L2Cyber
Security Solutions
#SecuritySimplified

https://www.L2CyberSecurity.com

USE STRONG, UNIQUE PASSWORDS FOR ALL OF YOUR ONLINE ACCOUNTS.

Pro Tip: Use a password manager to help you keep track of your passwords.

Create a password that is at least 12 characters long and includes a mix of upper and lowercase letters, numbers, and symbols. Avoid using personal information in your passwords, such as your name, birthday, or address.

L2Cyber Security Solutions

#SecuritySimplified

https://www.L2CyberSecurity.com

KEEP YOUR SOFTWARE UP TO DATE.

Pro Tip: If you have any devices that you no longer use, make sure to uninstall them or wipe them clean before disposing of them.

Enable automatic updates for your operating system, software applications, and web browser.

L2Cyber
Security Solutions
#SecuritySimplified

https://www.L2CyberSecurity.com

BE CAREFUL ABOUT WHAT ATTACHMENTS YOU OPEN AND WHAT LINKS YOU CLICK ON.

Pro Tip: Use a spam filter to help block phishing emails from reaching your inbox.

Never open an email from someone you don't know or trust. If you're unsure about an email, don't click on any links or attachments.

L2Cyber Security Solutions

#SecuritySimplified

https://www.L2CyberSecurity.com

USE A FIREWALL AND ANTIVIRUS SOFTWARE.

Pro Tip: Schedule and run regular virus scans on your devices.

Make sure that your firewall and antivirus software are enabled and up to date.

L2Cyber Security Solutions

#SecuritySimplified

https://www.L2CyberSecurity.com

BACK UP YOUR DATA REGULARLY.

Pro Tip: Test your backups regularly to make sure that they are working properly.

Back up your data to a cloud storage service and/or an external hard drive.

L2Cyber
Security Solutions
#SecuritySimplified

https://www.L2CyberSecurity.com

SECURE YOUR WI-FI NETWORK.

Pro Tip: If your business offers guest Wi-Fi, set up a separate network for guests and isolate it from your main network.

Use a strong password for your Wi-Fi network and enable encryption.

L2Cyber
Security Solutions
#SecuritySimplified

https://www.L2CyberSecurity.com

EDUCATE YOUR EMPLOYEES ABOUT CYBERSECURITY.

Pro Tip: Consider conducting regular security awareness training for your employees.

Train your employees on how to identify phishing emails, avoid malware, create strong passwords and use multi-factor authentication You should also have a policy in place for reporting suspicious activity.

L2Cyber Security Solutions

#SecuritySimplified

https://www.L2CyberSecurity.com

IMPLEMENT MULTI-FACTOR AUTHENTICATION (MFA).

Pro Tip: Use a variety of MFA methods, such as SMS codes, authenticator apps, and hardware tokens.

Enable MFA for all of your business accounts, including email, social media, and cloud storage.

L2Cyber
Security Solutions
#SecuritySimplified

https://www.L2CyberSecurity.com

HAVE A CYBER SECURITY INCIDENT RESPONSE PLAN IN PLACE.

Pro Tip: Test your incident response plan regularly to make sure that it is effective.

Your plan should include steps for identifying, containing, and eradicating threats, as well as communicating with customers and employees.

L2Cyber Security Solutions

#SecuritySimplified

https://www.L2CyberSecurity.com

BE CAREFUL ABOUT WHAT APPS YOU INSTALL ON YOUR DEVICES.

Pro Tip: Check the app's permissions and look at its reputation before you install it. If there are a lot of 1 star and 5 star reviews, it's probably dodgy.

Only install apps from trusted sources, such as the official app store for your device.