Cyber Security for SOHO Environments

Where did this material come from?

In February of 2023; The National Security Agency (United States of America) created a Public Security Advisory for all United States citizens to secure their home network against possible cyber-attacks.

Since the small office threat model generally shares a similar amount of attack vectors, we have built on this Public Service Advisory; adding on updates and personal takes on known security vulnerabilities, to make a Guide updated for current times.

Defence Strategy

Let us say that each “hackable point”, i.e. in layman terms, everything that is vulnerable to a virus, is a bulls’ eye/target. And obviously, there are very many ways each device can fall prey to a virus.

The more the number of targets, the more likely it is to hit one; likewise, the more vulnerabilities you have, the more likely you are to get hacked.

Remember; everything from Cars to Mobiles to Computers are running on millions of lines of programming; so **everything can be hacked!**

Defence Strategy

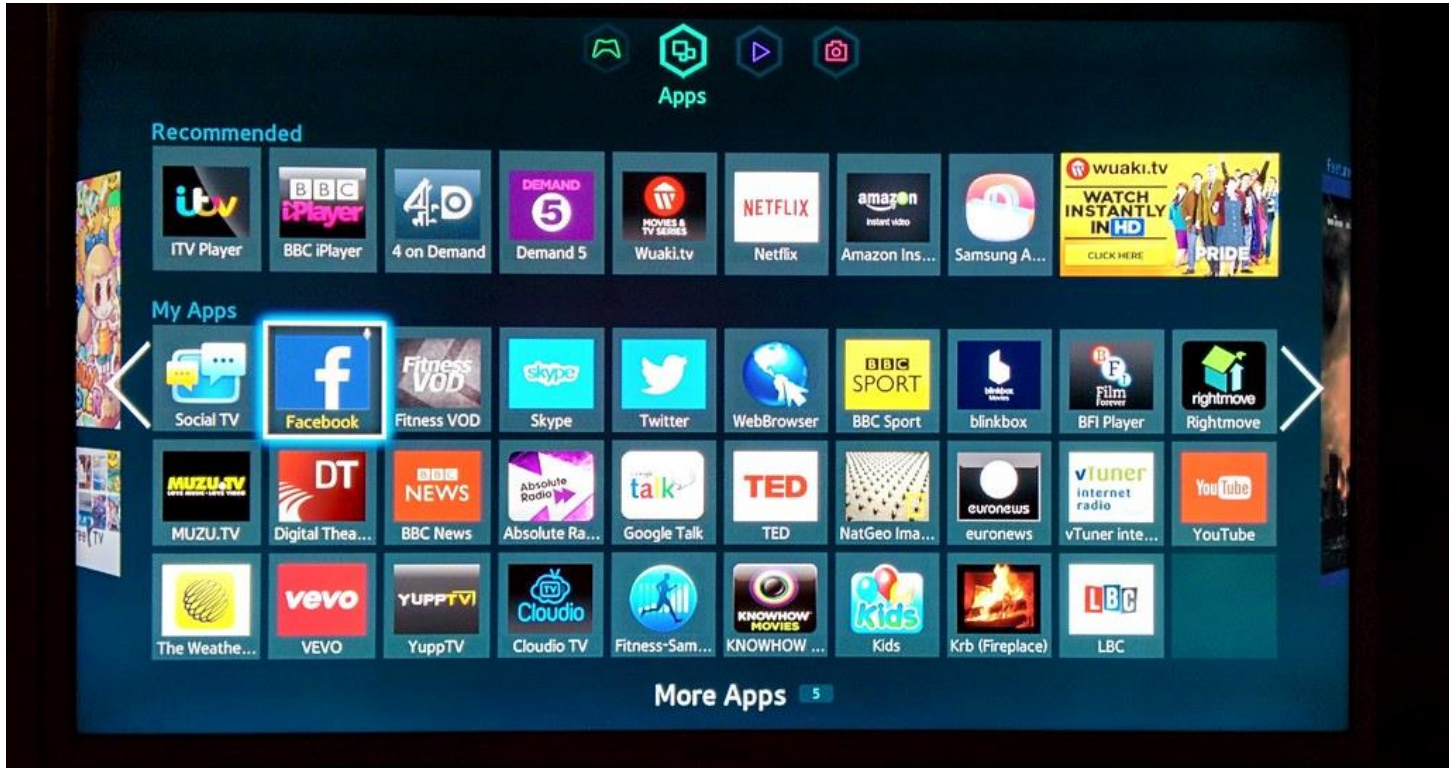
Now each device that communicates with others, is an “endpoint”. For securing a home network; we have to secure **each and every endpoint.**

There are 4 major endpoint categories in an average home:

1. Smart Devices
2. Mobile Devices
3. Router/Modem
4. Desktops and Laptops

Remember; everything from Cars to Mobiles to Computers are running on millions of lines of programming; so **everything can be hacked!**

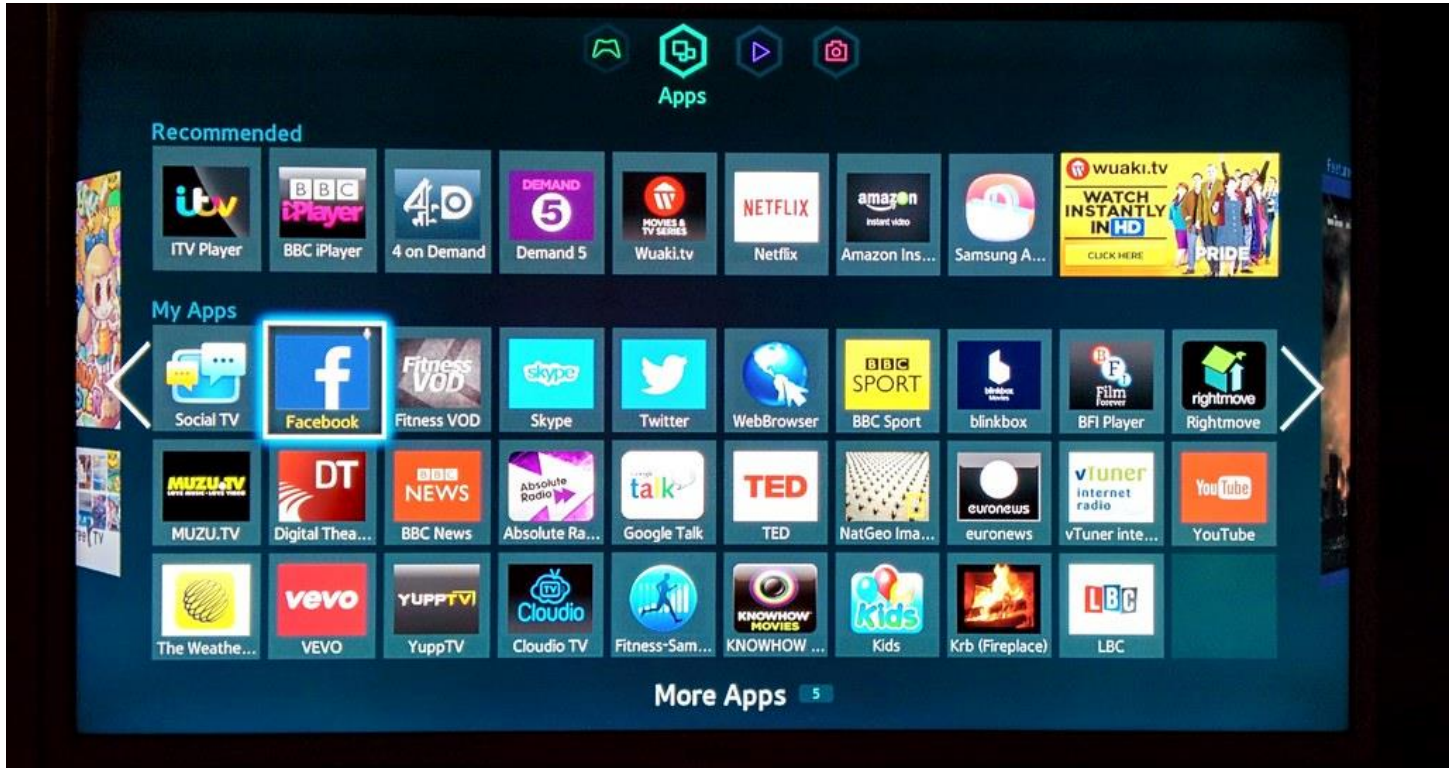
Securing Smart Devices



Smart Devices refer to devices such as a Smart TV, Smart Lighting, Voice Assistants, etc. These are commonly targeted; as they are the easiest to exploit and can become powerful spyware/prank tools.

Since we connect them to the main Wi-Fi; they also become a “landing point” for an attacker to launch a further attack onto some other devices on the network.

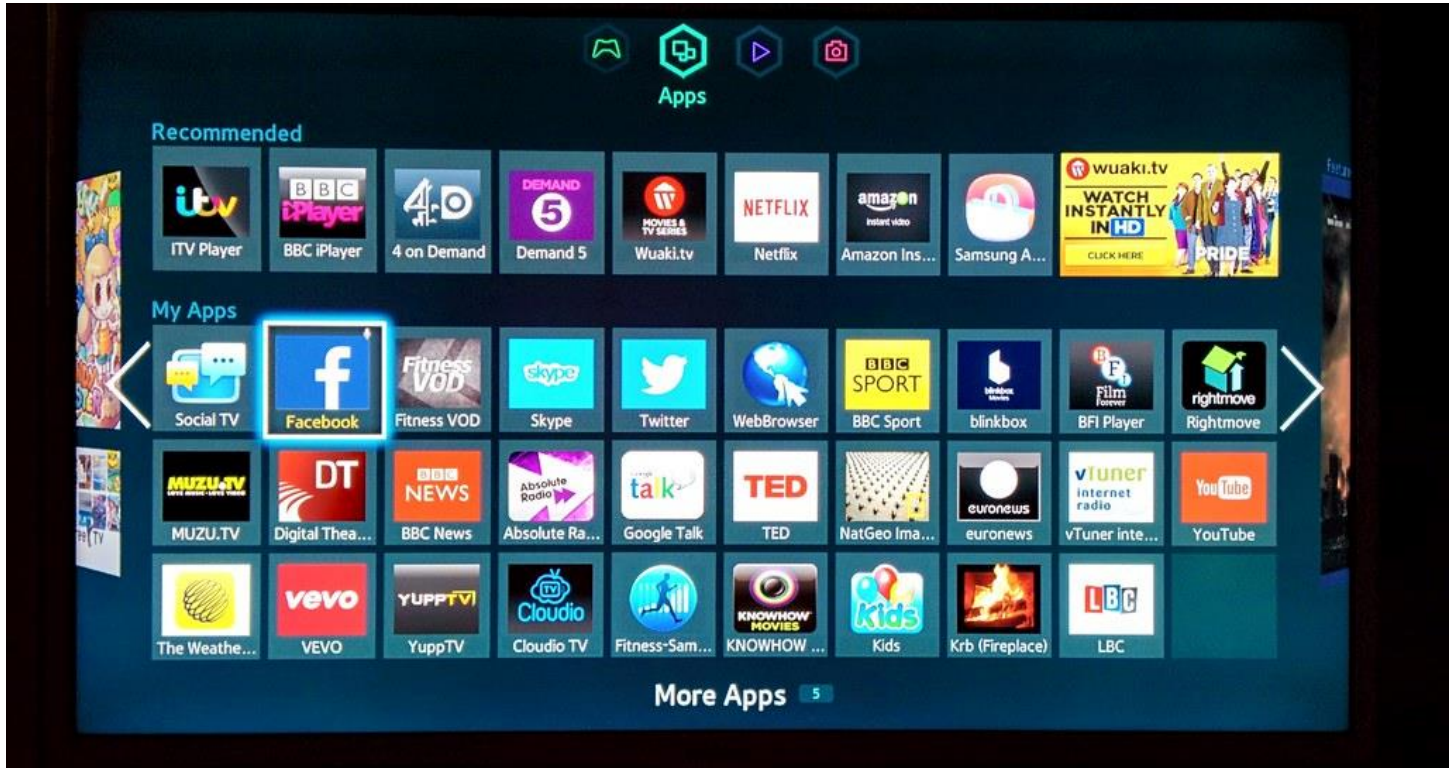
Securing Smart Devices



Zigbee/Zwave: These are systems to take Smart Devices **off the Wi-Fi network,** by connecting them to the internet via another device, like Homey**.**

These devices are generally more secure than routers; and even if cracked, your other devices **are not discoverable**. You will need a home automation service to set this up for your office/home.

Securing Smart Devices

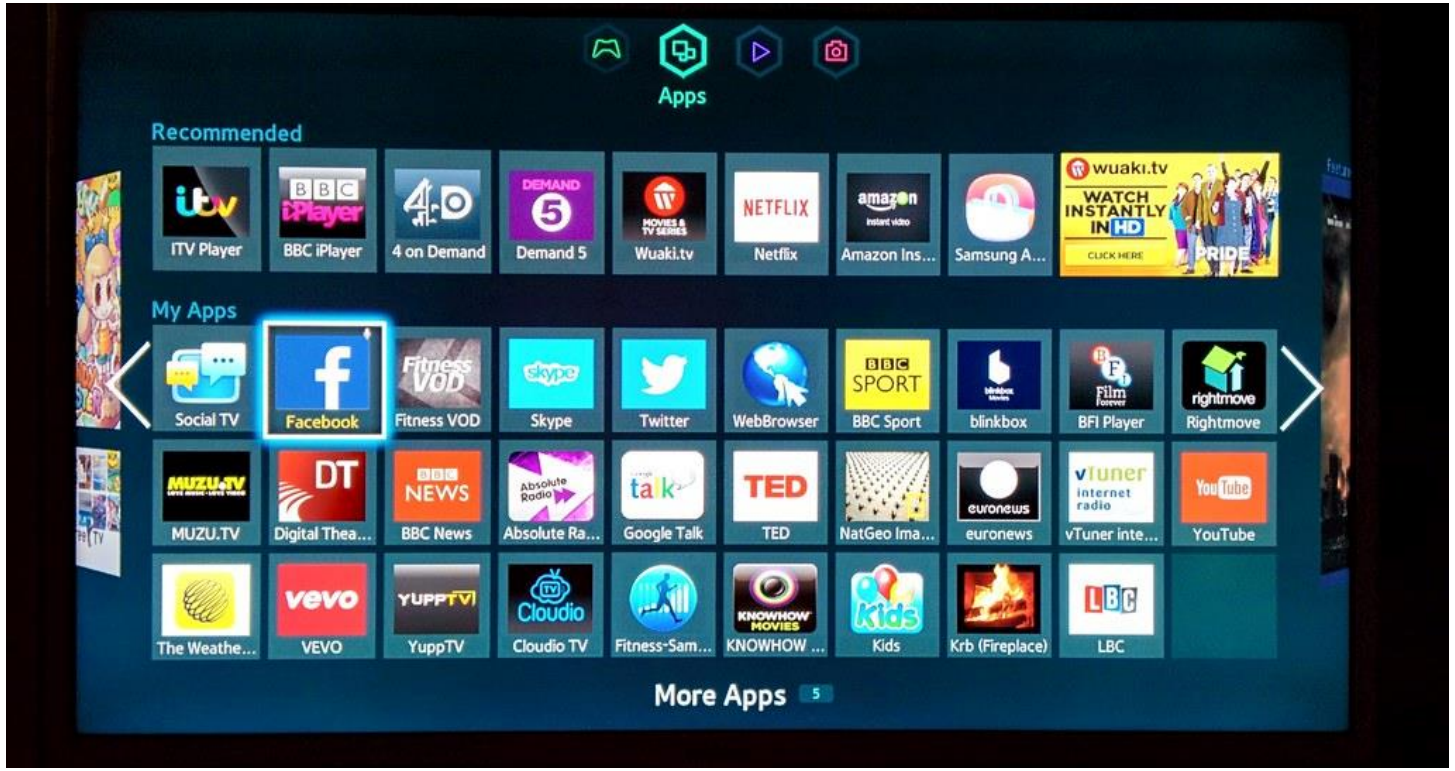


More tips:

2. Changing default credentials: Credentials for admin login to smart devices are often kept at default by the persons who set it up; whether it is consumer or vendor. This is *extremely poor security*.

3. Auto-updating device firmware: Just like our computers, Smart TV are also running on Operating Systems applications that will regularly have vulnerabilities, so it is important to patch them as soon as possible.

Securing Smart Devices



How to Update the 2:

Both 2 and 3 can easily be configured from Settings menu in the Smart TV.

Example for #2:
Settings > Support > Software Update and select Auto Update

Example for #3:
Settings > All Settings > General & Privacy > System Manager > Change PIN. Enter 0000 OR 1234 (one of the two should work) > Enter custom pin.

It is similar for all smart devices.

Securing Web Browsers

Web browsers are one of the two biggest cyber security vulnerabilities; since they are one of the two points that are used for every interaction over the internet.

They are also more vulnerable than other softwares, since they have to run unknown code in the form of websites and web apps.

Think about it, when we download an application we have some idea about who made it and what it's like; but what do we **verifiably** know about the sites we open?

Securing Web Browsers

Common browser attacks include:

1. Fileless malware (cyber attack is built into bad website; so you don't have to download or click anything to get hacked),
2. Tabnabbing: When a user switches tabs and returns to an inactive tab, the content of the tab is replaced with a malicious page
3. Cross-site scripting, where cyber attacks are injected into trusted websites

Among many, many others.

Securing Web Browsers

Firefox is recommended, due to its features such as:

1. **Enhanced Tracking Protection (ETP)**: Blocks trackers, cookies, fingerprints, and cryptomining scripts by default.
2. **Better Extensions Market:** Many great security extensions, such as Ublock Origin, are not available on browsers such as Chrome
3. Ease of Usage: Unlike more secured browsers, there is barely any technical proficiency required to use FireFox.

Securing Web Browsers

Here's how to make it even more secure:

1. **Disable Firefox telemetry:** Go to **Open Menu** (three bars at the top right corner) **> Options > Privacy & Security > Firefox Data Collection and Use.**

   Uncheck all boxes here.
2. **Block Potentially Malicious Content**: Go to **Menu > Options > Privacy and Security > Content Blocking;** and select **"Strict".**

3. **Turn on HTTPS-only mode:** Click Firefox on the menu bar, hit Preference and find Privacy & Security on the left menu. Scroll down and click HTTPS-Only Mode.

Securing Web Browsers

Caveat: You can disable content blocking for certain sites by clicking Disable content blocking for specific sites; Simply enter the website URL, then click the "i" icon to the left of the address bar, then click the grey button to "**Turn off Blocking for This Site**."

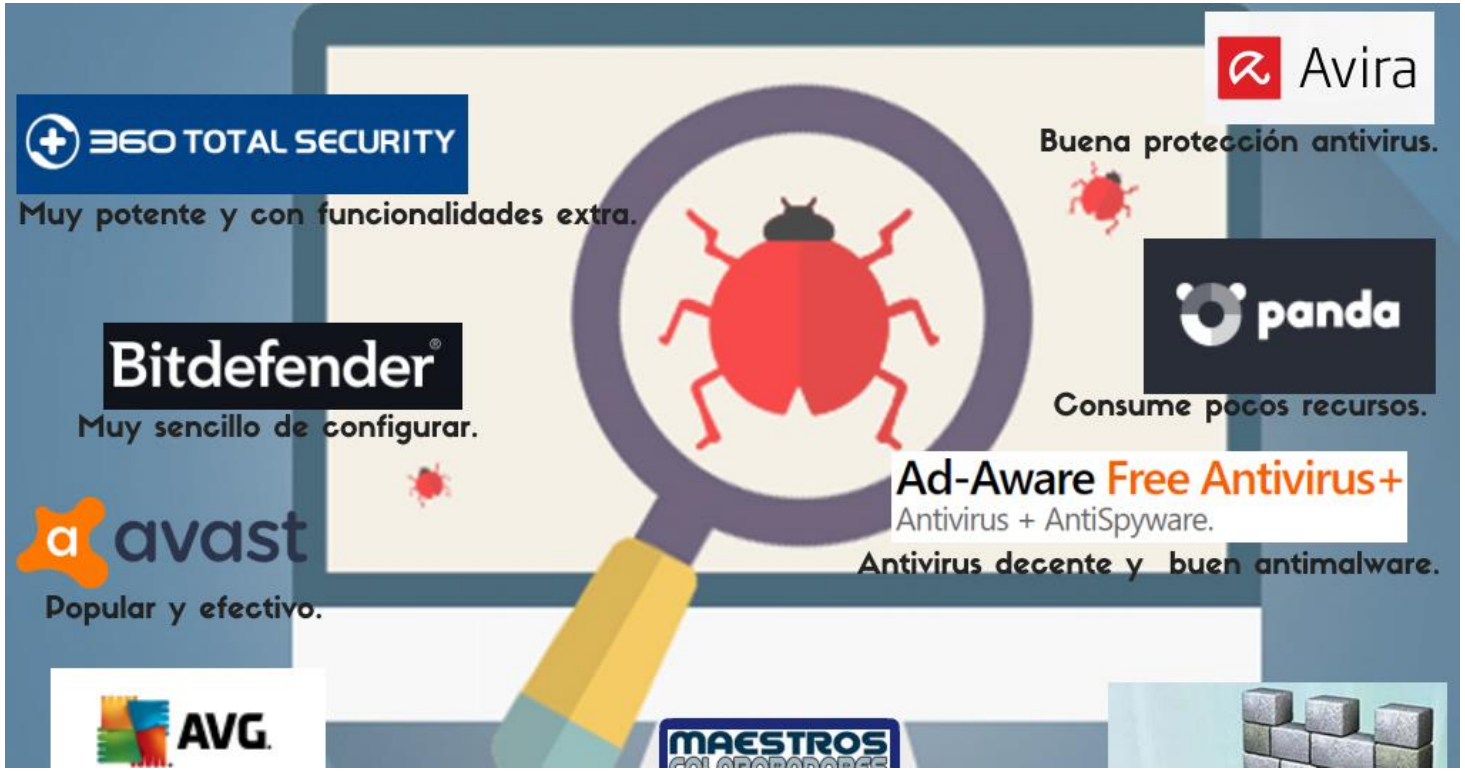
1. Install the following browser extensions:
    1. Privacy Badger
    2. uBlock Origin
    3. Trend Micro Check
    4. Emsisoft Browser Security
2. Steps to Install:
    1. Go to extensions menu
    2. Search names in extension store
    3. Only install ones with verified badge

Securing Web Browsers

Needless to say:

This must be done for all computers in the house/office.

Securing Personal Computers

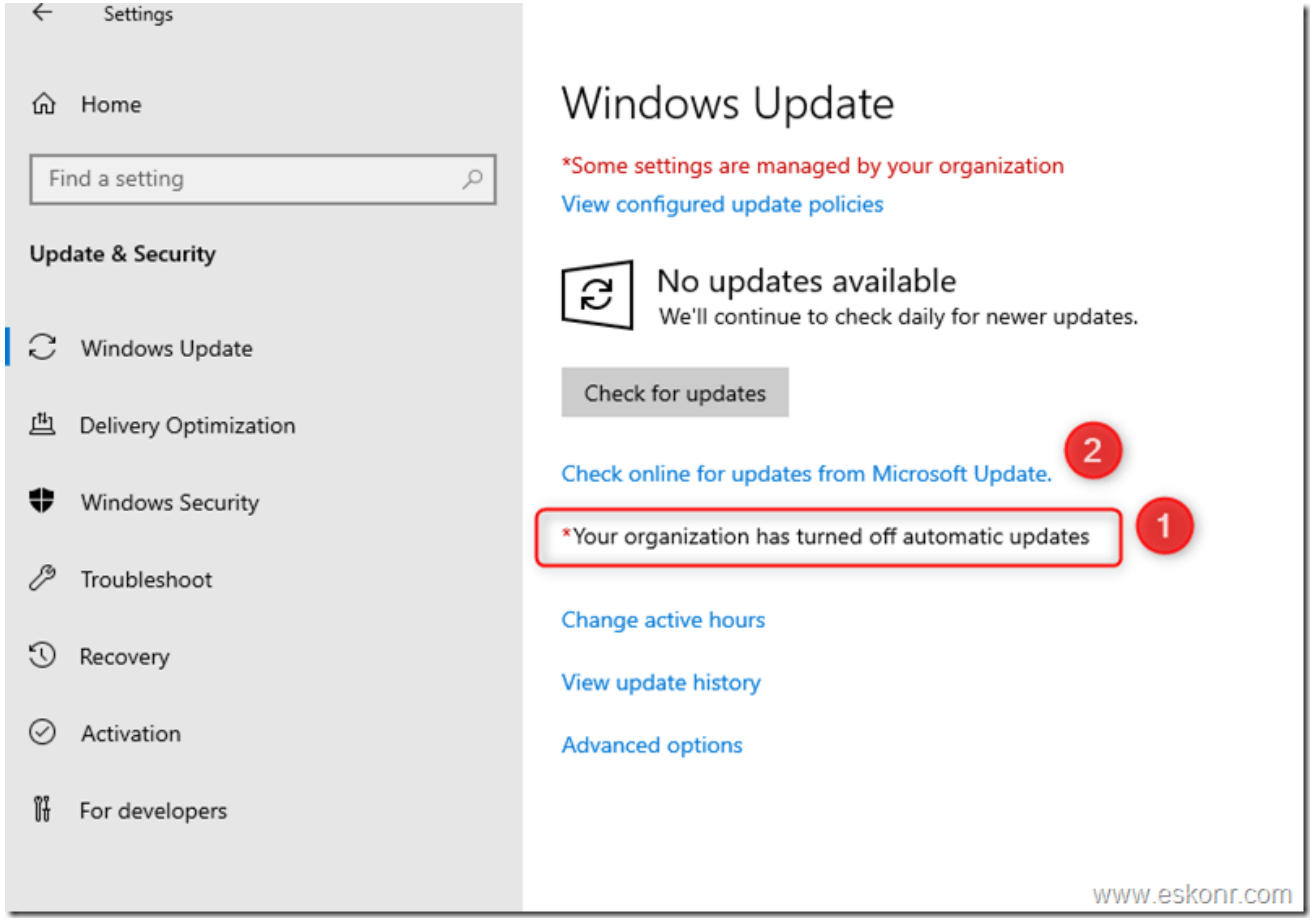


Get one of the following paid antivirus for each device, **not cloud**:
Norton, Bitdefender, Sophos.

Enable the following settings in whichever antivirus you choose:

1. Regular Vulnerability Scanning
2. Firewall Capabilities
3. AntiSpam
4. Data Protection/Ransomware Remediation
5. Cryptomining Protections
6. Anti-Theft and Backups
7. Safepay
8. Video/Audio Protections
9. Parental Controls

Securing Personal Computers

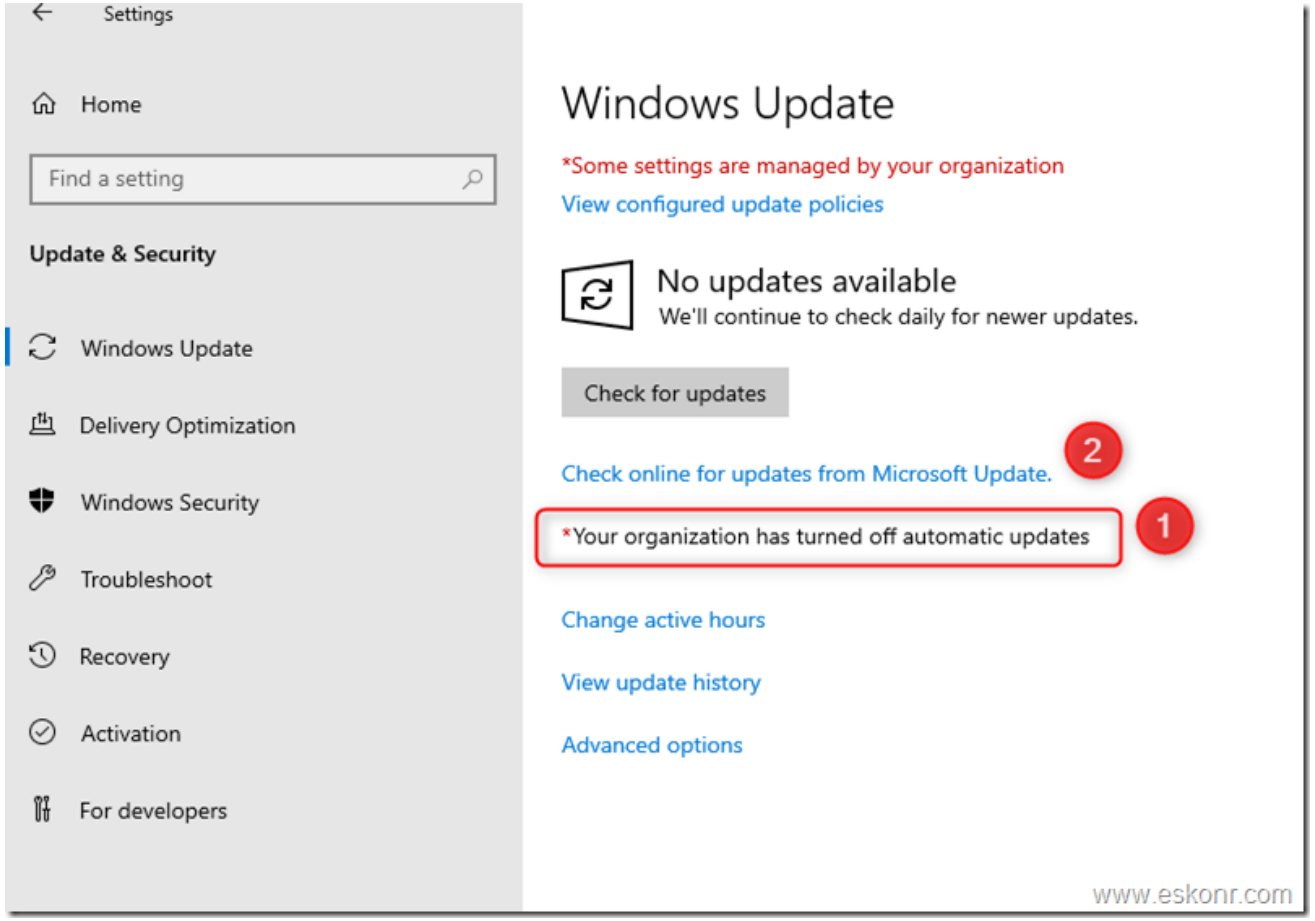


Microsoft once estimated a majority of hacked customers were hacked via **vulnerabilities patched years ago.**

We can prevent this by finding updates in the “Settings”/”Control Panel” menus and enabling automatic updates. It is similar for each operating system.

It must be checked at least once a week; ideal would be to set up multiple reminders on your phone over the weekend.

Securing Personal Computers



Once set up all you have to do is verbally ensure that every person has checked their own devices for auto-updating.

Auto-Updates for MacOS:

Navigate to System Settings > General > Software Update and turn on the desired update options

For Linux machines:

1. You can either set up a cron task for apt-get upgrade
2. OR install tools like unattended upgrades

Router and Modem Security

Since router firmwares are more technical than personal computer OS tasks; we'd recommend consulting your Internet Service Provider for the following :

1. Built-In Antivirus
2. Built-In VPN
3. Guest Networks
4. High Reputation Third-Party Firewall

They may have to figure out a bit themselves, since most SOHO networks don't bother with security, but don't worry! Every good ISP has skilled engineers.

Account Access Security

By getting services like the following (or free versions), you can strengthen your accounts multifold against being hacked:

1. Data Privacy Services like DeleteMe
2. Credential Monitoring Services like Flashpoint
3. Randomized passwords with Password Managers like KeePass
4. MFA using Authenticator Apps like Microsoft Authenticator

Smartphone Security

Privacy

Vulnerabilities

Physical Security

Privacy

- **Privacy** is about **controlling who can access your personal information**
- **Security** is about **protecting yourself and your assets**
- **Most attacks start with reconnaissance:** Attackers gather info to find weaknesses
- **Strong privacy reduces what attackers can learn:** Makes attacks harder to plan or execute.

Vulnerabilities

Vulnerabilities are weaknesses in systems or software: basically, flaws in code that attackers can misuse.

In Operating Systems:

- Often found in critical components like network services
- *Example:* The **EternalBlue** exploit in Windows allowed attackers to run any code they wanted

In Applications:

- Common issues include insecure APIs, weak authentication, and poor input validation
- These flaws can lead to **unauthorized access**, **data breaches**, and other security problems

Physical Security

Physical security means protecting your devices from being physically accessed by others.

- If someone **physically accesses your device**, digital defenses can be bypassed
- Risks include unauthorized access, theft, tampering, and direct malware installation
- Stolen devices can expose sensitive data, leading to identity theft or financial loss
- Strong physical security helps prevent these risks and improves overall cybersecurity

Physical Security

SIM PIN:

- Protects your SIM from SIM swapping and unauthorized use.
- Set a unique PIN and remember it!

Rooting (Android):

- Gaining full control by bypassing OS restrictions.
- Not recommended—can cause device issues and open security risks

Jailbreaking (iOS):

- Removing Apple's restrictions to customize or install unauthorized apps.
- Also not recommended due to potential instability and security vulnerabilities

Physical Security

Anti-Theft:

- Use high-quality locks and straps to secure your device to your pocket or hand.
- Makes stealing very difficult and often causes thieves to give up.

Power Banks:

- Avoid using free public charging stations, which can carry malware ("Juice Jacking").
- Carry your own power bank and cables to stay safe.

USB Data Blockers:

- Use USB data blockers to charge your device without data transfer.
- Acts as a safeguard when you can't use your own power bank.

iPhone SECURITY GUIDE

Privacy Concerns with iPhone

- 2024: Apple's lawyers told a judge, "Given Apple's extensive privacy disclosures, **no reasonable user would expect that their actions in Apple's apps would be private from Apple**."

- 2022 to 2023: Apple's hardware sales fell by over $18 billion. Meanwhile, revenue from services, such as targeted advertising, has grown steadily. To deliver targeted ads, Apple shares information about **your device, location, App Store searches, viewing history, browsing history etc to third party advertisers.**

- 2021: Security researchers reported an Apple bug that allowed attackers to identify senders via AirDrop, which many "trigger-happy" governments publicly said they used to identify people sharing "inappropriate information". Even when **the patch for this bug was publicly released (same researchers), Apple did not patch the vulnerability.**

Malware Statistics

- New malware for iOS **grew more than 70% in 2020**
- 2% of the top 1000 highest-grossing apps on the app store are scam apps. Guardsquare claims these **scam apps have earned over $48 million in revenue.**
- iOS apps do not keep their word regarding privacy and tracking software. For example, Subway Surfers was found sending 29 pieces of information about the iOS device to a third party advertising company, **even for users who selected "Do not track"**
- Sophisticated banking trojans, such as GoldPickAxe.iOS are on the rise. This particular malware steals biometric data, intercepts (reads and/or modifies) text messages **in order to gain access to victims' financial applications/data.**

Security steps

iPhone Stock Settings

- **Password:** Use a **very** strong password to login; **disable** biometrics and lock patterns. The reason for this is that biometrics and lock patterns are not only very easy to bypass, but Apple may be forced to share it private companies under situations; from which it can easily leak (via attacks on said company) to cybercrime markets.
- **Lock Screen:** Disable voice assistance (Siri) and notifications over the lock screen; this disables multiple vulnerabilities used for bypassing your screen lock.
- **Communication:** Do not use iMessages; use a more secure application such as WhatsApp or Signal for communications in which you will be sending media.

Other Steps

- **Browsers**: **Only** use Stock Safari, Brave or DuckDuckGo; and avoid others like Chrome.

- **Search Engines:** Set your default search engine as DuckDuckGo to avoid Phishing Links utilizing SEO on Google Search**.**

- **Virtual Private Networks:** Utilizing VPNs as a default not only encrypts your data but also has built in firewall and domain name security features**.**

- **SIM Pin:** By contacting your mobile company, you can set up a required pin code to access your SIM card. This prevents SIM swapping.

Other Steps

Utilize Third Party Antivirus: While iOS is not one of the most exploited platforms present today; exploits against iOS are increasing in both number and intensity, so we recommend you subscribe to any two of the three different third party antivirus solutions below

According to CyberNews, subscribe to the following iOS Antivirus Solutions for best security against all possible problems**:**

1. **TotalAV**
2. **Norton 360**
3. **Avira Antivirus**

ANDROID SECURITY GUIDE

Googles' History with Privacy

- 2007: Privacy International votes Google as "Hostile to Privacy", the lowest rating possible, and the only company to get that rating that year
- 2010: Google is found tracking and selling data even from consumers who "opted out" of data tracking, a legal requirement Google had to obey.
- 2012: The European Union fines Google for providing restricted and personal data to the National Security Agency of the United States under the PRISM program
- 2024: The Information Commissioners' Office (United Kingdom) expresses concerns after Google cancels plan to remove trackers ("malware" that sticks to your browser, relaying every data about your browsing, 24/7/365) present across the Internet.

Android Malware Statistics

- Threat intelligence researchers estimate that as of March 2025, there are almost 36 million instances of malware on Android devices – Norton
- Android is the main target for attackers focused on mobile malware, attracting between 95& and 98% of mobile malware – SpaceLift
- Zimperium Labs discovered earlier this year that 95 percent of Android devices could be hacked with a simple text message – Kaspersky
- Researchers from the University of Cambridge found that 87 percent of all Android smartphones are exposed to at least one critical vulnerability – Kaspersky

Security steps

Lock Screen

- Use a **very** strong password to login; disable biometrics and lock patterns. The reason for this is that biometrics and lock patterns are not only very easy to bypass, but Google and Device Manufacturer (eg. Samsung) may be forced to share it with private companies under situations; from which it can easily leak to cybercrime markets (via attacks on company).
- Disable voice assistance and notifications over the lock screen; this disables multiple vulnerabilities used for bypassing your screen lock.
- Screen Pinning: If for example handing your phone to another person, utilize screen pinning to ensure the person cannot use anything other than a specific application.

Private Applications

- Browsers: **Only** use DuckDuckGo, Firefox Focus or Bromite browser for personal browsing; and **avoid others** like Chrome.

- **Rely on FOSS Apps:**
  - FOSS (Free and Open-Source Software) is software with publicly available source code, allowing global collaboration and transparency.
  - Changes are reviewed by a global community, making FOSS quick to fix vulnerabilities and resistant to hidden trackers.
  - This makes it more secure and trustworthy than proprietary software.
  - You can get this by installing F-Droid on your mobile, and disabling Play Store

Private Applications

- **Special Focus:** Disable Google Search, Google Photos Upload, and almost every other synchronizing Stock application.
- **Virtual Private Networks:** Utilizing VPNs encrypts our web traffic and provides firewall functions
- **Utilize Third Party Antivirus:** Android is one of the most exploited platforms present today; so we recommend you subscribe to not one but three different third-party antivirus solutions.

1. **Bitdefender**
2. **Trend Micro**
3. **Avast One Gold**

Bonus SECURITY TIPS

Bonus Security Tips

Phishing Awareness

Regular Router Settings Monitoring

Annual Penetration Test

Secure Access to IT Rooms

Use Cloudflare Free Security for Websites