your logs in Event Viewer to identify suspicious behaviors.

If you suspect a system has been infected, you should observe the following best practices to remove the malware:

- Identify the malware symptoms.
- Quarantine the infected system.
- Disable system restore to prevent the malware from being saved in a restore point (and to prevent an uninfected restore point from being potentially deleted to make room for a new restore point).
- Remediate the infected system.
- Update the anti-malware definitions.
- Scan for and remove the malware. Some malware can be removed while the system is running normally. However, some malware can be removed only while in Safe Mode or in the Pre-Installation Environment.
- Schedule future scans and updates.
- Re-enable system restore and create a new restore point.
- Educate users to prevent the infection from happening again.