

Module 3:

Software

Troubleshooting



Module 3

Software Troubleshooting



Module 3

Learning Objectives

Identify and recommend solutions to Windows operating system issues.

Identify and remediate PC security issues.

Summarize best practice procedures for malware removal.

Explain and identify appropriate solutions to common mobile operating systems and application issues.

Explain and identify appropriate solutions to common mobile operating systems and application security issues.

Table of Contents

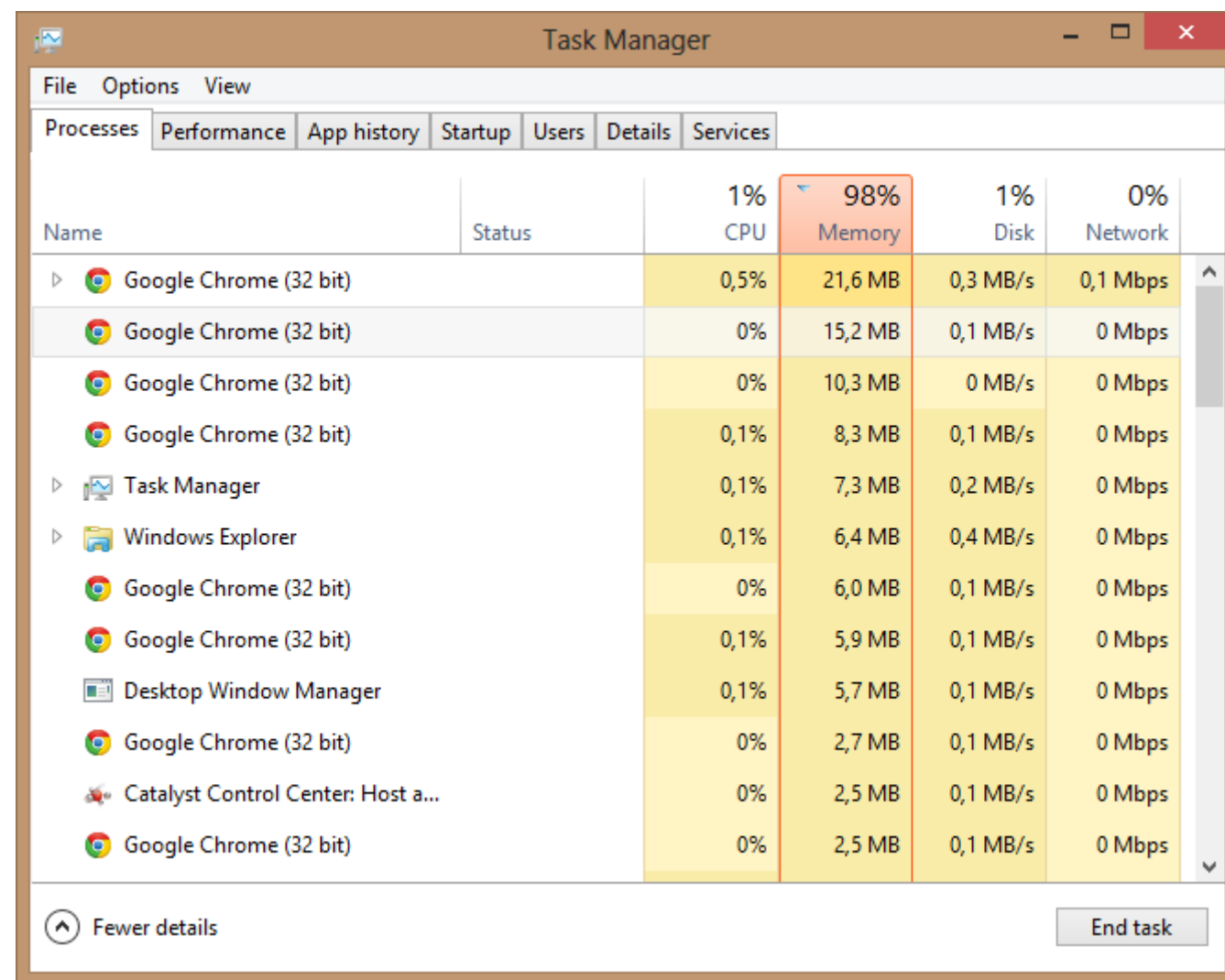
- 1 Windows OS Problems
- 2 PC Security Issues
- 3 Mobile OS and Application Issues
- 4 Mobile OS and Application Security Issues

Topic: Windows OS Problems

In this section, we will cover:

- Common Symptoms & Warnings
- Boot Order/Sequencing
- Master Boot Record (MBR) Corruption
- Bluescreen of Death (BSOD)
- Kernel Panic
- Common Troubleshooting Steps
- Initial Actions (Reboot, Restart, Reinstall)
- Additional Resources
- OS Management
- Patching
- Updates
- Rollback
- Print Spooler

common symptoms and warnings



The screenshot shows the Windows Task Manager window with the 'Performance' tab selected. The 'Memory' section is highlighted, showing a usage of 98%. Below this, a list of running processes is displayed with columns for Name, Status, CPU, Memory, Disk, and Network. The processes listed include multiple instances of Google Chrome (32 bit), Task Manager, Windows Explorer, Desktop Window Manager, and Catalyst Control Center: Host a... The memory usage for each process is shown in the 'Memory' column.

Name	Status	1% CPU	98% Memory	1% Disk	0% Network
Google Chrome (32 bit)		0,5%	21,6 MB	0,3 MB/s	0,1 Mbps
Google Chrome (32 bit)		0%	15,2 MB	0,1 MB/s	0 Mbps
Google Chrome (32 bit)		0%	10,3 MB	0 MB/s	0 Mbps
Google Chrome (32 bit)		0,1%	8,3 MB	0,1 MB/s	0 Mbps
Task Manager		0,1%	7,3 MB	0,2 MB/s	0 Mbps
Windows Explorer		0,1%	6,4 MB	0,4 MB/s	0 Mbps
Google Chrome (32 bit)		0%	6,0 MB	0,1 MB/s	0 Mbps
Google Chrome (32 bit)		0,1%	5,9 MB	0,1 MB/s	0 Mbps
Desktop Window Manager		0,1%	5,7 MB	0,1 MB/s	0 Mbps
Google Chrome (32 bit)		0%	2,7 MB	0,1 MB/s	0 Mbps
Catalyst Control Center: Host a...		0%	2,5 MB	0,1 MB/s	0 Mbps
Google Chrome (32 bit)		0%	2,5 MB	0,1 MB/s	0 Mbps

1

- Sluggish performance
- System instability
- Frequent shutdowns
- Applications crashing
- Services not starting
- Slow profile load
- Low memory warnings
- USB controller resource warnings

2

Many of the warnings may indicate additional issues.

boot order/ sequencing



1

The boot sequence is a sequential list of locations to load the OS from. If it finds the boot sector and boot information, it will start loading the OS. If no boot sector is found, it moves to the next device. If it finds a bootable device but no boot file, it stops looking. This can result in a “No OS Found” error.

2

You can change these settings in the BIOS/UEFI of a computer. A boot order/sequence includes standard storage drives, optical drives, USB drives (any type), and networks (PXE).

master boot record (MBR) corruption

— A **master boot record (MBR)** corruption is when a sector in the MBR becomes corrupted.

During master boot record (MBR) corruption, a computer might be unable to boot to the OS.

— Common Errors:

- Invalid Partition Table
- No Bootable Devices Found
- Error Loading Operating System
- A Black Screen

Try using the bootrec commands like bootrec/fixmbr to repair any bad sectors in the hard drive where the OS is stored.

Bluescreen of Death (BSOD)



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

1

The most common **Bluescreen of Death (BSOD)** is due to device drive errors; however, malware infections can cause BSOD.

2

You can set the "Kernel Dump," which will write a file to your computer to review later.

kernel panic



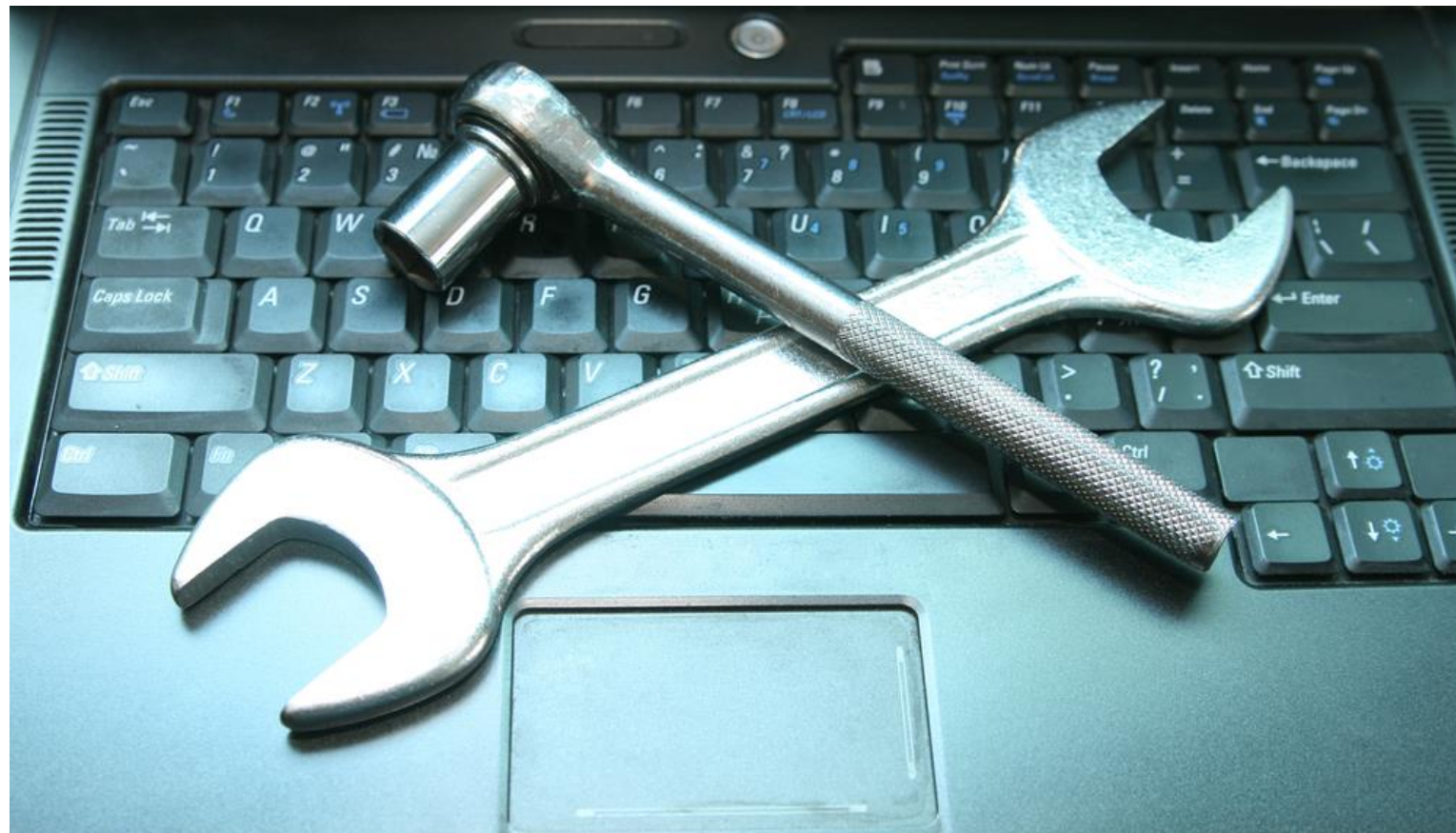
A **kernel panic** is a screen that displays as the computer is shutting off due to a malfunction.



A kernel panic happens in Mac devices, for example, when the computer is malfunctioning; it is the same as the Windows BSOD.

Be sure to record any error codes to research common symptoms and solutions to the issue.

common troubleshooting steps



Initial actions (reboot, restart)

Uninstall/reinstall/update

Add resources

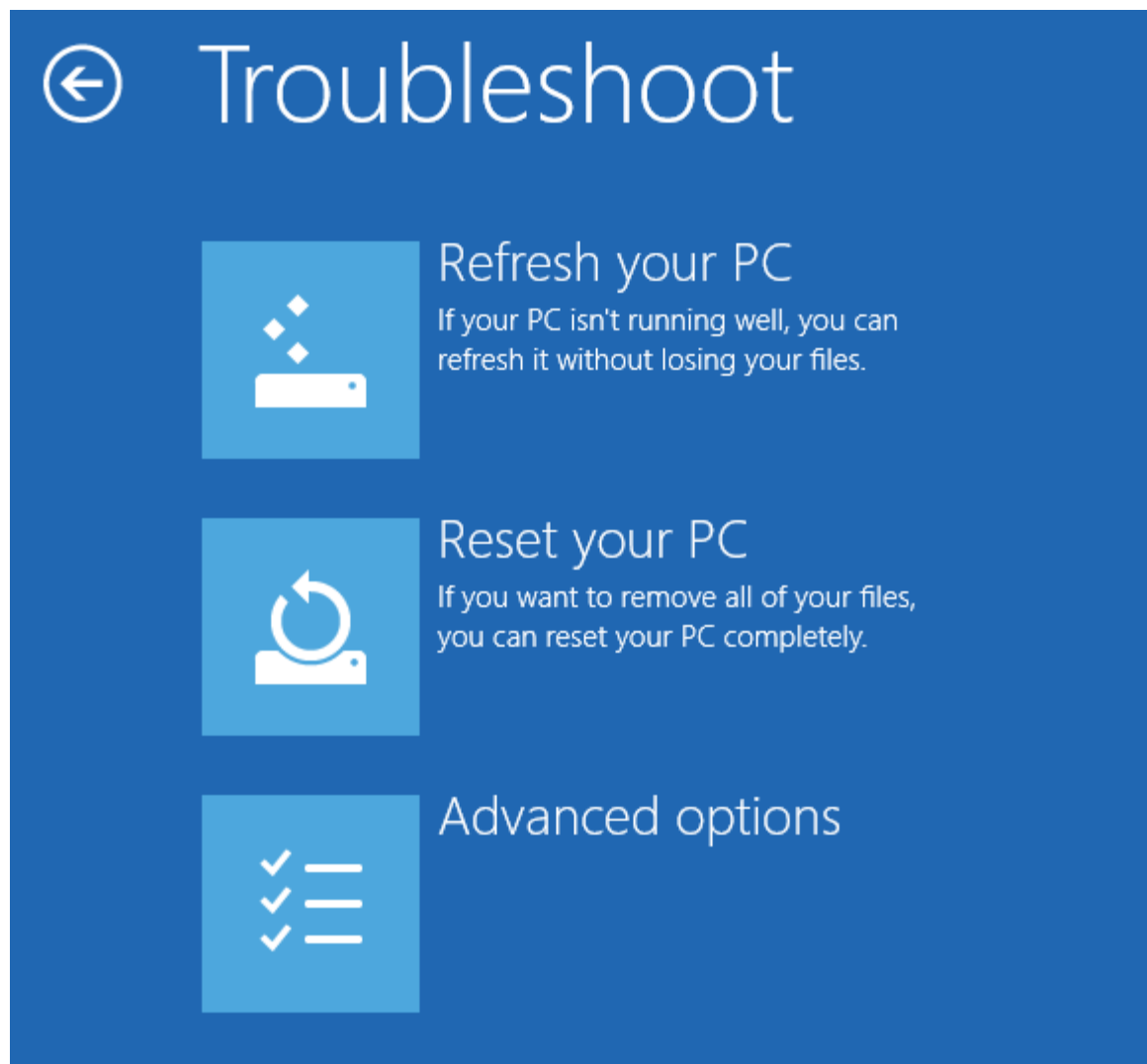
OS Management steps:

- Verify system requirements
- System file check
- Windows/restore/reimage
- Rollback updates
- Rebuild Windows profiles

Based on the symptoms, take appropriate action.

Where in the boot process did it stop?
Does it fail early, after login, or later?

initial actions (reboot, restart, reinstall)



1

Reboot (Safe Mode) can be entered when you first start the computer up. Be sure to press the correct keyboard button when instructed. You can use safe mode with or without the internet.

2

Restart services
Uninstall/reinstall/update
applications

patching



1

When a vendor has a few changes to their software, they will release a **minor** update to fix all of the small issues at different times.

Note: The term “updating” is frequently used with patching, but technically an “update” is when they have major revisions – normally jumping to the next full version number, such as moving from version 3.3 to 4.0.

2

It is recommended that all updates and patches are tested before implementing them into a production environment. Once tested, it should be implemented immediately to address vulnerabilities.

updates



1

When a vendor has a lot of changes to their software, they will release a major update to remediate the discovered vulnerabilities.

2

It is recommended that all updates and patches are tested before implementing them into a production environment. Once tested, it should be implemented immediately to address vulnerabilities.

rollback



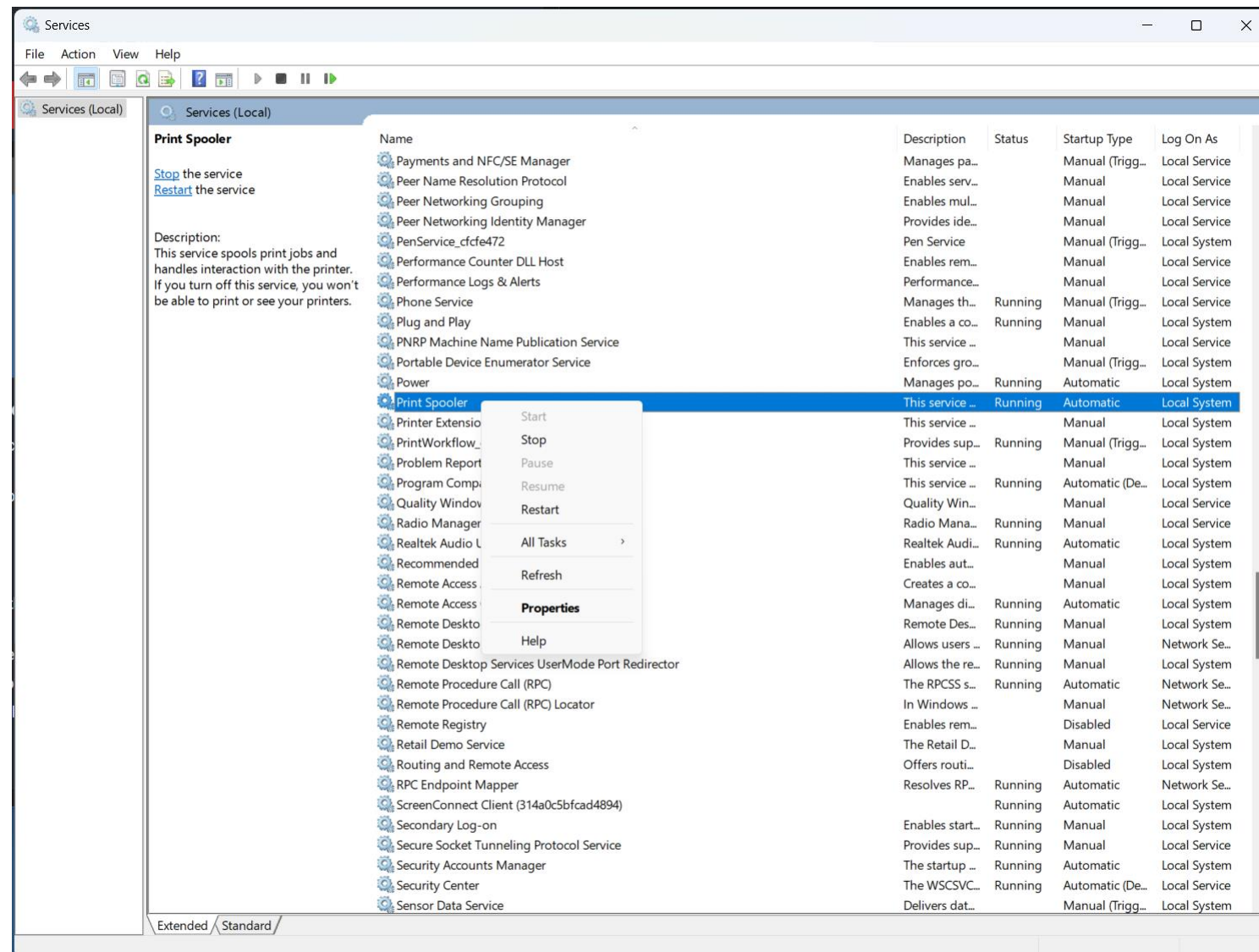
1

Some device driver or application updates can become corrupted or interact unexpectedly, causing performance issues; you can roll back the update items to previous versions.

2

Device drivers can be rolled back from the Device Manager menu and applications from their property menu. A rollback is a way to use the previous device driver or application.

print spooler



1

Upon starting a print job, the print job is sent to the print spooler. You can cancel, restart, or continue printing an item from the print queue. There is usually a printer icon in the notification area until the job is complete. This is a simple way to view and manage the queue.

2

As a standard user, you can cancel some print jobs, but generally, a user with administrator privileges will need to cancel print jobs that become stuck. The print spooler, located in Services, can be used for troubleshooting printing issues.

Topic: PC Security Issues

In this section, we will cover:

- Common Symptoms
- Browser-Related Symptoms
 - Pop-Ups
 - Security Alerts
 - Certificate Warnings
 - Browser Redirection

common symptoms

1

- Unable to access the network
- Desktop alerts.
- False alerts regarding antivirus protection.
- Altered system or personal files.
- Missing/renamed files
- Unwanted notifications within the OS.
- OS update failures.

2

Knowing how to spot a real versus fake alert will be important:

- False Negatives
- False Positives
- True Negatives
- True Positives

browser-related symptoms

1

- Random/frequent pop-ups
- Security alerts
- Certificate warnings
- Browser redirection

pop-ups



A pop-up is a small window that opens as a warning or notification.

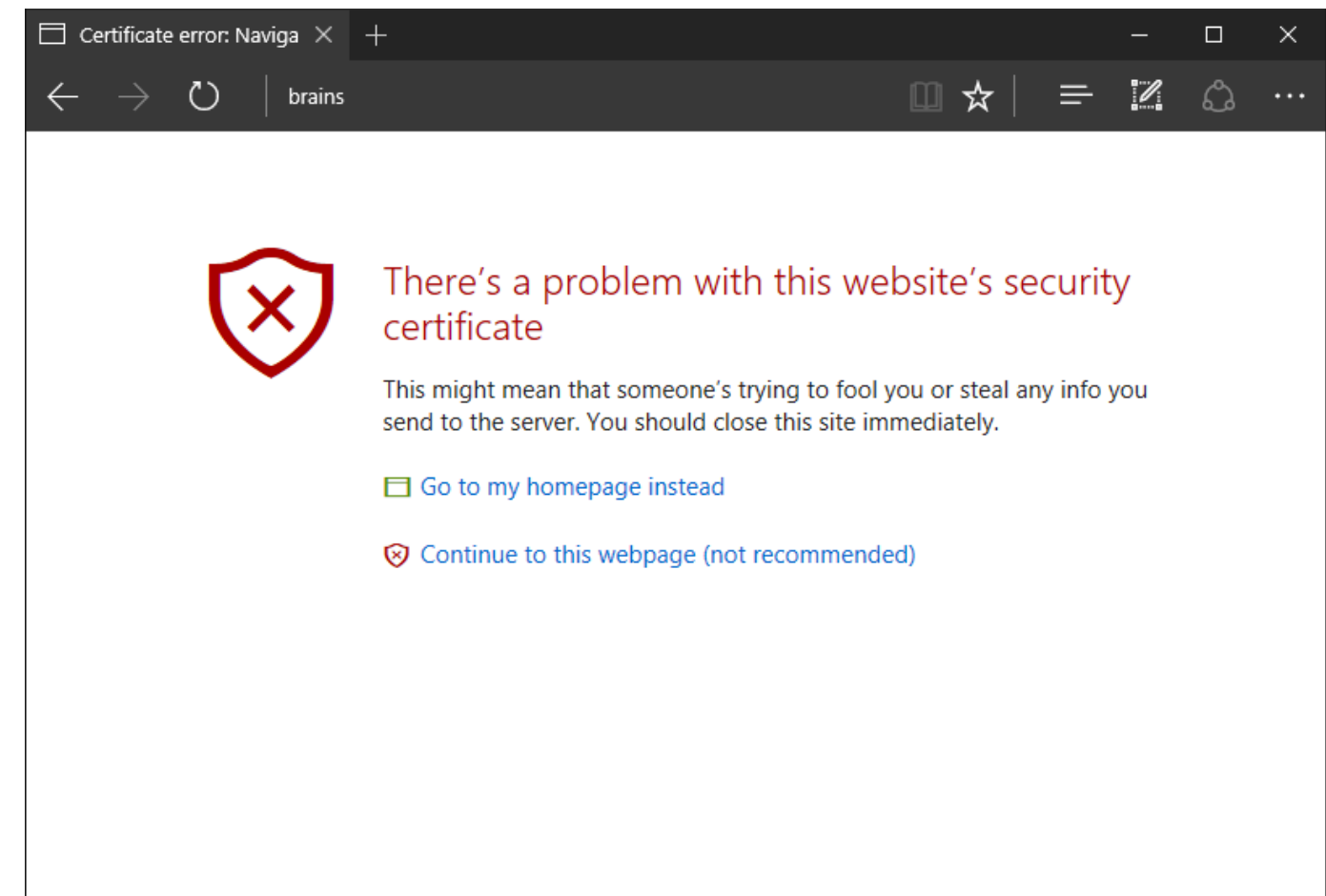


Usually, a pop-up is used to display separate actions that need to be done by the user. Pop-ups may be maliciously caused by malware. Pop-up windows may also be system related and not malicious.

certificate warnings

Certificate warnings occur when there is no valid certificate or the certificate for the website has expired.

Shown below is a typical certificate warning.



browser redirection



Browser redirection is an intentional or unintentional redirection to another website.



A hacker using malware can cause you to be redirected to another website than the one to which you originally intended.

Most commonly, the DNS records of websites have been infected with malware or manipulated.

Topic: Malware Removal

In this section, we will cover:

- Investigate and verify malware symptoms
- Quarantine infected systems
- Disable System Restore in Windows
- Remediate infected systems
- Schedule scans and run updates
- Enable System Restore and create a restore point in Windows
- Educate the end user

Investigate: Notification windows, poor performance, unusual behavior, system/app crashes.

Verify: Is the notification legitimate? Is the poor performance just old hardware? Research the symptoms of known malware at anti-malware vendor sites.

**Investigate and
verify malware
symptoms**

Malware Removal

- ✓ **Investigate and verify**
- ✓ Quarantine
- ✓ Disable
- ✓ Remediate
- ✓ Schedule scans/updates
- ✓ Enable
- ✓ Educate

Quarantine: Remove the system from all network connections. This is not just the wired connection. Remove from all wireless connections as well; WiFi, Bluetooth, and mobile data.

Detach and contain: all removable storage media needs to be disconnected and contained to ensure it is not re-connected to other devices.

Quarantine Infected Systems

Malware Removal

- ✓ Investigate and verify
- ✓ **Quarantine**
- ✓ Disable
- ✓ Remediate
- ✓ Schedule scans/updates
- ✓ Enable
- ✓ Educate

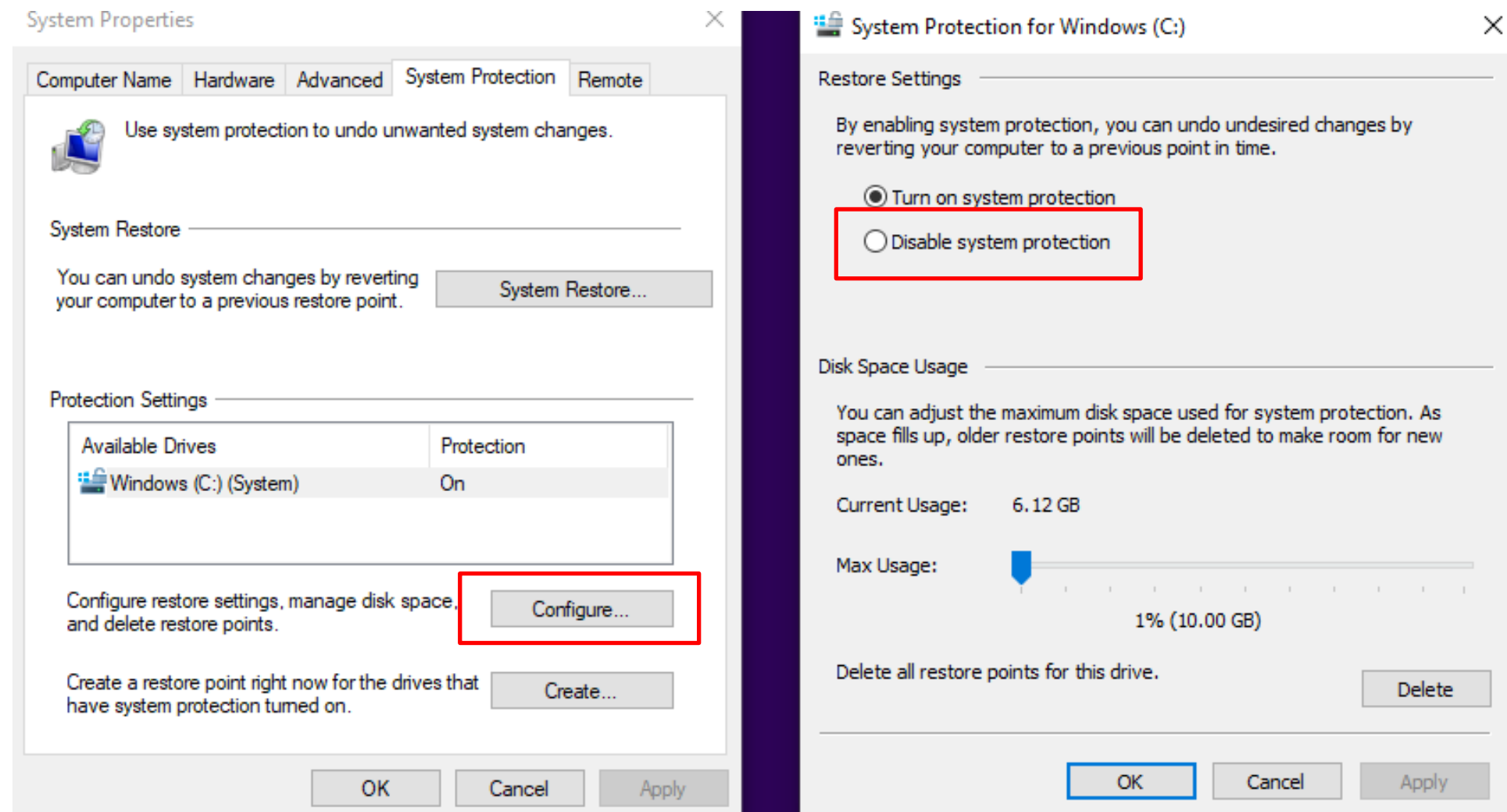
Disable System Protection: Windows has a handy, simple tool to restore your system to a previous state. While this is beneficial at times, you will want to disable it immediately so no new restore points are captured and so that a restore operation isn't triggered during remediation since the restore points are possibly infected.

Disable System Restore (1 of 2)

Malware Removal

- ✓ Investigate and verify
- ✓ Quarantine
- ✓ **Disable**
- ✓ Remediate
- ✓ Schedule scans/updates
- ✓ Enable
- ✓ Educate

Disable System Protection:



Malware Removal

- ✓ Investigate and verify
- ✓ Quarantine
- ✓ **Disable**
- ✓ Remediate
- ✓ Schedule scans/updates
- ✓ Enable
- ✓ Educate

Disable System Restore (2 of 2)

Update: An anti-malware application and its signature files must be updated frequently. These files should be gathered from an uninfected system and then transferred using removable media. This prevents the malware from causing from interfering with the update process.

Malware Removal

- ✓ Investigate and verify
- ✓ Quarantine
- ✓ **Disable**
- ✓ Remediate
- ✓ Schedule scans/updates
- ✓ Enable
- ✓ Educate

Remediate Infected Systems (1 of 2)

Scan and remove: run the installed anti-malware application to scan and remove the malware. Some malware, such as rootkits, are very difficult to remove, and there are guides for the removal of these specific types of infections.

May require: using Safe-mode; Pre-installation environment via isolated network or removable media; boot records repair.

Malware Removal

- ✓ Investigate and verify
- ✓ Quarantine
- ✓ Disable
- ✓ **Remediate**
- ✓ Schedule scans/updates
- ✓ Enable
- ✓ Educate

Remediate Infected Systems (2 of 2)

Schedule future scans and updates: Setup a schedule for scans and turn on automatic updates. This includes checking that Windows Updates is set to automatically update.

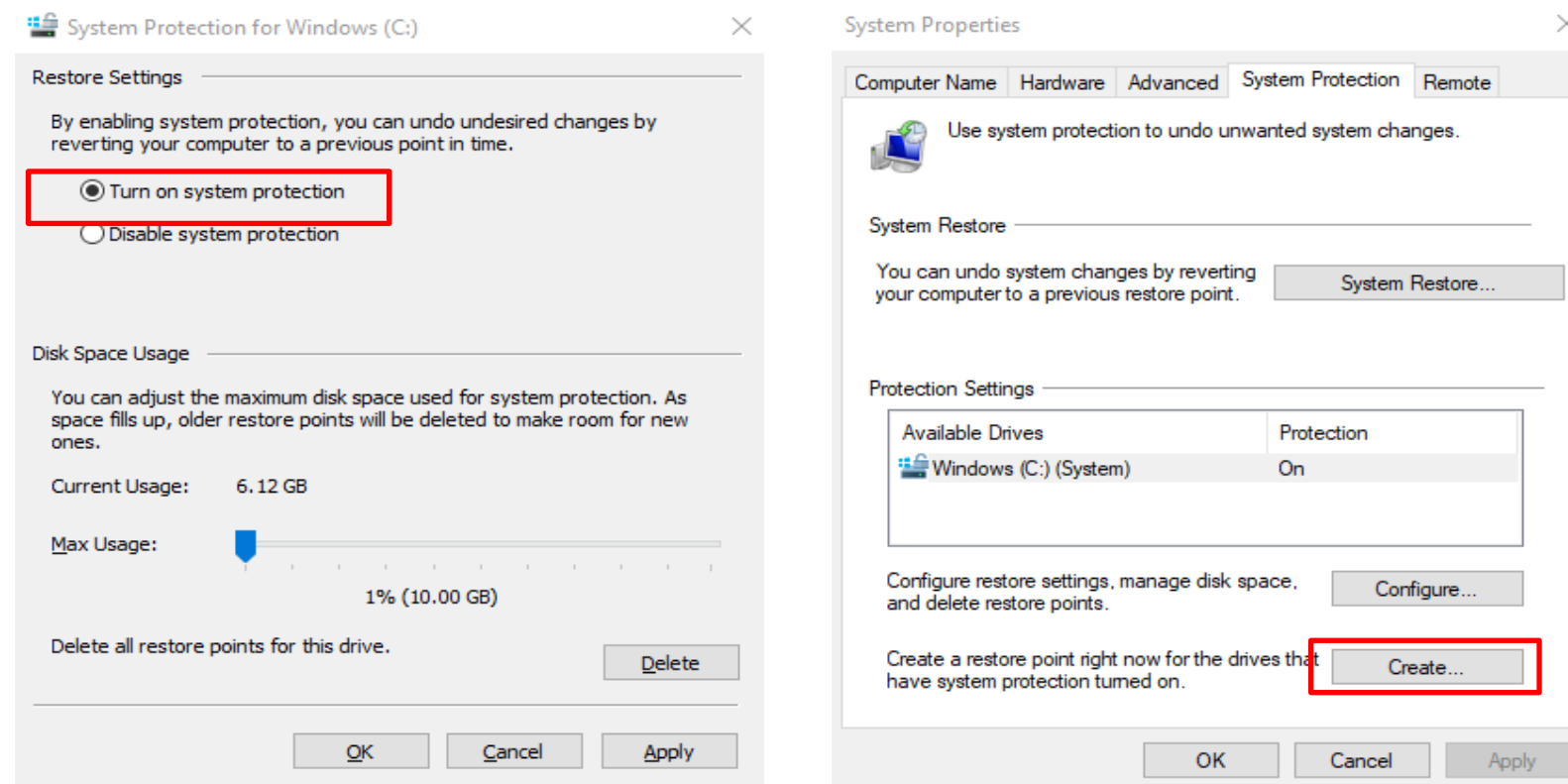
Many free versions of anti-malware do not have this option, which may require an upgrade to a paid version.

Schedule Scans and Updates

Malware Removal

- ✓ Investigate and verify
- ✓ Quarantine
- ✓ Disable
- ✓ Remediate
- ✓ **Schedule scans/updates**
- ✓ Enable
- ✓ Educate

Enable/Configure System Protection: Ensure that System Protection is re-enabled or enabled for the first time. Once configured, click the Create button to create a new Restore Point.



Enable System Restore

Malware Removal

- ✓ Investigate and verify
- ✓ Quarantine
- ✓ Disable
- ✓ Remediate
- ✓ Schedule scans/updates
- ✓ **Enable**
- ✓ Educate

Malware Removal

Educate: The End-Users involved must be trained on the policies and procedures, and a regular organization-wide refresher is recommended.

- ✓ Investigate and verify
- ✓ Quarantine
- ✓ Disable
- ✓ Remediate
- ✓ Schedule scans/updates
- ✓ Enable
- ✓ **Educate**

Educate the End-User

Topic:

Mobile OS and Application Issues

In this section, we will cover:

- Common Mobile OS and Application Symptoms
- Connectivity Issues

common mobile OS and application symptoms

1

- Application fails to launch
- Application fails to close/crashes
- Application fails to update
- Slow to respond
- OS fails to update
- Battery life issues
- Randomly reboots
- Screen does not autorotate

2

Any or all of these are signs that something needs to be investigated and corrected.

connectivity issues

1

Connectivity Issues:

- Bluetooth
- Wi-Fi
- Near-field communication (NFC)
- AirDrop

2

Test all of these before returning the unit(s) back to the end user.
Ensure company policies for these are followed.

Topic:

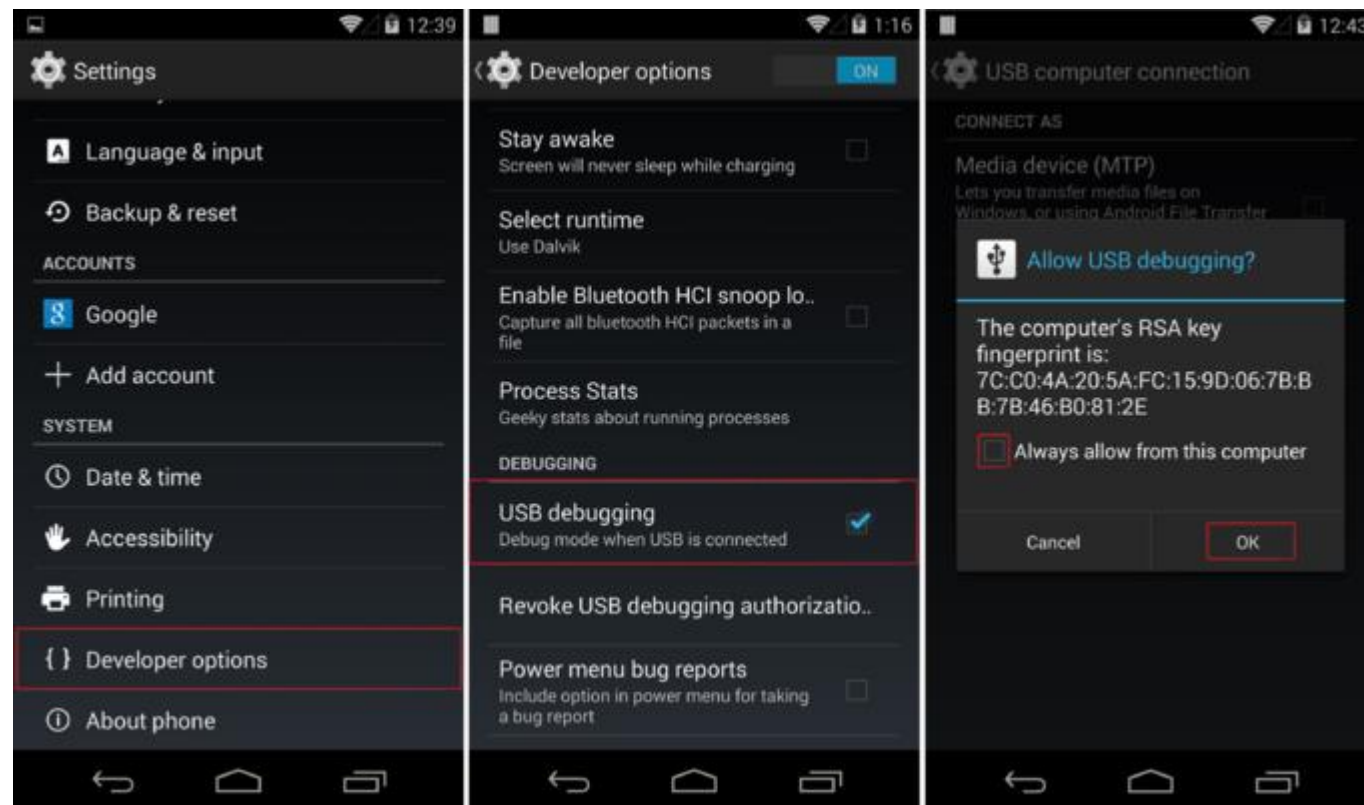
Mobile OS and Application Security Issues

In this section, we will cover:

- Developer Mode
- Root Access/Jailbreak
- Android Package (APK)
Source
- Bootleg/Malicious
Application

Developer Mode

Great for developers but really is better described as administrator mode.



Developer mode is like logging in to a computer as an administrator. You now have access to programs and settings that can cause problems, from a simple misconfiguration to allowing malware-laden software to be installed.

root access / jailbreak

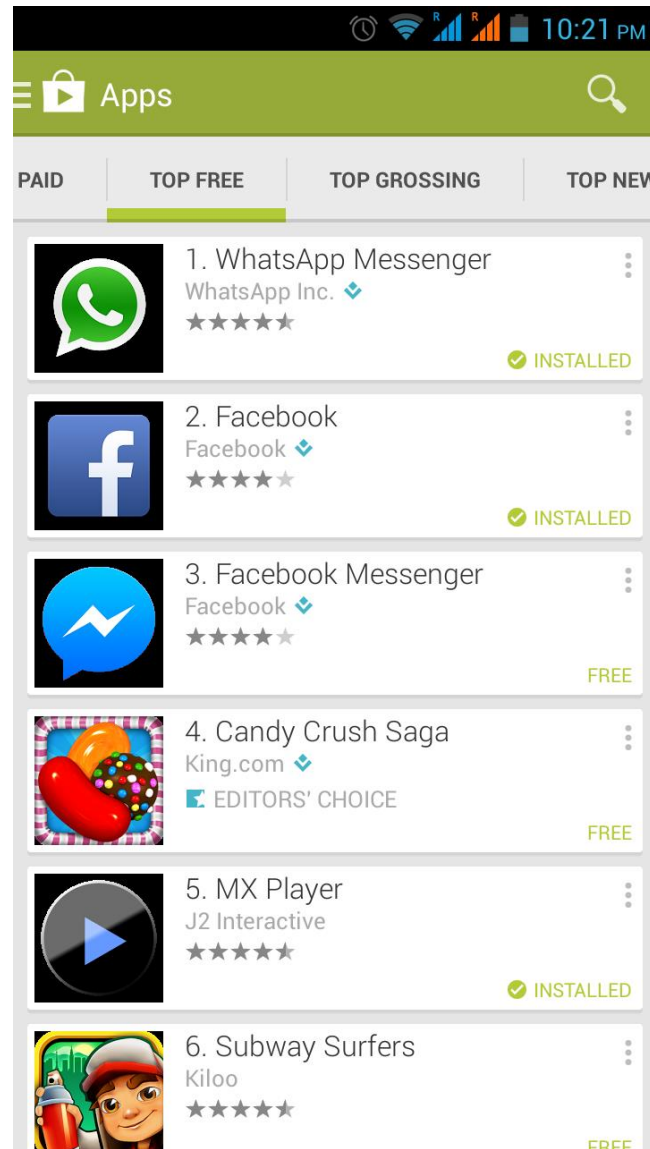


Benefits and risks must be weighed.

Rooting your mobile device is like logging in to a computer as an administrator, like developer mode, except the change is permanent. Similar to logging into a linux system as the root user.

Rooting a mobile device enables you to replace the operating system with a new one. It will no longer be protected by the preinstalled OS and may void your warranty.


Android package (APK) source




APKs are the software packages used to install applications on Android devices.

Care must be taken when installing packages that it is downloaded from a trusted source, for example, from Google Playstore.

bootleg/ malicious application



Bootleg software is illegally distributed software. These types of software normally contains malware or may not perform the function it was intended for.

- 
- Bootleg applications
 - Malicious Applications
 - Application spoofing due to lower security checks

common symptoms for mobile OS & applications

1

- High network traffic
- Sluggish response time
- Data-usage limit notification
- Limited Internet connectivity
- No Internet connectivity
- High number of ads
- Fake security warnings
- Unexpected application behavior
- Leaked personal files/data

summary

In this module, we covered:

- Windows OS Problems
- PC Security Issues
- Mobile OS and Application Issues
- Mobile OS and Application Security Issues