Antivirus & Anti-malware Cheatsheet

A quick reference guide to antivirus and anti-malware tools, covering key concepts, types of software, and best practices for system protection.

Core Concepts

Key Definitions

Antivirus (AV)	Software designed to detect, prevent, and remove malware.
Anti-malware	A broader category of software that protects against various types of malicious software, including viruses, worms, trojans, spyware, and ransomware.
Malware	Malicious software designed to disrupt, damage, or gain unauthorized access to a computer system.
Threat Signature	A unique pattern that identifies a specific piece of malware. AV software uses these signatures to detect known threats.
Heuristic Analysis	A method of detecting malware by analyzing its behavior rather than relying solely on signatures. It can identify new or modified threats.
False Positive	Incorrectly identifying a legitimate file or program as malware.

Types of Malware

Viruses	Malicious code that replicates itself by attaching to other files or programs.
Worms	Self-replicating malware that can spread across networks without human interaction.
Trojans	Malware disguised as legitimate software that performs malicious actions when executed.
Ransomware	Malware that encrypts a victim's files and demands a ransom payment for their decryption.
Spyware	Malware that collects information about a user without their knowledge or consent.
Adware	Software that displays unwanted advertisements on a user's computer.

Detection Methods

Antivirus and anti-malware software use various methods to detect malicious software:

- **Signature-based detection:** Identifies known malware based on their unique signatures.
- **Heuristic-based detection:** Analyzes the behavior of files and programs to identify suspicious activities.
- **Behavioral analysis:** Monitors system activities for malicious behavior.
- **Sandboxing:** Executes suspicious files in an isolated environment to observe their behavior without risking the system.

Antivirus Software

Popular Antivirus Solutions

Norton Antivirus	A widely used antivirus software with a comprehensive set of features, including real-time protection, firewall, and password manager.
McAfee Antivirus	Another popular antivirus software offering real-time scanning, web protection, and a variety of security tools.
Bitdefender Antivirus	Consistently ranked among the top antivirus solutions, known for its excellent detection rates and minimal impact on system performance.
Kaspersky Antivirus	A comprehensive antivirus solution offering real-time protection, web filtering, and anti-phishing capabilities.
Avast Antivirus	A free antivirus software with a large user base, offering real-time protection, web protection, and a variety of additional features.
Windows Defender (Microsoft Defender)	The built-in antivirus software in Windows, providing basic protection against malware. It is automatically enabled and updated.

Key Features

Typical features of antivirus software include:

- **Real-time scanning:** Continuously monitors files and programs for malicious activity.
- **On-demand scanning:** Allows users to manually scan specific files or folders.
- **Automatic updates:** Regularly updates the virus definitions to protect against the latest threats.
- **Web protection:** Blocks access to malicious websites and prevents phishing attacks.
- **Firewall:** Monitors network traffic and blocks unauthorized access.
- **Behavioral analysis:** Detects suspicious behavior and blocks potentially malicious programs.

Selecting an Antivirus

When selecting an antivirus solution, consider the following:

- **Detection rate:** Choose a software with a high detection rate for various types of malware.
- **Performance impact:** Select a software that doesn't significantly slow down your computer.
- **Features:** Consider the features that are important to you, such as real-time protection, web protection, and firewall.
- **Price:** Compare the prices of different antivirus solutions and choose one that fits your budget.
- **User reviews:** Read user reviews to get an idea of the software's performance and usability.

Anti-Malware Software

Popular Anti-Malware Solutions

Malwarebytes	A popular anti-malware software that specializes in detecting and removing malware that traditional antivirus software may miss.
SUPERAntiSpyware	An anti-spyware and anti-malware software that detects and removes spyware, adware, trojans, and other types of malware.
Spybot Search & Destroy	A free anti-malware software that detects and removes spyware, adware, and other types of malware. It also offers advanced features for experienced users.
HitmanPro	A cloud-based anti-malware scanner that uses multiple antivirus engines to detect and remove malware.

Key Features

Anti-malware software typically includes features such as:

- **Deep scanning:** Thoroughly scans the system for malware, including hidden and hard-to-detect threats.
- **Real-time protection:** Continuously monitors the system for malicious activity.
- **Behavioral analysis:** Detects suspicious behavior and blocks potentially malicious programs.
- **Rootkit detection:** Detects and removes rootkits, which are malware that hide themselves from the operating system.
- **Removal tools:** Provides tools to remove malware that cannot be removed by traditional antivirus software.

Using Anti-Malware in Conjunction with Antivirus

Anti-malware software is often used in conjunction with antivirus software to provide a more comprehensive level of protection. While antivirus software focuses on preventing malware from infecting the system, anti-malware software specializes in detecting and removing malware that has already bypassed the antivirus protection. Using both types of software can help ensure that your system is fully protected against a wide range of threats.

Best Practices

General Security Tips

- **Keep your software up to date:** Regularly update your operating system, web browser, and other software to patch security vulnerabilities.
- **Use strong passwords:** Use strong, unique passwords for all of your online accounts.
- **Be careful about what you click:** Avoid clicking on links or attachments from unknown senders.
- **Use a firewall:** Enable a firewall to monitor network traffic and block unauthorized access.
- **Back up your data:** Regularly back up your important data to an external hard drive or cloud storage.
- **Enable Two-Factor Authentication (2FA):** Add an extra layer of security to your accounts.

Antivirus/Anti-malware Specific Practices

- **Schedule regular scans:** Schedule regular scans with your antivirus and anti-malware software to detect and remove any malware that may have slipped through.
- **Enable real-time protection:** Enable real-time protection to continuously monitor your system for malicious activity.
- **Keep virus definitions up to date:** Regularly update the virus definitions to protect against the latest threats.
- **Review scan logs:** Review the scan logs to see if any malware was detected and removed.
- **Run a full system scan after a suspected infection:** If you suspect that your system has been infected with malware, run a full system scan with both your antivirus and anti-malware software.

Responding to an Infection

If your system becomes infected with malware, take the following steps:

- **Disconnect from the internet:** Disconnect your computer from the internet to prevent the malware from spreading to other devices.
- **Run a full system scan:** Run a full system scan with both your antivirus and anti-malware software.
- **Quarantine or remove the malware:** Quarantine or remove any malware that is detected.
- **Change your passwords:** Change the passwords for all of your online accounts.
- **Monitor your accounts:** Monitor your accounts for any suspicious activity.
- **Reinstall your operating system (if necessary):** If the malware is particularly persistent or damaging, you may need to reinstall your operating system.