



# TECHLORE

Insider Tips to Make Your Business Run Faster, Easier and More Profitable

## INSIDE THIS ISSUE:

Why Securing Your Software Supply Chain is Critical	Page 1	Common Mobile Malware Traps	Page 2
Gadget of The Month	Page 1	Tech Tip of The Month	Page 2
Maximize Your Microsoft 365	Page 2	Tackling "Technical Debt" at Your Company	Page 2
Mobile-Optimized Workspace	Page 2	Cyber Security Survey	Page 2



"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"  
 -Ruben Diaz  
 NeoLore Networks

## Why Securing Your Software Supply Chain is Critical

In today's world, everything's connected. That includes the software your business relies on, whether you've installed that software locally or use it in the cloud. Protecting the entire process that creates and delivers your software is very important. From the tools developers use to the way updates reach your computer, every step matters. A breach or vulnerability in any part of this chain can have severe consequences.

A recent example is the global IT outage that happened last July. This outage brought down airlines, banks, and many other businesses. The culprit for the outage was an update gone wrong. This update came from a software supplier called CrowdStrike. It turns out that the company was a link in a LOT of software supply chains.

What can you do to avoid a similar supply chain-related issue? Let's talk about why securing your software supply chain is absolutely essential.

### Increasing Complexity and Interdependence

- **Many Components.** These include open-source libraries, third-party APIs, and cloud services.
- **Interconnected Systems.** A vulnerability in one part of the

supply chain can affect many systems. The interdependence means that a single weak link can cause widespread issues.

• **Continuous Integration and Deployment.** Securing the CI/CD pipeline is crucial to prevent the introduction of malicious code.

### Rise of Cyber Threats

- **Targeted Attacks.** Attackers infiltrate trusted software to gain access to wider networks.
- **Sophisticated Techniques.** These include advanced malware, zero-day exploits, and social engineering. A robust security posture is necessary to defend against these threats.

• **Financial and Reputational Damage.** Companies may face regulatory fines, legal costs, and loss of customer trust. Recovering from a breach can be a lengthy and expensive process.

### Regulatory Requirements

- **Compliance Standards.** These include regulations like GDPR, HIPAA, and the Cybersecurity Maturity Model Certification (CMMC).
- **Vendor Risk Management.** Companies must ensure that their suppliers adhere to security best practices.
- **Data Protection.** Securing the supply chain helps protect sensitive data from unauthorized access.

### Ensuring Business Continuity

- **Preventing Disruptions.** A secure supply chain helps prevent disruptions in business operations as cyber-attacks can lead to downtime.
- **Maintaining Trust.** By securing the supply chain, companies can maintain the trust of their stakeholders.

### Steps to Secure Your Software Supply Chain

- **Strong Authentication.** Use strong authentication methods for all components of the supply chain.
- **Phased Update Rollouts.** Keep all software components up to date, but don't do all systems at once.

- **Security Audits.** Assess the security measures of all vendors and partners.
- **Secure Development Practices.** Ensure that security is integrated into the development lifecycle from the start.
- **Threat Monitoring.** Use tools like intrusion detection systems (IDS) as well as security information and event management (SIEM) systems.
- **Education.** Awareness and training help ensure that everyone understands their role in maintaining security.

A breach or outage can have severe consequences. Securing your software supply chain is no longer optional; investing in this is crucial for the resilience of any business.



## CLVX 1 Keyboard by Clevetura

The CLVX 1 is a Gesture Keyboard with a Touchpad inside, currently offered via Indiegogo. The Type and Touch Modes switch automatically, indicated at the spacebar. It offers a full-sized ANSI layout with a numeric

keypad, navigation cluster, and a fully customizable Fn row. When typing, the touchpad is blocked. When making gestures, it works as a touchpad. Get one at <https://clevetura.com/>

# Essential Settings to Maximize your Microsoft 365 Experience

Microsoft 365 is a powerful suite of tools. But to get the most out of it, it's important to optimize the settings. Otherwise, you may only be using a fraction of the power you have. Here are some tips to get more from your M365 business subscription.

## 1. Optimize Email with Outlook Features

**Set Up a Focused Inbox.** This helps you manage your email more efficiently. It separates important emails from the rest.

**Organize with Rules.** Create rules to move emails to specific folders or mark them as read to reduce clutter.

## 2. Enhance Collaboration with Teams

**Set Up Channels.** Channels in Teams organize discussions by

topic or project. Create channels for different teams or events.

**Manage Notifications.** Notifications keep you informed but can be overwhelming. Customize them by going to Settings > Notifications.

**Use Tabs for Quick Access.** Tabs in Teams give fast access to important files and apps. Add tabs for frequently used documents, websites, or apps.

**3. Secure Your Data Set Up Data Loss Prevention (DLP) Policies.** DLP policies help prevent data breaches. Create policies to identify and protect sensitive information.

**Manage Mobile Device Security.** Ensure mobile devices accessing Microsoft 365 are secure with Microsoft Business Premium and use Intune.

## 4. Customize SharePoint

**Organize with Document Libraries.** Document libraries in SharePoint help organize and manage files. Create libraries for different departments or projects.

**Use Site Templates.** Use templates for common site types, like team sites or project sites.

## 5. Maximize Productivity with OneDrive

**Sync Files for Offline Access.** OneDrive allows you to sync files for offline access. This ensures you can access important files without needing an internet connection.

**Use Version History.** Version history in OneDrive allows you to restore previous versions of files.

## 6. Leverage Advanced Features

**Use Power Automate for Workflow Automation.** Power Automate helps automate repetitive tasks. Go to the Power Automate website and create flows for common workflows.

**Analyze Data with Power BI.** Connect Power BI to your Microsoft 365 data sources to create interactive reports and dashboards.

**Add Copilot for Microsoft 365.** Copilot is Microsoft's generative AI engine. It can dramatically reduce the time it takes for all types of tasks.

Using these essential settings can maximize your Microsoft 365 experience. This can lead to improved security, efficiency, and collaboration.

# Enhancing Employee Performance with a Mobile-Optimized Workspace

## Core Components of a Mobile-Optimized Workspace

- **Cloud-Based Everything.** This ensures seamless access to files, applications, and collaboration tools from any device.
- **Mobile-First Applications.** Ensure they are intuitive, responsive, and offer the same functionality as desktop versions.
- **Robust Collaboration Tools.** Features like real-time editing, file sharing, and video conferencing are essential.
- **Secure Mobile Device Management.** Protect sensitive company data on mobile devices.
- **Employee Training.** Equip employees with skills to effectively use mobile devices for work.

## Benefits of a Mobile-Optimized Workspace

- **Increased Productivity**
- **Enhanced Collaboration**
- **Improved Decision Making**
- **Attracting Top Talent**
- **Cost Savings**

## Challenges and Considerations

- **Security Risks:** Increased device usage means a larger attack surface.
- **Employee Distractions:** Encourage employees to use focus modes or apps to reduce interruptions.
- **Data Usage:** Be mindful of data consumption. Consider providing mobile hotspots or Wi-Fi allowances.
- **Device Management:** Consider using mobile device management (MDM) solutions to streamline the process.

# 5 Tips to Troubleshoot Common Business Network Issues

1. **Inspect Physical Connections.** Quickly rule out or identify simple problems.
2. **Test Network Connectivity.** Simple testing can provide valuable insights.
3. **Analyze Network Configuration.** Errors here can often cause connectivity problems.
4. **Monitor Network Performance.** This helps identify ongoing issues and potential bottlenecks.
5. **Ensure Security and Updates.** Regular updates and checks can prevent many common issues.

# Common Mobile Malware Traps

Mobile malware can arrive in various forms, from sneaky apps to deceptive links. Ignorance is not bliss here. Understanding the common traps is your first line of defense.

- **Phishing Attacks.** Clicking links or downloading attachments can lead to malware infection.
- **Malicious Apps.** Always research apps before downloading.
- **SMS Scams.** Be wary of unexpected messages, especially those asking for sensitive info.
- **Public Wi-Fi networks.** Avoid accessing sensitive information on public Wi-Fi.
- **Fake Apps.** Always verify app authenticity
- **Adware.** Less harmful but can be annoying and can expose you to other threats.

# 8 Strategies for Tackling "Technical Debt" at your Company

- **Identify and Prioritize.** Focus on the most critical issues that will drive the most value first.
- **Integrate Debt Management into Your Workflow.** Maintain a balance between new development and debt reduction.
- **Educate and Train Your Team.** Foster a culture of quality thinking.
- **Improve Documentation.** It provides a reference for current and future team members.

- **Regularly Update and Refactor Systems.** This involves making small, manageable changes for quality.
- **Optimize Security Practices.** Helps maintain system reliability and performance.
- **Manage Dependencies.** Tracking ensures compatibility and security.
- **Foster a Culture of Continuous Improvement.** Encourage learning, celebrating successes, and regular reflection to drive ongoing enhancement.

# Take the NeoLore Cyber Security Survey

Has your company done a Cyber Security Maturity Assessment within the last year? Do you have an IT security policy in place? Do you know if you've been hacked or are leaking data?

If your answer was "no" or "I'm not sure" to any of those questions, your company may be at risk for a devastating cyberattack.

Get the NeoLore Networks Cyber Security eBook for Free!

## It Features

- Information on the various threats to your business
  - NIST Security Framework
  - CIS Controls
  - Basic Controls
- And More!

<https://neolore.com/cybersecurity>