



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

Multiple Choice Questions on Threats and Prevention & Malware:

1. What is the main goal of threat prevention?

- A. To recover lost data
- B. To stop threats after they cause damage
- C. To stop threats before they enter a system
- D. To identify employees responsible for data loss

Answer: C. To stop threats before they enter a system

Explanation: According to the text, threat prevention aims to stop specific threats before they enter a system or cause any damage.

2. Which of the following best defines a "threat" in cybersecurity?

- A. A tool used to repair software
- B. A backup method
- C. A potential danger to systems or data
- D. A type of software update

Answer: C. A potential danger to systems or data

Explanation: As stated, threats are any potential dangers that can harm systems, steal data, or disrupt communication.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

3. Which of these is not typically considered a threat?

- A. Data theft
- B. System crash due to malware
- C. Strong password creation
- D. Communication disruption

Answer: C. Strong password creation

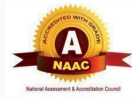
Explanation: Strong passwords help prevent threats; they are a security measure, not a threat themselves.

4. How do security organizations typically handle cyber threats?

- A. By ignoring minor attacks
- B. By using simple manual methods
- C. By using sophisticated tools
- D. By shutting down systems

Answer: C. By using sophisticated tools

Explanation: The passage states that sophisticated tools are used by security organizations to detect and prevent threats.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

5. Which of the following could be an example of a threat?

- A. Antivirus software
- B. Firewall configuration
- C. Malware trying to enter a system
- D. Secure user authentication

Answer: C. Malware trying to enter a system

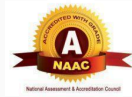
Explanation: Malware is a potential danger that can harm systems—making it a cyber threat.

6. What happens if threat prevention fails?

- A. Systems remain safe
- B. No data is affected
- C. The threat may cause damage or steal data
- D. The threat disappears on its own

Answer: C. The threat may cause damage or steal data

Explanation: If threats are not prevented, they may harm systems, steal data, or disrupt communication.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

7. Which of the following is the best reason to implement threat prevention tools?

- A. To run system updates faster
- B. To allow more users into a system
- C. To stop threats before they cause harm
- D. To increase data entry speed

Answer: C. To stop threats before they cause harm

Explanation: The core purpose of threat prevention is to stop threats before they enter or cause any damage.

8. Threats can lead to which of the following outcomes?

- A. Improved system performance
- B. Faster communication
- C. Data theft or communication disruption
- D. Reduced need for security

Answer: C. Data theft or communication disruption

Explanation: The definition of a threat includes data theft and disruption of communication.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

9. What kind of tools do organizations use to deal with threats?

- A. Entertainment software
- B. Sophisticated detection and prevention tools
- C. Budget management software
- D. Manual paperwork

Answer: B. Sophisticated detection and prevention tools

Explanation: As per the text, security organizations use sophisticated tools to detect and prevent threats.

10. Which of the following statements is true based on the passage?

- A. Threat prevention begins after an attack
- B. Threats only target hardware
- C. Threats can harm systems or steal data
- D. Prevention tools are rarely used by security organizations

Answer: C. Threats can harm systems or steal data

Explanation: The passage clearly says threats may harm systems, steal data, or disrupt communication.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

11. What is a computer virus?

- A. A protective software
- B. A hardware malfunction
- C. A malicious program that attaches itself to clean files
- D. An email encryption tool

Answer: C. A malicious program that attaches itself to clean files

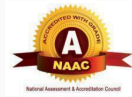
Explanation: A virus is defined as a malicious program that attaches itself to legitimate files or programs to infect and spread.

12. How does a computer virus typically spread?

- A. When the infected file or program is deleted
- B. When the infected file or program runs
- C. Only through internet downloads
- D. By turning off the computer

Answer: B. When the infected file or program runs

Explanation: The virus activates and spreads only when the infected file or program is executed.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

13. What is a common effect of a virus on a computer system?

- A. It increases computer performance
- B. It optimizes system memory
- C. It can corrupt or delete files
- D. It installs security updates

Answer: C. It can corrupt or delete files

Explanation: Viruses often corrupt, delete, or modify files and may slow down the system.

14. What might happen to your system's performance when infected with a virus?

- A. It becomes faster
- B. It freezes and crashes more often
- C. It uses less memory
- D. It automatically updates

Answer: B. It freezes and crashes more often

Explanation: Viruses can slow down performance, cause system instability, or make it crash frequently.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

15. Which of the following is a method to help prevent virus infections?

- A. Running unknown executable files
- B. Disabling antivirus software
- C. Installing and updating antivirus software
- D. Clicking on suspicious email links

Answer: C. Installing and updating antivirus software

Explanation: Antivirus software helps detect and remove viruses and must be regularly updated.

16. A virus typically needs _____ to spread.

- A. no user interaction
- B. a firewall
- C. execution of an infected file
- D. a Bluetooth connection

Answer: C. execution of an infected file

Explanation: Viruses require a host file or program to be executed to begin spreading.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

17. What is a computer worm?

- A. A malicious software that requires a host file to spread
- B. A type of protective software
- C. A malware that self-replicates and spreads on its own
- D. A browser extension

Answer: C. A malware that self-replicates and spreads on its own

Explanation: A worm is self-replicating malware that spreads without attaching to other files or needing user interaction.

18. How do worms typically spread?

- A. Only through USB drives
- B. Only by clicking suspicious links
- C. Automatically across networks or devices
- D. Through social media posts only

Answer: C. Automatically across networks or devices

Explanation: Worms are designed to spread automatically across networks, often exploiting vulnerabilities in systems.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

19. What can be a major effect of a worm on a network?

- A. Stronger security
- B. Increased internet speed
- C. Overloaded networks and system crashes
- D. Improved file access

Answer: C. Overloaded networks and system crashes

Explanation: Worms can rapidly replicate and spread, consuming bandwidth and crashing systems.

20. Which of the following best describes the self-replication ability of worms?

- A. They ask for user permission before copying
- B. They copy themselves only once
- C. They duplicate themselves continuously without user help
- D. They require a download to spread

Answer: C. They duplicate themselves continuously without user help

Explanation: Worms self-replicate automatically, without needing user action.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

21. A computer worm spreads most effectively through_____.

- A. isolated devices
- B. networks with weak security
- C. strongly encrypted connections
- D. printed documents

Answer: B. Networks with weak security

Explanation: Worms exploit vulnerabilities in poorly secured networks to spread rapidly.

22. Why are worms considered dangerous even if they don't delete files?

- A. They provide tech support
- B. They improve user speed
- C. They overload systems and networks, leading to crashes
- D. They reduce power usage

Answer: C. They overload systems and networks, leading to crashes

Explanation: Worms can degrade performance and crash networks, even if they don't directly destroy files.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

23. What is ransomware?

- A. Malware that deletes all files immediately
- B. Malware that locks or encrypts files and demands payment
- C. A type of antivirus software
- D. A network monitoring tool

Answer: B. Malware that locks or encrypts files and demands payment

Explanation: Ransomware encrypts or locks your files and demands a ransom to unlock them.

24. How does ransomware commonly spread?

- A. Through malicious email attachments or infected websites
- B. Only through USB drives
- C. By physical theft of computers
- D. By software updates

Answer: A. Through malicious email attachments or infected websites

Explanation: Ransomware often spreads via phishing emails with infected attachments or by visiting compromised websites.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

25. What happens when your files are infected by ransomware?

- A. They are backed up automatically
- B. You lose access to the files until you pay the ransom
- C. Files are deleted immediately
- D. Files become read-only but accessible

Answer: B. You lose access to the files until you pay the ransom

Explanation: Ransomware encrypts files so they can't be accessed unless the ransom is paid (though paying is risky).

26. Which of the following is the best way to respond to ransomware?

- A. Pay the ransom immediately
- B. Ignore the attack
- C. Restore files from backups and seek professional help
- D. Delete all files manually

Answer: C. Restore files from backups and seek professional help

Explanation: Paying ransom is risky and not recommended. Restoring from Clean backups are the safest approach.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

27. Which type of malware locks your files and demands money?

- A. Virus
- B. Worm
- C. Ransomware
- D. Spyware

Answer: C. Ransomware

Explanation: Ransomware's key characteristic is file encryption with a ransom demand.

28. How can users reduce the risk of ransomware infection?

- A. Opening all email attachments quickly
- B. Regularly updating software and using security tools
- C. Disabling firewalls
- D. Using the same password everywhere

Answer: B. Regularly updating software and using security tools

Explanation: Good security hygiene reduces vulnerability to ransomware attacks.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

29. Which method is a common infection vector for ransomware?

- A. USB charging cables
- B. Malicious email attachments
- C. Printer drivers
- D. Secure VPN connections

Answer: B. Malicious email attachments

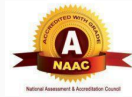
Explanation: Phishing emails with infected attachments are a common way ransomware spreads.

30. What is the main effect of ransomware on your data?

- A. Data is copied to a safe location
- B. Data is permanently deleted
- C. Data is encrypted and inaccessible
- D. Data is shared with friends

Answer: C. Data is encrypted and inaccessible

Explanation: Ransomware encrypts files making them inaccessible until decrypted.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

31. What is spyware?

- A. Software that protects your privacy
- B. Software that secretly monitors your computer activity
- C. A type of virus that deletes files
- D. A file compression tool

Answer: B. Software that secretly monitors your computer activity

Explanation: Spyware runs without the user's knowledge to track activities and steal data.

32. How does spyware commonly spread?

- A. Through official software updates
- B. Bundled with free software or installed unknowingly
- C. Only via email attachments
- D. Through physical device damage

Answer: B. Bundled with free software or installed unknowingly

Explanation: Spyware is often hidden inside free downloads or installed without clear user consent.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

33. What kind of information can spyware steal?

- A. System updates
- B. Personal info like passwords and credit card numbers
- C. Only system logs
- D. Printer settings

Answer: B. Personal info like passwords and credit card numbers

Explanation: Spyware targets sensitive data such as passwords, browsing habits, and financial info.

34. What is a common effect of spyware infection?

- A. Increased computer speed
- B. Unauthorized stealing of personal information
- C. Automatic file backup
- D. Improved battery life

Answer: B. Unauthorized stealing of personal information

Explanation: Spyware compromises user privacy by collecting personal data without consent.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

35. Which of the following is a good way to avoid spyware?

- A. Download software only from trusted sources
- B. Open all pop-up ads
- C. Disable antivirus software
- D. Use the same password for all accounts

Answer: A. Download software only from trusted sources

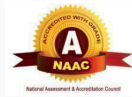
Explanation: Avoiding unknown or untrusted downloads reduces risk of spyware.

36. Spyware is usually installed ____.

- A. with explicit user permission
- B. secretly, without the user's knowledge
- C. only through physical USB devices
- D. when the computer is turned off

Answer: B. secretly, without the user's knowledge

Explanation: Spyware hides its installation and operation from users.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

37. How can spyware affect your computer's performance?

- A. It speeds up processing
- B. It may slow down your system due to extra background activity
- C. It deletes unnecessary files
- D. It improves internet speed

Answer: B. It may slow down your system due to extra background activity

Explanation: Spyware consumes resources, which can degrade system performance.

38. What tool is most effective at detecting spyware?

- A. Firewall
- B. Antivirus or anti-spyware software
- C. Disk defragmenter
- D. Screensaver

Answer: B. Antivirus or anti-spyware software

Explanation: Specialized security tools can detect and remove spyware.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

39. Which behavior might indicate spyware infection?

- A. Frequent pop-up ads and slow computer
- B. Faster startup times
- C. Increased available storage
- D Regular system backups

Answer: A. Frequent pop-up ads and slow computer

Explanation: Spyware often causes unwanted pop-ups and slows system performance.

40. Which practice can help protect against spyware?

- A. Clicking unknown links
- B. Installing only trusted applications
- C. Ignoring security updates
- D. Sharing passwords openly

Answer: B. Installing only trusted applications

Explanation: Being cautious about software installation limits spyware risks.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

41. What is adware?

- A. Software that protects your computer
- B. Software that shows unwanted ads on your screen
- C. Software that deletes files
- D. Software that speeds up browsing

Answer: B. Software that shows unwanted ads on your screen

Explanation: Adware displays unwanted advertisements, often interrupting user activity.

42. How does adware typically spread?

- A. Through bundled free apps or downloads
- B. Only via email attachments
- C. Through physical device damage
- D. Only via official app stores

Answer: A. Through bundled free apps or downloads

Explanation: Adware often comes bundled with free software or gets downloaded without the user's knowledge.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

43. What is a common effect of adware on a device?

- A. Faster device performance
- B. Annoying ads and slower device speed
- C. Automatic file backups
- D. Improved security

Answer: B. Annoying ads and slower device speed

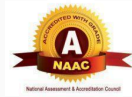
Explanation: Adware slows down devices and causes frequent unwanted ads.

44. Which of the following is usually true about adware?

- A. It is always dangerous and deletes files
- B. It's generally annoying but not harmful
- C. It improves browsing speed
- D. It requires user permission to install

Answer: B. It's generally annoying but not harmful

Explanation: Adware is typically annoying but does not usually cause serious harm.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

45. How can you reduce the risk of getting adware?

- A. Download software from trusted sources only
- B. Click every pop-up ad
- C. Disable your antivirus software
- D. Use public Wi-Fi networks frequently

Answer: A. Download software from trusted sources only

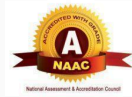
Explanation: Avoiding untrusted downloads reduces the risk of adware infection.

46. What effect can adware have on your browsing habits?

- A. It speeds up page loading times
- B. It may track your browsing habits
- C. It encrypts your data
- D. It blocks all ads

Answer: B. It may track your browsing habits

Explanation: Some adware collects data about your browsing for targeted advertising.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

47. What is a common sign that your computer might have adware?

- A. Increased storage space
- B. Frequent pop-up ads appearing unexpectedly
- C. Faster downloads
- D. System updates

Answer: B. Frequent pop-up ads appearing unexpectedly

Explanation: Adware causes frequent and unwanted pop-up advertisements.

48. Which of these is an effective way to remove adware?

- A. Ignoring the ads
- B. Using anti-adware or antivirus software
- C. Restarting your device repeatedly
- D. Clicking on the ads to stop them

Answer: B. Using anti-adware or antivirus software

Explanation: Specialized security software can detect and remove adware.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

49. What is a Trojan horse in cybersecurity?

- A. A hardware device
- B. Malware disguised as legitimate software
- C. A type of firewall
- D. A backup program

Answer: B. Malware disguised as legitimate software

Explanation: Trojans trick users by appearing safe but contain malicious code.

50. How does a Trojan usually spread?

- A. By being downloaded or run as what seems like safe software
- B. Only through email spam
- C. Through physical damage to the device
- D. Automatically via operating system updates

Answer: A. By being downloaded or run as what seems like safe software

Explanation: Trojans rely on tricking users into installing them, often disguised as normal apps.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

51. What can a Trojan horse malware do once installed?

- A. Protect your data
- B. Open backdoors for hackers
- C. Speed up your computer
- D. Defragment your hard drive

Answer: B. Open backdoors for hackers

Explanation: Trojans often allow attackers to access or control infected systems remotely.

52. How can users protect themselves from Trojans?

- A. Download software only from trusted sources
- B. Disable antivirus software
- C. Click on unknown email links
- D. Ignore system warnings

Answer: A. Download software only from trusted sources

Explanation: Avoiding suspicious downloads reduces the risk of Trojan infection.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

53. What is a "backdoor" in the context of Trojan malware?

- A. A method to update software
- B. A secret access point for hackers
- C. A security patch
- D. A firewall rule

Answer: B. A secret access point for hackers

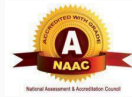
Explanation: Backdoors let attackers bypass normal security controls.

54. Which of these actions can help detect a Trojan?

- A. Regular antivirus scans
- B. Disabling firewalls
- C. Ignoring pop-up warnings
- D. Running unknown apps

Answer: A. Regular antivirus scans

Explanation: Antivirus software can detect and remove Trojans.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

55. Why is Trojan malware dangerous even if it doesn't self-replicate?

- A. Because it damages hardware
- B. Because it can create openings for hackers and steal data
- C. Because it improves system security
- D. Because it speeds up software installation

Answer: B. Because it can create openings for hackers and steal data

Explanation: Trojans enable attackers to control infected systems and steal information.

56. What is a keylogger?

- A. Software that speeds up typing
- B. Malware that secretly records everything you type on your keyboard
- C. A type of antivirus program
- D. Software that encrypts files

Answer: B. Malware that secretly records everything you type on your keyboard

Explanation: Keyloggers capture keystrokes to steal information without user knowledge.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

57. How does keylogger malware commonly spread?

- A. Through bundled malware or phishing attacks
- B. Only through physical access to the keyboard
- C. By updating operating systems
- D. Through secure websites

Answer: A. Through bundled malware or phishing attacks

Explanation: Keyloggers are often installed alongside other malware or via deceptive phishing emails.

58. What kind of data can keyloggers steal?

- A. Passwords, credit card numbers, and personal messages
- B. Only system logs
- C. Software installation files
- D. Screen resolution settings

Answer: A. Passwords, credit card numbers, and personal messages

Explanation: Keyloggers capture sensitive data typed on the keyboard.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

59. Which of the following is a typical effect of keylogger infection?

- A. Improved system speed
- B. Theft of sensitive personal information
- C. Automatic software updates
- D. Enhanced security

Answer: B. Theft of sensitive personal information

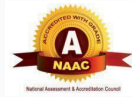
Explanation: Keyloggers compromise privacy by stealing confidential data.

60. Which practice helps reduce keylogger risk?

- A. Clicking on suspicious email links
- B. Keeping your software updated
- C. Using weak passwords
- D. Ignoring security warnings

Answer: B. Keeping your software updated

Explanation: Updates fix vulnerabilities that malware exploits.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

61. Why is it important to keep software up to date?

- A. To slow down your device
- B. To fix security vulnerabilities and bugs
- C. To increase advertising
- D. To reduce internet speed

Answer: B. To fix security vulnerabilities and bugs

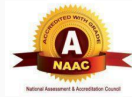
Explanation: Updates patch security holes that attackers could exploit.

62. What does reliable antivirus or anti-malware software do?

- A. Deletes all files
- B. Detects and removes malicious software
- C. Speeds up your internet connection
- D. Creates pop-up ads

Answer: B. Detects and removes malicious software

Explanation: Antivirus software protects your device by finding and eliminating malware.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

63. Why should you be careful with email attachments and links?

- A. They may contain malware or phishing scams
- B. They always improve security
- C. They speed up your device
- D. They never cause harm

Answer: A. They may contain malware or phishing scams

Explanation: Malicious attachments or links can infect your system or steal information.

64. What is the risk of downloading software from untrusted sources?

- A. You get the latest features
- B. You may download malware or unwanted programs
- C. Software runs faster
- D. Software updates automatically

Answer: B. You may download malware or unwanted programs

Explanation: Untrusted sources often distribute malicious or fake software.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

65. What is the purpose of enabling firewall protection?

- A. To allow all network traffic freely
- B. To block unauthorized access to your device or network
- C. To disable antivirus software
- D. To speed up downloads

Answer: B. To block unauthorized access to your device or network

Explanation: Firewalls act as barriers to keep intruders out.

66. What's the risk of using public Wi-Fi without caution?

- A. It is always secure
- B. Attackers can intercept your data or launch attacks
- C. It improves internet speed
- D. It disables firewalls

Answer: B. Attackers can intercept your data or launch attacks

Explanation: Public Wi-Fi can be insecure, making data vulnerable to theft.



Name of the Bundle	Proficient Bundle V1	Subject	Networking V1
Topic	Threats and Prevention & Malware	Last updated on	11 September 2025

67. How does two-factor authentication (2FA) improve account security?

- A. It requires two passwords
- B. It adds an extra step to verify your identity
- C. It removes password requirements
- D. It shares your password with trusted friends

Answer: B. It adds an extra step to verify your identity

Explanation: 2FA requires a second factor (like a code) beyond the password, enhancing security.

68. Why should you avoid pirated or cracked software?

- A. It's free and safe
- B. It may contain malware and violates laws
- C. It improves device performance
- D. It comes with free customer support

Answer: B. It may contain malware and violates laws

Explanation: Pirated software often includes malware and is illegal to use.