2023-24 Competitive Events Guidelines
Cyber Security

Cyber Security provides members with the opportunity to demonstrate knowledge about defending and attacking viruses, spam, and spyware. This competitive event consists of an objective test. This event aims to inspire members to learn about cyber security.

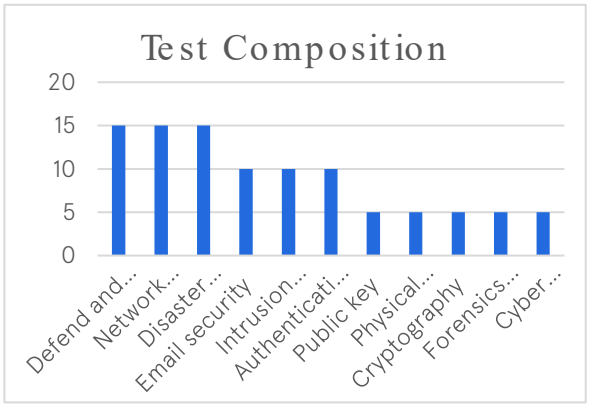
Event Overview

Division: High School
Event Type: Individual
Event Category: Objective Test, 100-multiple choice questions (breakdown of question by competencies below)
Objective Test Time: *50 minutes*
NACE Connections: Career & Self-Development

Equipment Competitor Must Provide: Pencil
Equipment FBLA Provides: One piece of scratch paper per competitor

Objective Test Competencies

- Defend and attack (virus, spam, spyware)
- Network security
- Disaster recovery
- Email security
- Intrusion detection
- Authentication
- Public key
- Physical security
- Cryptography
- Forensics security
- Cyber security policy



District/Region/Section

Check with your District/Region/Section leadership for District/Region/Section-specific competition information.

State

Check with your State Leader for state-specific competition information.

National

Policy and Procedures Manual

- Competitors should be familiar with the Competitive Events Policy & Procedures Manual, found on the Competitive Events page on www.fbla.org.

Eligibility

- FBLA membership dues are paid by 11:59 pm Eastern Time on March 1 of the current program year.

- Members may compete in an event at the National Leadership Conference (NLC) more than once if they have not previously placed in the top 10 of that event at the NLC. If a member places in the top 10 of an event at the NLC, they are no longer eligible to compete in that event.
- Members must be registered for the NLC and pay the national conference registration fee in order to participate in competitive events.
- Members must stay in an official FBLA hotel to be eligible to compete.
- Each state may submit four entries per event.
- Each member can only compete in one individual/team event and one chapter event (American Enterprise Project, Community Service Project, Local Chapter Annual Business Report, Partnership with Business Project).
- Picture identification (physical or digital driver's license, passport, state-issued identification, or school-issued identification) is required when checking in for competitive events.
- If competitors are late for an objective test, they will be allowed to compete until such time that results are finalized, or the accommodation would impact the fairness and integrity of the event. Competitive event schedules cannot be changed. Competitive events start in the morning before the Opening Session of the NLC.

Recognition

- The number of competitors will determine the number of winners. The maximum number of winners for each competitive event is 10.

Event Administration

- This event is an objective test administered online at the NLC.
- No reference or study materials may be brought to the testing site.
- No calculators may be brought into the testing site; online calculators will be provided through the testing software.

Tie Breaker

- Ties are broken by comparing the correct number of answers to 10 pre-determined questions on the test. If a tie remains, answers to 20 pre-determined questions on the test will be reviewed to determine the winner. If a tie remains, the competitor who completed the test in a shorter amount of time will place higher.

Americans with Disabilities Act (ADA)

- FBLA meets the criteria specified in the Americans with Disabilities Act for all competitors with accommodations submitted through the conference registration system by the registration deadline.

Penalty Points

- Competitors may be disqualified if they violate the Competitive Event Guidelines or the Honor Code.
- Five points are deducted if competitors do not follow the Dress Code or are late to the testing site.

Electronic Devices

- All electronic devices such as cell phones and smart watches must be turned off before competition begins.

Study Guide: Competencies and Tasks

A. Defend and Attack
   1. Identify basic security risks and issues to computer hardware, software, and data.
   2. Define the various virus types and describe the common symptoms caused by viruses and their potential effects.
   3. Define concepts such as phishing, social engineering, spoofing, identify theft, and spamming.
   4. Describe the importance and process of incidence reporting.
   5. Implement security preventive maintenance techniques such as installing service packs and patches.
   6. Assess security threats, diagnose, and troubleshoot hardware, software, and data security issues.
   7. Implement virus protection and removal procedures to recover information form failures and security breaches (e.g., malware and viral infection).
   8. Explain the impact of malware protection, including antivirus software, spam, adware, spyware filtering, and patch management.
   9. Scan storage devices and equipment for viruses and spyware and disinfect as needed.
   10. Install and configure anti-X software (e.g., anti-virus, anti-spyware, and anti-spam).
   11. Identify potential sources of virus infection and describe methods of preventing the spread of computer viruses.
   12. Identify how to protect privacy and personal security online (e.g., to avoid fraud, identity theft and other hazards).
   13. Explain the benefits and demonstrate the use of privacy, password, and protection utilities.

B. Network Security
   1. Explain the importance of network security (e.g., ethics and rights).
   2. Explain principles of basic network security (e.g., IP spoofing, packing sniffing, password compromise, and encryption).
   3. Determine threats and analyze risks to network perimeters.
   4. Determine the impact on network functionality of a particular security implementation (e.g., port blocking/filter, authentication, and encryption).
   5. Identify the following security protocols and describe their purpose and function: IPSEC, L2TP, SSL, WEP, WPA, and 802.1x.
   6. Identify specific access levels that need to be accommodated.
   7. Match security system design to identify security requirements.
   8. Develop, document and implement a network security plan (e.g., install, configure, upgrade, and optimize security).
   9. Train users in malicious software prevention technologies.

10. Diagnose and troubleshoot hardware, software, and data security issues.
11. Implement hardware and software network security solutions (e.g., VPN, SSL, and firewall).
12. Identify the purposes and characteristics of access control and permissions, auditing and event logging.
13. Know and implement user security policies and procedures to maintain, monitor, and support the security and integrity of a network.
14. Implement secured access to network resources.
15. Describe the importance and demonstrate forms of network security (e.g., password strategies and user accounts).
16. Illustrate fundamental legal issues involved with security management.
17. Design an audit policy and incident response procedures.
18. Manage and distribute critical software updates that resolve known security vulnerabilities and other stability issues.
19. Explain the importance of educating users and supervisors in regard to network security.
20. Implement security controls such as MAC or DAC to ensure user policies and enabled.
21. Implement server and Web-based services security features.
22. Describe what a firewall is, its uses, and how it works.
23. Explain the characteristics, uses, and benefits of software firewalls and hardware firewalls.
24. Install and update a firewall.
25. Configure personal firewall protection.
26. Describe the four basic firewall techniques (e.g., proxy server, packet filter, application gateway, and circuit-level gateway).
27. Implement global, domain, and local account policies.
28. Distinguish among the following security methods: DMX (including dual-homed and triple-homed firewalls), VLan, intranet, extranet, PKI.

C. Email Security

1. Identify common problems associated with electronic communication (e.g., delivery failure, junk mail, fraud hoaxes, phishing, and viruses) and recommend mitigation strategies.
2. Define e-mail and instant messaging protocol.
3. Recognize social engineering and address social engineering situations.
4. Identify netiquette including the use of e-mail, social networking, blogs, texting, and chatting.
5. Explain the benefits and demonstrate the use of privacy, password, and protection utilities.
6. Discuss security issues and guidelines for legal and responsible electronic communications and internet use for business (e.g., includes copyright, netiquette, privacy issues, and ethics).
7. Scan e-mail messages and attachments received to ensure they are not spam.
8. Establish and manage spam/junk mail folders.
9. Identify issues regarding unsolicited e-mail (spam) and how to minimize or control unsolicited mail.

10. Identify contamination protection strategies for e-mail.

D. Intrusion Detection
    1. Explain concepts such as denial of service, hacking/cracking, intrusion, and intellectual property.
    2. Assess security threats and develop plan to address.
    3. Analyze and inspect the system's configuration and vulnerabilities to detect inadvisable settings.
    4. Inspect the password files to detect inadvisable passwords.
    5. Inspect other system areas to detect policy violations.
    6. Assess system and file integrity.
    7. Recognize patterns typical of attacks.
    8. Analyze abnormal activity patterns.
    9. Track user policy violations.
    10. Demonstrate an understanding of internet use and security issues.
    11. Investigate security issues related to internet technology (e.g., viruses, firewalls, spam, system backup, passwords, wireless, and data encryption).
    12. Identify types of intrusion detection and recommend tools to protect against each type.

E. Public Key
    1. Define public key infrastructure.
    2. Describe the advantages and risks associated with a public key infrastructure.
    3. Identify and analyze precautions included in programs used on networks (e.g., self-metering, security keys, and required configuration settings).
    4. Explain the purpose of temporary certificates and single sign-on.
    5. Describe Web of Trust and when it is appropriate to use.
    6. Describe certificate authority and its role in security.
    7. Distinguish between public key encryption and digital signatures.
    8. Describe cryptographic protocols and applications, like digital cash, password-authenticated key agreement, multi-party key agreement, and time stamping service.

F. Authentication
    1. Describe authentication process to network devices for users.
    2. Discuss the need for authentication and non-repudiation of information (e.g., PKI).
    3. Describe the steps to achieve authentication and confidentiality.
    4. Provide for user authentication (e.g., assign passwords and access level).
    5. Identify and resolve a network configuration with incorrect protocols, client software misconfiguration, authentication misconfiguration, and insufficient rights/permissions.
    6. Evaluate electronic sources of information for authenticity.
    7. Identify authentication protocols (e.g., CHAP, MS-CHAP, PAP, RADIUS, Kerbero, and EAP.)
    8. Explain and implement Secure Sockets Layer (SSL) authentication.
    9. Explain and install a certificate.
    10. Describe concepts related to logon authentication.
    11. Educate employees on how to properly handle passwords.

12. Establish policies on choosing a secure password.
13. Describe the biometrics authentication method.
14. Give an example of a two-factor authentication security process.
15. Discuss the need for dual-role authentication.

G. Disaster Recovery
1. Identify possible effects of natural disasters on computers.
2. Describe the purpose and characteristics of disaster recovery: backup-restore, offsite storage, hot and cold spares, and hot, warm, and cold sites.
3. Differentiate between disaster recovery and business continuity.
4. Design a disaster recovery plan.
5. Compare different options of backing up and securing data and restoring a system and perform system backup.
6. Select and test a disaster recovery plan against several disaster scenarios.
7. Demonstrate the ability to recover operating systems (e.g., boot methods, recovery console, ASR, and ERD).
8. Backup and restore files and directories.
9. Implement procedures used to recover information from failures and security breaches (e.g., malware and viral infection).
10. Identify methods for avoiding common computer system disasters (e.g., UPS and RAID).
11. Compare/contrast streaming file-by-file backup systems.
12. Establish process for archiving files.
13. Use the features of a server operating system to prevent a disaster or recover when one occurs.
14. Identify and maintain battery backup equipment.
15. Install surge suppression protection.
16. Develop and document a plan to avoid data loss, including backups and remote storage.

H. Physical Security
1. Define physical security.
2. Identify names, purposes, and characteristics of hardware and software security issues including wireless, data, and physical security.
3. Describe basic physical security risks inherent to computer hardware and software.
4. Describe physical security best practices for enterprises.
5. Describe risk-mitigation techniques (e.g., policies, procedures, hardware, and software).
6. Establish and implement controls for physical site access and security.
7. Identify and analyze environmental hazards (e.g., fire, flood, moisture, temperature, electricity) and establish environmental security controls to protect and restore.
8. Perform a physical configuration audit.
9. Train and test employees in the area of physical security awareness.
10. Describe the physical security components of a Disaster Recovery/Business Continuity Plan.

I. Cryptography
    1. Explain the purpose of cryptography.
    2. Identify levels of encryption.
    3. Describe the types of cryptography algorithms (e.g., secret key, public key, and hash functions).
    4. Describe trust models such as web of trust, Kerberos, and certificates.
    5. Identify cryptography applications used for password protection and private communication. (IP security protocol, clipper, Identify Base Encryption, Internet Security Association and Key Management Protocol, and Secure Sockets Layer).
    6. Illustrate concepts of data encryption and its use with protecting network resources.
    7. Identify uses for VPN and network data encryption.
    8. Define the advantages and risks associated with passwords.
    9. Explain how passwords are stored.
    10. Describe DES (Data Encryption Standards) and explain how it operates.
    11. Explain the purpose and use of AES (Advanced Encryption Standard).
    12. Explain export controls associated with cryptography.

J. Forensics Security
    1. Review incident responses, priorities, and requirements.
    2. Identify recoverable evidence in computer hardware and mobile devices.
    3. Preserve evidence in an acceptable forensically manner.
    4. Review timeline of computer files based on the creation, file modification, and file access.
    5. Identify past internet browsing, downloads, and e-mail communications.
    6. Examine and analyze evidence.
    7. Differentiate between operating systems from a forensics standpoint.
    8. Use computer forensics software tools to cross validate findings in computer evidence-related cases.
    9. Prepare a report of findings.
    10. Identify forensic analysis tools and their uses.
    11. Describe Legislative Acts governing Digital Forensics.

K. Cyber Security Policy
    1. Identify national legislative initiatives that affect cyber security.
    2. Identify Executive Orders that affect cyber security.