



Congratulations on the purchase of your Mark37 Laptop. You have taken a great step in taking back control of your data and privacy.

Your new laptop utilizes FOSS: Free and open-source software (FOSS) is a term used to refer to groups of software consisting of both free software and open-source software[a] where anyone is freely licensed to use, copy, study, and change the software in any way, and the source code is openly shared so that people are encouraged to voluntarily improve the design of the software

Taking your first steps into the FOSS world can leave you feeling overwhelmed and uncertain, but we are here to help you make this move as easy as possible.

With Big Tech you have no control. With Linux and FOSS you are in full control.

Your Ghost Laptop comes installed with Zorin OS. If you are a new user of Zorin OS, an Ubuntu-based Linux distribution designed to be user-friendly, here are some getting started tips to help you understand how to use it:

- Familiarize Yourself with the Desktop Environment: Zorin OS uses the GNOME desktop environment, which has a taskbar at the top of the screen and an activities overview in the top-left corner. Spend some time exploring the desktop environment and understanding its basic elements.
- Understand the App Menu: To access installed applications, click on the "Z" logo or the "Activities" button in the top-left corner. This will open the app menu, where you can search for and launch applications. You can also browse through categories to find specific programs.
- Customize Your Desktop: Zorin OS offers various customization options to personalize your desktop. Right-click on the desktop and select "Customize" to access settings like wallpaper, icons, themes, and fonts. Experiment with different options to make your desktop feel comfortable for you.
- Use the Software Center: Zorin OS includes a Software Center, similar to an app store, where you can easily install and manage applications. Open the Software Center from the app menu, browse different categories, and install the software you need with just a few clicks.
- Update Your System: Keeping your system up to date is important for security and stability. Zorin OS provides regular updates, and you should

install them when prompted. To manually update your system, open the app menu, search for "Software Updater," and follow the instructions.

- Explore the File Manager: Zorin OS uses the Nautilus file manager, which allows you to navigate and manage your files and folders. It has a sidebar on the left with quick access to important locations like Home, Documents, and Downloads. Spend some time familiarizing yourself with its features and options.
- Learn Terminal Basics: While Zorin OS provides a graphical user interface, learning some basic commands in the terminal can be helpful. The terminal allows you to execute commands and perform advanced system tasks. Open the terminal by searching for "Terminal" in the app menu and try out basic commands like navigating directories, creating folders, or updating the system.
- Join the Community: Zorin OS has an active community of users and developers who can provide support and guidance. Visit the Zorin OS website and explore forums, documentation, and tutorials. Engage with the community to ask questions, share experiences, and learn more about the operating system.

Remember, learning a new operating system takes time and practice. Be patient with yourself and don't hesitate to explore and experiment. Zorin OS is designed to be user-friendly, making it easier for newcomers to adapt to the Linux environment.

The two QR codes below link to videos that will help you in familiarizing yourself with Zorin OS installed on your Mark37 Ghost Laptop.



<https://youtu.be/mSEIOyAME4E>  
<https://youtu.be/VJJSez0HAbA>

Your Ghost Laptop is fully set up and ready to use so you can begin familiarizing yourself with Zorin OS right away and telling your friends and family you use

Linux.

## **IMPORTANT!! Change the Password**

The password to log into your device is **1234**. You need to change this password to a strong secret password of your own. We strongly encourage you to do this for your own privacy and security.

To set your own password click the “start” menu in in the lower left and select settings on the right side of the menu. Once in the settings menu on the left window pane scroll down and find **Users**. Click on users and at the top you will see a pink bar asking you to “Unlock to Change Settings”. Click unlock and enter the current password (1234) and then you may set your own super-secret password. Just be sure to record your password in a safe and private location. If you forget it and lose it you will be permanently locked out and will lose your data on your laptop.

You may also change your username here and add a profile picture by click the pencil icon.

## **Connect to a Wi-fi Network**

Back in the settings menu, on the left side of the window pane scroll to the top and at the very top will be Wi-Fi. Click on Wi-Fi and on the top left verify that the toggle is turned on. It should automatically find your Wi-Fi network and display it in a list of visible networks. Select your network and it will ask you to enter your Wi-Fi network password. You should then be connected to your Wi-Fi network.

## **TimeShift**

TimeShift is FOSS software for backing up Linux machines. It is installed on your Ghost Laptop and we highly recommend you learning to use it and making a habit of keeping your machine backed up. We recommend backing up to a external hard drive for these backups in case of a drive failure on your Ghost laptop. Below is a link to a decent video showing how to use TimeShift.



<https://youtu.be/U-IMJHcjCVs>

## **Optional - The Command Line:**

Although this section is optional and not required to learn to use your Mark37 Ghost Laptop, by not learning the command line you will not be taking full advantage of the power of Linux. We encourage you to learn some Linux terminal commands. You do not need to be a power user to take advantage of the

command line. Learning enough to install some software, navigate your file structure and checking your system status will give much more control of your machine.

Something every Linux user should know how to do through the command line is to update their system. To do this, first open a terminal window by pressing **ctrl + alt + t** and then type the following command: **sudo apt update && sudo apt upgraded** You will most likely be prompted to answer a yes or no question presented like **Y/n**. You may respond by typing **y** for yes and **n** for no and pressing the enter key. If you are unsure what to respond with, you are safe to respond by just pressing the enter key which will tell the system to use the default option.

Doing the above is not a requirement as Zorin OS will take care of system updates through the Graphical Software Updater. But, it is a good to get you familiar with the command line and not see it as a scary place. Learning and getting familiar with the command line will enable you to have full control of your computer and allow you to learn many of the same “secrets” and tools that Big Tech does not like for you to know as it gives them power over you.

We recommend you make use of our forums for asking questions about using your new Ghost Laptop and the software options available for your daily use and productivity.

Mark37 Forums:

<https://forums.mark37.com>

We also suggest the Jeff.pro website and his forums for helping you along on your Linux journey and your break away from big tech.

Jeff Pro website:

<https://forums.jeff.pro>

If you do not find an answer to your question or the issue you may have in the resources we recommend, reach out to us through live chat on our website **MARK37.com** or email us at [support@mark37.com](mailto:support@mark37.com).

We wish you the best in your journey of reclaiming your personal and digital sovereignty!

## **FAQ**

### ***Is Zorin OS a secure operating system?***

Zorin OS, like any modern Linux distribution, puts a strong emphasis on security.

While no operating system can claim to be completely immune to vulnerabilities or attacks, Zorin OS incorporates several security features to help protect your system and data. Here are some aspects that contribute to the security of Zorin OS:

- **Linux Security Model:** Zorin OS is built on top of the Linux kernel, which benefits from the robust security mechanisms inherent in Linux. This includes access controls, process isolation, and user privilege management.
- **Regular Updates:** Zorin OS provides regular software updates to address security vulnerabilities, bug fixes, and performance improvements. It's crucial to keep your system up to date to benefit from the latest security patches.
- **Secure Software Sources:** Zorin OS utilizes software repositories that are carefully curated and monitored by the Zorin OS team. This helps ensure that the software you install comes from trusted sources, reducing the risk of malware or compromised packages.
- **AppArmor and Firejail:** Zorin OS incorporates security frameworks like AppArmor and Firejail. AppArmor allows for the confinement of applications, restricting their access to system resources and protecting against potentially malicious actions. Firejail provides additional sandboxing capabilities to isolate applications and limit their access to sensitive areas of the system.
- **User Account Control:** Zorin OS implements user account control, which prompts for administrative privileges when performing system-level changes. This helps prevent unauthorized modifications to critical system files or settings.
- **Firewall and Network Security:** Zorin OS includes a built-in firewall (iptables) that can be configured to control incoming and outgoing network traffic. Additionally, Zorin OS benefits from the security features provided by the Linux kernel, such as secure networking protocols and strong encryption.
- **Privacy Settings:** Zorin OS offers privacy settings that allow you to control the data collection and telemetry aspects of the operating system. You can customize privacy settings during the initial setup or modify them later through the system settings.

It's important to note that while Zorin OS incorporates these security features, maintaining a secure system also relies on responsible user behavior. Practicing good security habits, such as using strong passwords, regularly updating software, avoiding untrusted software sources, and being cautious while browsing the internet, further enhances the security of your Zorin OS installation.

### ***What settings can I configure in Zorin OS to make it more secure than the default security?***

Zorin OS provides several settings that you can configure to enhance the security of your system beyond the default settings. Here are some key areas where you can make adjustments:

- **Firewall Configuration:** Zorin OS includes a built-in firewall called iptables. To configure the firewall, you can use a graphical front-end tool like gufw. Open the Software Center, search for "gufw," and install it. Once installed, launch gufw and enable the firewall if it's not already active. You can then customize incoming and outgoing rules to control network traffic.
- **User Account Management:** Zorin OS uses user accounts to manage access to the system. By default, Zorin OS prompts for administrative privileges when performing system-level changes. You can further enhance security by creating a separate, non-administrative user account for regular daily use. This helps minimize the impact of any potential security breaches.
- **Password and Authentication Policies:** You can strengthen password security by enforcing stronger password policies. Open the "Settings" app, go to "Details" > "Users," and click on the gear icon next to your user account. From there, you can set a password policy that requires stronger passwords or enforces password expiration. Additionally, consider enabling two-factor authentication (2FA) for your user account and any online services you use.
- **Privacy Settings:** Zorin OS provides privacy settings that allow you to control data collection and telemetry. Open the "Settings" app, go to "Privacy," and review the various options available. You can disable or customize data collection settings for usage statistics, error reporting, and location services according to your preferences.
- **Software Updates:** Keeping your system up to date is crucial for security. By

default, Zorin OS prompts you to install updates. However, you can configure automatic updates for increased convenience and security. Open the "Software & Updates" app, go to the "Updates" tab, and select your preferred update settings.

- **Encrypted Home Folder:** Zorin OS offers the option to encrypt your home folder, which provides an additional layer of security for your personal files and data. During the installation process or afterward, you can enable home folder encryption. This ensures that your files are encrypted and protected from unauthorized access in case your system is compromised.
- **AppArmor Profiles:** Zorin OS uses AppArmor to confine applications and limit their access to system resources. You can further enhance security by enabling additional AppArmor profiles for applications that do not have them enabled by default. You can install the `apparmor-profiles` package from the Software Center, which provides a collection of additional AppArmor profiles.
- These are just a few examples of the settings you can configure to enhance the security of your Zorin OS system. It's important to strike a balance between security and usability and tailor the settings to your specific needs and requirements. Regularly reviewing and updating your security settings is recommended to stay protected.

### ***How can I learn more about using Zorin OS to enhance personal privacy when connected to the internet?***

To learn more about enhancing personal privacy in Zorin OS while connected to the internet, you can explore various resources and follow best practices. Here are some steps you can take:

- **Online Documentation:** Zorin OS provides official documentation that covers a wide range of topics, including privacy and security. Visit the Zorin OS website and look for documentation or user guides that specifically address privacy-related features and settings. This documentation will provide detailed instructions and explanations.
- **Privacy-Centric Websites and Blogs:** Many websites and blogs focus on privacy and provide valuable information and guides related to Zorin OS and other Linux distributions. Explore websites such as [PrivacyTools](#)

([privacytools.io](https://www.privacytools.io)) or blogs like It's FOSS ([itsfoss.com](https://itsfoss.com)) for articles and tutorials specifically tailored to privacy in Linux. These resources often cover topics such as secure browsing, encrypted communication, and privacy-focused applications.

- **Privacy-Focused Software:** Zorin OS offers a variety of applications that can enhance privacy when connected to the internet. For example, consider using privacy-focused web browsers like Firefox or Brave, which offer enhanced privacy features and support add-ons for additional privacy measures. Explore and install privacy-oriented applications available in the Zorin OS Software Center.
- **Encryption and VPNs:** Zorin OS includes built-in support for disk encryption, which allows you to encrypt your entire system or specific partitions. This protects your data in case your device is lost or stolen. Additionally, consider using a virtual private network (VPN) when connecting to the internet, which adds an extra layer of privacy by encrypting your internet traffic. There are several VPN providers available that offer Linux-compatible clients.
- **Privacy Extensions and Add-ons:** Web browser extensions can enhance your privacy while browsing the internet. Popular extensions like uBlock Origin, HTTPS Everywhere, and Privacy Badger can help block ads, enforce secure connections, and protect against online tracking. Install these extensions from your browser's extension store.
- **Privacy-Oriented Search Engines:** Consider using privacy-focused search engines like DuckDuckGo or Startpage instead of mainstream search engines. These search engines prioritize user privacy by not tracking or storing personal information.
- **Privacy Settings:** Zorin OS provides privacy settings that allow you to control data collection and telemetry. Review and adjust these settings to align with your privacy preferences. Open the "Settings" app, go to "Privacy," and explore the available options.

Remember that privacy is a multifaceted topic, and it's important to approach it holistically. Continuously educate yourself on emerging privacy concerns and regularly review and update your privacy measures as needed. By combining privacy-conscious software choices, secure browsing habits, and appropriate privacy settings, you can enhance your personal privacy while using Zorin OS and being connected to the internet.



In Summary:

### ***Is Zorin OS a secure operating system?***

- Yes, Zorin OS is designed with security in mind.
- It incorporates security features like access controls and process isolation.
- Regular updates are provided to address security vulnerabilities.
- It includes security frameworks like AppArmor and Firejail for application confinement.
- Good security practices and responsible user behavior are still important.

### **What settings can I configure in Zorin OS to make it more secure than the default security?**

- Enable and configure the built-in firewall using a graphical tool called gufw.
- Set stronger password policies and consider enabling two-factor authentication (2FA).
- Review and customize privacy settings to control data collection and telemetry.
- Keep your system up to date with regular software updates.
- Consider encrypting your home folder for added security.
- Explore additional AppArmor profiles for applications without them.

### **How can I learn more about using Zorin OS to enhance personal privacy when connected to the internet?**

- Explore Zorin OS's official documentation for privacy-related features and settings.
- Visit privacy-focused websites and blogs that offer guides and tutorials for Zorin OS.
- Use privacy-focused software like secure web browsers and VPNs.
- Install browser extensions for ad-blocking and privacy protection.
- Consider using privacy-oriented search engines.
- Review and adjust privacy settings in the Zorin OS "Privacy" section of the settings.

\*Remember, it's important to strike a balance between security and usability, and continuously educate yourself on privacy best practices.

~ The MARK37 Team