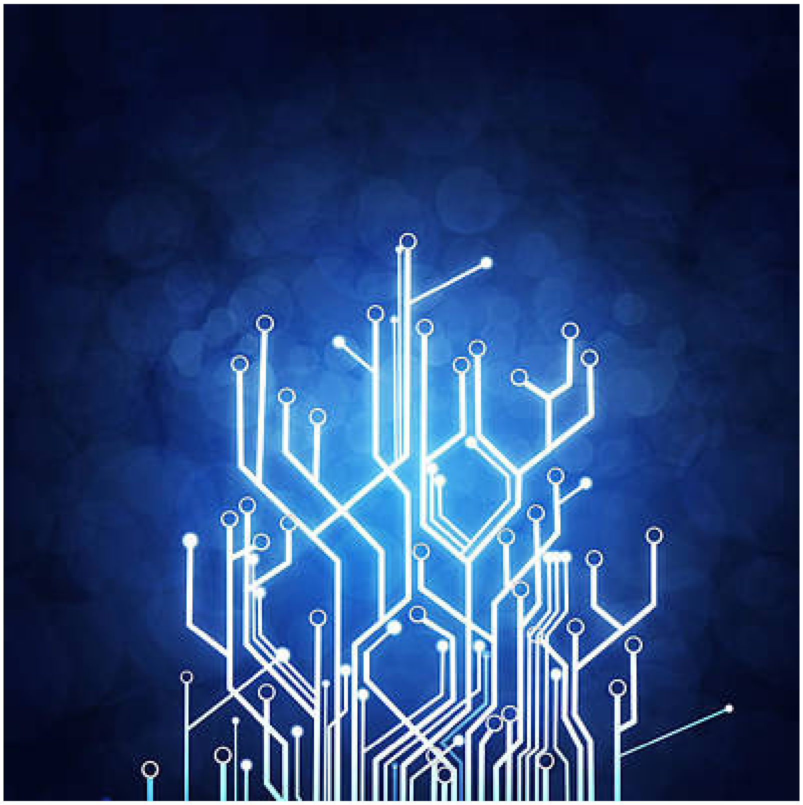
Internet Access Guide

AN OPEN-ACCESS RESOURCE



Introduction

Welcome to the University of Maryland's Student Government Association (UMD SGA) Internet Access Guide! As a student at UMD, you're part of a vibrant community where staying connected is essential for academic success and personal enrichment. This guide has been crafted to help you navigate the complexities of campus internet access, ensuring you can make the most out of the digital resources available. In today's fast-paced world, accessing reliable internet is not just a convenience but a necessity. Whether working on research papers, collaborating with classmates, attending virtual lectures, or simply staying in touch with family and friends, having a seamless online experience is crucial. At UMD, we understand the importance of connectivity in facilitating your educational journey, and we aim to provide you with the tools and information needed to optimize your online experience. From exploring the various Wi-Fi networks available across campus to troubleshooting common connectivity issues, this guide covers everything you need to know about accessing the internet at UMD. We'll walk you through the steps to connect to Wi-Fi in different locations, highlight significant resources for troubleshooting technical problems, and offer tips for staying secure online. Whether you're a new student navigating campus for the first time or a returning student looking to enhance your digital experience, this guide is designed to be your go-to resource for all things internet-related at UMD. As your representatives in the Student Government Association, we are committed to ensuring that your voice is heard and your needs are met. If you have any questions, concerns, or suggestions regarding internet access on campus, don't hesitate to contact us. We're here to support you every step of the way as you embark on your academic journey at the University of Maryland.

— University of Maryland, Student Government Association

Table of Contents

6. Antivirus Software

Introduction and Support

The Division of Information Technology here on campus works closely with the HelpDesk. The hours are as follows:

1. Service Desk
   Phone: 301.405.1500, itsupport@umd.edu
   Telephone support hours: Monday-Thursday 8 a.m.-10 p.m., Friday 8 a.m.-6 p.m., Weekend 12 p.m.-4:00 p.m.

2. Live Chat and email hours: Monday-Thursday 8 a.m.-10 p.m., Friday 8 a.m.-6 p.m., Weekend 12 p.m.-4:00 p.m.

3. Terrapin Tech (Computer sales and support)
   Phone: 301.314.7000, terpstore@umd.edu
   We are located on the ground floor of the Edward St. John Learning and Teaching Center (ESJ).

4. Monday-Friday, 8:30 a.m.-8 p.m.

5. Campus Information Services
   Phone: 301.405.1000
   Telephone support hours: Monday-Thursday 8 a.m.-10 p.m., Friday 8 a.m.-6 p.m.

6. Classroom Support
   Phone: 301.405.2500, classrooms@umd.edu
   Monday-Thursday 7:30 a.m.-10 p.m., Friday 7:30 a.m.-5 p.m.

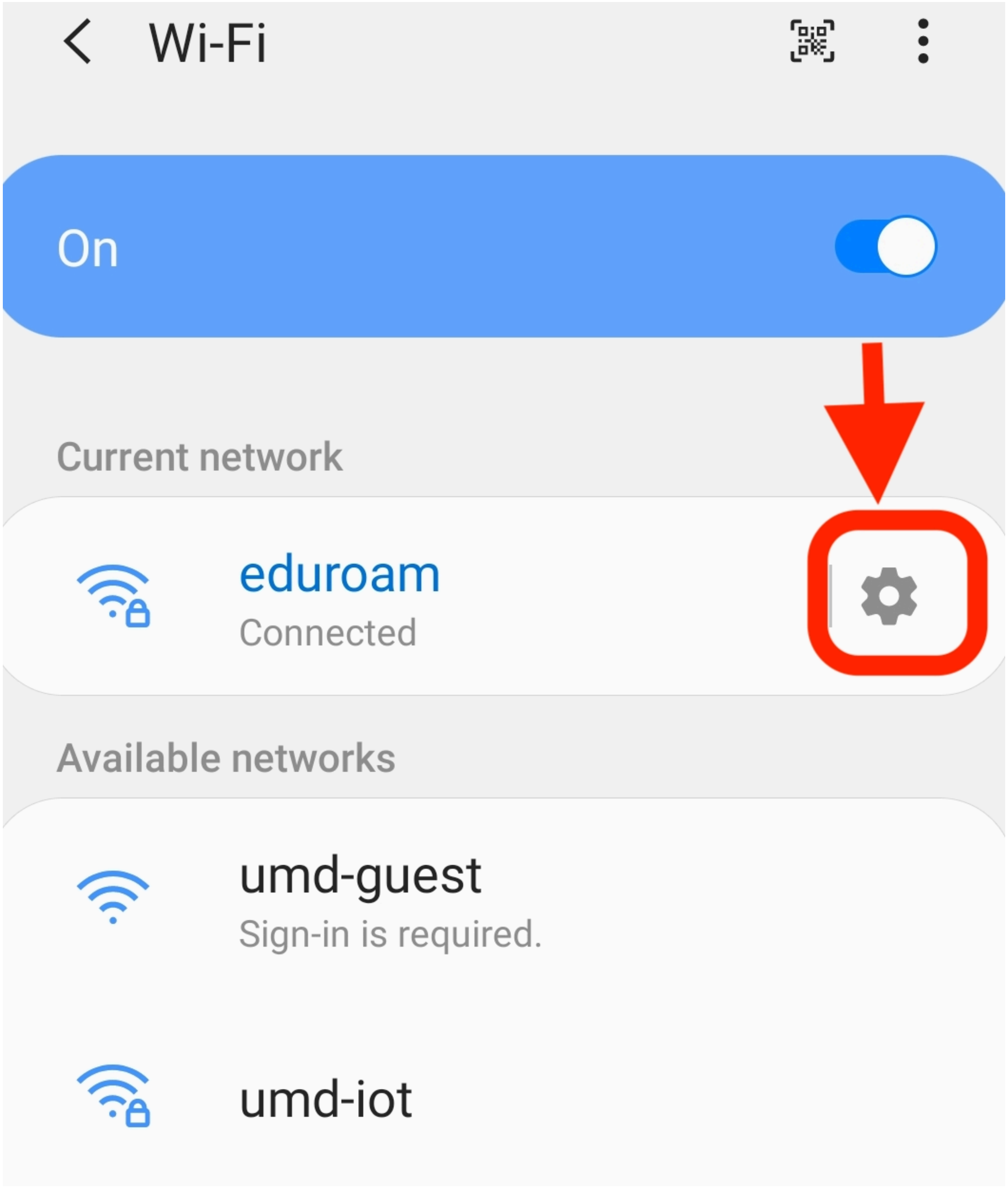
You can also open a ticket directly by visiting https://itsupport.umd.edu/itsupport!

What is Advised to Include:

1. Directory ID: This is needed to assign the ticket to you. This is the part of your email address before the "@" symbol.

2. Building: What building do you live in on-campus (or just say "commuter" if you don't live on campus network residence hall)
3. Room: Your UMD room or Apartment number.
4. Phone Number: We need your best contact phone number, which is very important!
5. Hours of availability: When can we contact you for troubleshooting? Tell us so we can sync up!
6. MAC Address: If Wired or Wireless, the MAC Address will be helpful. See the respective Troubleshooting sections to get the MAC Address and other network information for the ticket if needed.
7. Jack ID (if wired): Your Wired/Ethernet Jack in your room usually has a label above or below it; let us know what that is.
8. Network name (if wireless): What wireless network are you having issues connecting to? Do any of them work? Are you using your email address to log in to EDUROAM?
9. Date/Time of issue: Let us know if you remember experiencing the problem. This helps us look through logs and focus on the time of the issue.
10. Description of the issue: What is not working? Are they wired or Wireless? When did the problem start? Is there a pattern to the issue occurring or not occurring? Did you have a problem registering? Give whatever details you feel are relevant, but know that the more accurate a description you give us, the better chance we have of resolving the issue quicker for you!

UMD Wifi



UMD provides three wireless internet connectivity networks on campus: eduroam, umd-guest, and umd-iot. *UMD students, faculty, and staff should use eduroam to connect to UMD's Wi-Fi service with cell phones and laptops.*

EduROAM:

SecureW2 should be launched before connecting a device for the first time or after a Directory ID passphrase update.

Or

Open the network selection screen of your device
Tap or click eduroam from the list of detected wireless networks.
Log in using your DirectoryID@umd.edu (even if that is not the email address you use) in the User Name field and your DirectoryID password.
Click Join, Connect, or OK, depending on your device.
A Verify Certificate window may open depending on your device.
Click Continue or Trust to authenticate the server certificate.
Android users may need to use the following settings:

1. EAP method: PEAP
2. Phase-2 authentication: MSCHAPV2
3. CA certificate: Select "Use system certificates" (if this option is not available, please try SecureW2 or contact the Division of IT Service Desk)
4. Domain: wireless.umd.edu
5. Identity: DirectoryID@umd.edu (even if that is not the email address that you use)
6. Anonymous identity: (leave blank)
7. Password: your directory ID password

Umd-guest:
Using a device that can receive SMS text messages (cellphone)

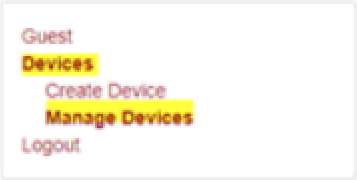
Choose the umd-guest network option and follow the prompts to request an account.
Wait for a text message (you may need to leave the library to receive the text)
Access the text message to get your 24-hour username and password
Sign on!
You can use your username and password to sign on with up to 3 devices. (Guest WiFi accounts are for use on your devices and cannot be used on Public PCs)

Guest Wi-Fi accounts expire after 24 hours. You can repeat the process if you need additional time.

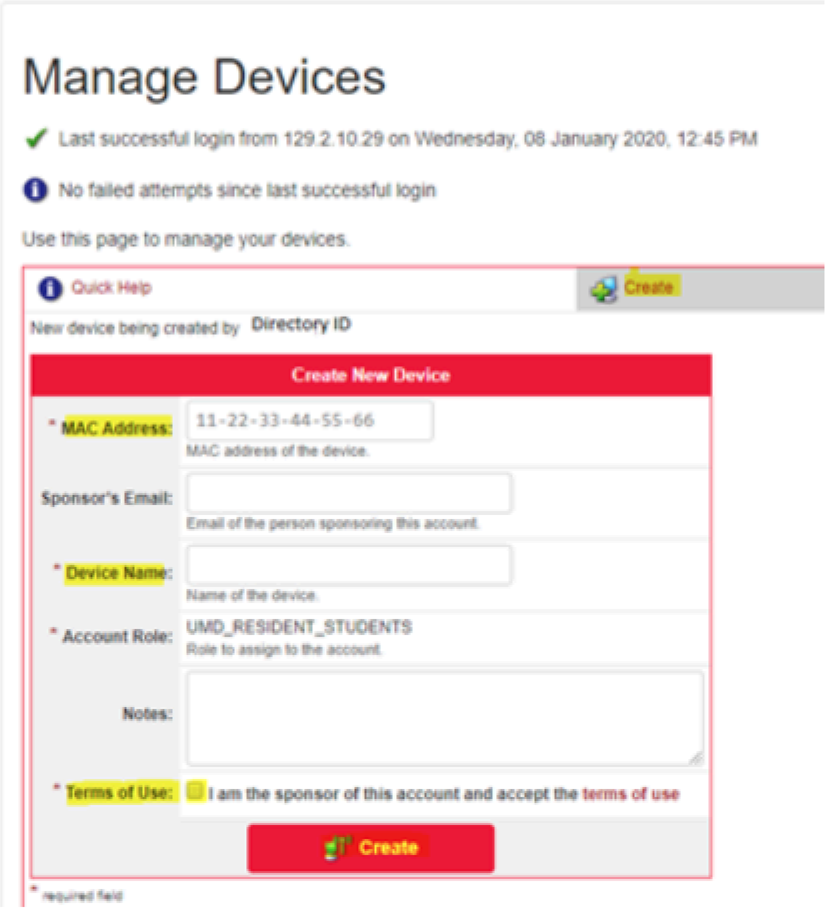
If you cannot connect to the umd-guest wireless network, you may use the public computers available in all campus Libraries. Please visit a service point to request a guest login account.

All university faculty and staff may provide Sponsored Accounts to personal guests if they wish to do so. (Library staff do not sponsor guest Wireless Accounts).

Device Registration



Guest
Devices
Create Device
Manage Devices
Logout



Manage Devices

✓ Last successful login from 129.2.10.29 on Wednesday, 08 January 2020, 12:45 PM

No failed attempts since last successful login

Use this page to manage your devices.

New device being created by Directory ID

Create New Device

* MAC Address:	11-22-33-44-55-66 MAC address of the device.
Sponsor's Email:	Email of the person sponsoring this account.
* Device Name:	Name of the device.
* Account Role:	UMD_RESIDENT_STUDENTS Role to assign to the account.
Notes:	
* Terms of Use:	□ I am the sponsor of this account and accept the terms of use

* required field

To enroll your network device on the WIRED/Ethernet network, you'll need to retrieve its MAC Address (also known as Physical Address) and proceed to http://mydevices.net.umd.edu. This platform is accessible both on and off campus. It's important to note that this system exclusively caters to WIRED/ETHERNET connections; WIRELESS Devices or MAC Addresses are incompatible, and attempting to register them will yield no results. For instance, an Amazon Echo won't function on the UMD Wireless network, regardless of registration. Upon reaching the initial page, you'll be prompted to enter your username and password. Your username corresponds to your Directory ID, a component of your UMD email address preceding the "@" symbol. The password aligns with this username. On campus, you might come across UID (User ID), the numerical sequence on the front of your UMD ID Card.

Following login, you'll encounter the Acceptable Use Policy. Review the terms thoroughly and opt to Accept to proceed. Alternatively, you can Decline, thereby nullifying subsequent steps. This stage involves registering your device's MAC Address. It's advisable to briefly peruse the bullet points on this page, particularly the bold/red note concerning a display anomaly. To register your device, click on ADD. Mandatory fields include Device Name and Device ID. A description is optional. Device Name can be any designation you prefer; it simply requires an entry. The device ID is where the MAC (Physical) Address should be entered. Please note that a MAC (Physical) Address may encompass numerals 0-9, letters A, and symbols such as periods, colons, and dashes for separation.

ITAC

DIVISION OF INFORMATION TECHNOLOGY

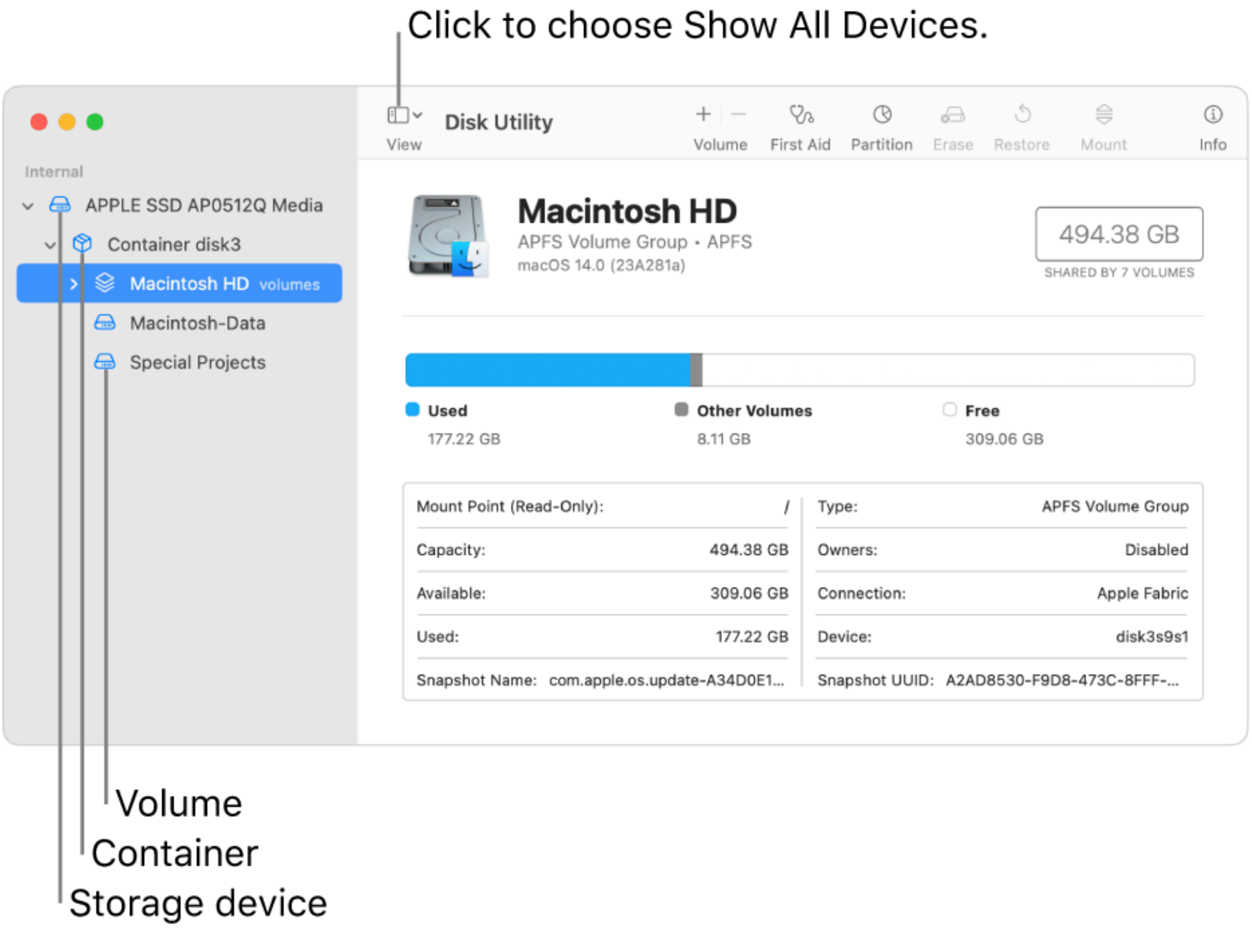
The Student IT Advisory Committee (ITAC) provides recommendations to the Vice President of Information Technology and Chief Information Officer (VP/CIO) about student access to information technology. Topics may include, but are not limited to:

1. campus-wide project proposals that help enhance the campus-wide student technology environment

2. communicating students' perspectives about the marketplace relating to information technology

ITAC will make IT-related recommendations at the University of Maryland based on the input of all colleges, departments, and centers. Its goal is to work with the entire university community to constantly improve and upgrade needed IT services to enhance the experience for all students, faculty, and staff. ITAC has its own website.

Device Security


Click to choose Show All Devices.

Macintosh HD
APFS Volume Group • APFS
macOS 14.0 (23A281a)

494.38 GB
SHARED BY 7 VOLUMES

● Used 177.22 GB
● Other Volumes 8.11 GB
○ Free 309.06 GB

Mount Point (Read-Only):	/	Type:	APFS Volume Group
Capacity:	494.38 GB	Owners:	Disabled
Available:	309.06 GB	Connection:	Apple Fabric
Used:	177.22 GB	Device:	disk3s9s1
Snapshot Name:	com.apple.os.update-A34D0E1...	Snapshot UUID:	A2AD8530-F9D8-473C-8FFF-...

Volume
Container
Storage device

Please make sure to note the MAC address on your wireless laptop or device. In the unfortunate event of losing your device, UMD may track it using the MAC Address to assist in its recovery. Keep this MAC Address securely stored in your phone, email, or a safe location, such as a notepad.

Antivirus Software

A firewall acts as a barrier between your device and the internet, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. Here's why enabling firewall protection is essential:

1. Blocking Unauthorized Access: A firewall blocks unauthorized access attempts to your device or network from external sources, such as hackers or malware. It filters incoming traffic to ensure that only legitimate connections are allowed.

2. Protection Against Cyber Threats: Firewalls can block known malicious IP addresses, prevent unauthorized access to vulnerable services or ports, and detect and block suspicious network traffic patterns.

3. Defense in Depth: Firewalls complement other security measures, such as antivirus software and intrusion detection systems, to provide layered protection against cyber threats. They add a barrier of defense to your device and network.

4. Customizable Security Rules: Modern firewalls often allow users to customize security rules based on their specific needs and preferences. You can configure firewall settings to block or allow traffic from particular IP addresses, ports, or applications.

Antivirus software is designed to detect, prevent, and remove malicious software, such as viruses, worms, trojans, spyware, and ransomware, from infecting your devices. Here's why it's crucial:

1. Detection: Antivirus software monitors your device for suspicious activity or files. It scans files, programs, and emails for known malware signatures or behavioral patterns that indicate malicious intent.

2. Prevention: Antivirus software often includes real-time protection features that can block malware from infecting your device. It may also include web protection to block access to malicious websites and phishing attempts.

3. Removal: If malware is detected on your device, antivirus software can quarantine or remove the malicious files to prevent further damage.

4. Regular Updates: Antivirus software relies on regularly updated virus definitions to detect and remove the latest threats effectively. Keep your antivirus software updated to protect against new and emerging malware threats.