



TALK NERDY TO ME

INSIDE THIS ISSUE:

AI for Efficiency	Page 1	Effective Small Business Backup and Recovery Plan	Page 2
Gadget of the Month	Page 1	Tech Tip of the Month	Page 2
Implementing Multi-Factor Authentication	Page 2	Remote Work Security Settings	Page 2
Decoding Cyber Insurance	Page 2	Client Testimonial	Page 2



We love technology and we love helping people. Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!
- Jason Horne
CEO

AI FOR EFFICIENCY: HOW TO AUTOMATE DAILY TASKS AND FREE UP YOUR TIME

Running a small business means wearing a lot of hats. These hats go from managing operations, handling customer inquiries to keeping everything running smoothly. There's a solution that can lighten the load, AI-powered automation. Thanks to technological advancements, these tools have become more accessible and cost-effective than ever, allowing small businessowners to automate tasks they previously had to handle manually.

Smart Ways to Automate Daily Tasks and Free Up Your Time

1. Automate Customer Support Without Losing the Personal Touch

- Use AI Chatbots for First-Line Support. AI-powered chatbots, like Tidio or Chatfuel, can handle frequently asked questions, schedule appointments, and collect customer information automatically.
- Smart Email Assistants. AI tools like Zendesk AI or Freshdesk can read incoming emails, categorize them, and even suggest replies. Some go a step further and can automate responses.
- AI-Enhanced Customer Feedback. AI tools like Survicate or Qualaroo can analyze customer feedback in real-time, spotting trends and highlighting areas for improvement automatically so you can act faster.

2. Streamline Scheduling and Calendar Management

- Let AI Handle Your Calendar. AI-powered tools like Calendly and Reclaim.ai can automatically suggest meeting times, taking into account everyone's availability, time zones, and preferences.
- AI-Powered Appointment Booking. If you offer services or consultations, tools like Acuity Scheduling let clients book appointments directly from your calendar.
- Optimized Time Allocation. AI tools like TimeHero or Trello use data and patterns from your calendar to suggest the most efficient way to allocate your time for various tasks.

3. Supercharge Your Marketing – Without Hiring an Agency

- Create Content with AI Writing Tools. AI writing tools like Jasper AI, Copy.ai, and ChatGPT can generate blog posts, social media content, and email campaigns quickly and efficiently.
- Automate Social Media Posts. Social media management platforms like Buffer or Later use AI to suggest the best times for posting, automatically queue content, and even generate hashtags.
- AI-Driven Analytics for Better Decision-Making. AI tools like Google Analytics and HubSpot can analyze the effectiveness of your marketing campaigns in real-time, providing insights into what's working.

4. Financial Tasks Made Easier

- Use AI Accounting Tools. Tools like QuickBooks Online and Xero automate tasks such as categorizing expenses, reconciling accounts, and generating reports.
- Automate Invoice Generation and Payment Reminders. Tools like Wave and Zoho Books let you generate invoices automatically and send payment reminders.
- Financial Forecasting with AI Insights. Tools like Fathom or Float forecast revenue, track expenses, and aid data-driven financial decisions.

5. Internal Team Collaboration & Workflow Automation

- Automate Repetitive Team Task. Tools like Zapier and Make.com

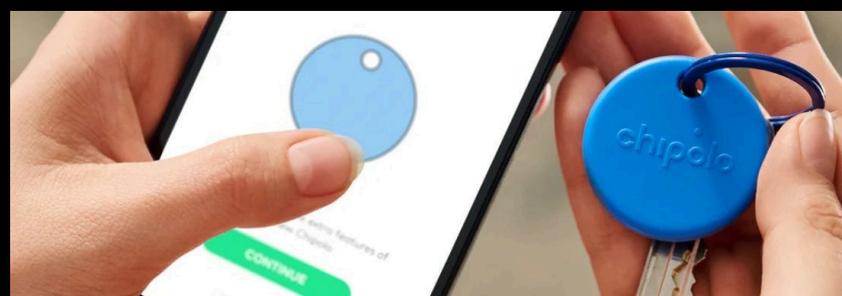
connect your apps and automate workflows.

- AI Note-Taking & Meeting Summaries. Tools like Otter.ai and Fireflies.ai transcribe meetings and generate notes automatically.
- Streamlined Project Management. Tools like Asana or Monday.com help you assign tasks, track deadlines, and monitor project progress.

Ready to integrate AI into your business?

If you're overwhelmed by daily tasks, consider AI-powered automation. You don't need a massive tech budget to start.

It's time to work smarter, not harder. Contact us for AI-powered solutions.



CHIPOLO POP

Never lose your essentials again with Chipolo POP!

With a loud ring, vibrant colors, replaceable battery, 200 ft range, and compatibility with iOS and Android, staying organized has never been easier.

This compact Bluetooth tracker helps you find your keys, wallet, or any item in seconds using the Chipolo app.

Chipolo POP also offers a community search feature, helping you locate lost items with the help of other users.

BEYOND THE PASSWORD: A SMALL BUSINESS GUIDE TO IMPLEMENTING MULTI-FACTOR AUTHENTICATION (MFA)

According to recent reports, nearly 43% of cyberattacks target small businesses, often exploiting weak security measures. One of the most overlooked yet highly effective ways to protect your company is through Multi-Factor Authentication (MFA). This extra layer of security makes it significantly harder for hackers to gain access, even if they have your password.

What is Multi-Factor Authentication?

Multi Factor Authentication (MFA) is a security process that requires users to provide two or more distinct factors when logging into an account or system. The factors are something you know (like a password or PIN), something you have (like a mobile phone or smart card), and something you are (like fingerprints or facial recognition).

How to Implement Multi-Factor Authentication in Your Business

Implementing Multi-Factor Authentication (MFA) is an important step toward enhancing your business's security. While it may seem like a complex process, it's actually more manageable than it appears, especially when broken down into clear steps. Below is a simple guide to help you get started with MFA implementation in your business:

- **Assess Your Current Security Infrastructure.** Conduct a thorough review of your existing security systems and identify which accounts, applications, and systems need MFA the most. Prioritize the most sensitive areas of your business.
- **Choose the Right MFA Solution.** Choosing the right one for your

business depends on your size, needs, and budget. Some popular options that can cater to small businesses include:

- Google Authenticator
- Duo Security
- Okta
- Authy

When selecting an MFA provider, consider factors like ease of use, cost-effectiveness, and scalability as your business grows.

Implement MFA Across All Critical Systems.

Once you've chosen an MFA provider, it's time to implement it across your business. Here are the steps to take:

- **Step 1: Set Up MFA for Your Core Applications:** Prioritize applications that store or access sensitive information, such as email platforms, file storage, and CRM systems.

- **Step 2. Enable MFA for Your Team:** Make MFA mandatory for all employees, ensuring it's used across all accounts.
- **Step 3. Provide Training and Support:** Offer clear instructions and training on how to set it up and use it.

Test Your MFA System Regularly

After implementation, it's essential to test your MFA system regularly to ensure it's functioning properly. Periodic testing allows you to spot any vulnerabilities, resolve potential issues, and ensure all employees are following best practices.

If you're ready to take your business's security to the next level, or if you need help implementing MFA, feel free to contact us. We're here to help you secure your business and protect what matters most.

DECODING CYBER INSURANCE: CHOOSING THE RIGHT POLICY

For small businesses navigating an increasingly digital world, cyber threats aren't just an abstract worry, they're a daily reality. Whether it's phishing scams, ransomware attacks, or accidental data leaks, the financial and reputational damage can be severe. That's why more companies are turning to cyber insurance to mitigate the risks.

How to Choose the Right Cyber Insurance Policy

Let's break down the steps to ensure you're selecting the best coverage for your organization.

Assess Your Business Risk

Start by evaluating your exposure:

- What types of data do you store? Customer, financial, and health data, all require different levels of protection.
- How reliant are you on digital tools or cloud platforms? You may need more extensive coverage.
- Do third-party vendors have access to your systems? Vendors can be a potential weak point.

Your answers will highlight the areas that need the most protection.

Ask the Right Questions

- Does this cover ransomware and social engineering fraud?
- Are legal fees and regulatory penalties included?
- What's excluded and when? Understand the fine print to avoid surprises if you file a claim.

Consider the Coverage Limits and Deductibles

Ensure that the coverage limit aligns with your business's potential risks. Choose a deductible that your business can afford in case of an incident.

Review Policy Renewal Terms and Adjustments

Cyber risk is constantly evolving. Check the terms for policy renewal and adjustments. It's important that your policy evolves with your business needs.

Assess your risks, read the fine print, and ask the right questions. Combine insurance with strong cybersecurity practices, and you'll be well-equipped to handle whatever the digital world throws your way.

COMMON PITFALLS WHEN CHOOSING CLOUD STORAGE

• Ignoring Security and Compliance Requirements

Always evaluate a provider's security certifications and data encryption methods.

• Choosing Based on Price Alone

Weigh costs against features, customer support, and the ability to grow with your business.

• Overlooking Integration with Existing Tools

Ensure the cloud storage solution integrates seamlessly with your current ecosystem.

• Underestimating Scalability Needs

Look for storage providers that offer flexible plans, tiered storage, and enterprise-ready infrastructure.

• Neglecting Backup and Redundancy

Storing data in the cloud doesn't automatically mean it's backed up. Look for providers with built-in backup and redundancy features.

SIMPLE AND EFFECTIVE BACKUP AND RECOVERY PLAN

Every business runs on data: customer information, financial records, communications, product files, and more. Yet data security is often in the bottom of the to-do list.

Unsure where to start? Here are simple, effective backup and recovery plans that every small business can use:

1. Know Your Storage Limits
2. Use a Cloud Service
3. Automate Your Backup Schedule
4. Test Your Recovery Plan
5. Keep a Local Backup for Fast Access
6. Educate Your Team
7. Keep Multiple Backup Versions
8. Monitor and Maintain Your Backups
9. Consider a Hybrid Backup Strategy

ADVANCED REMOTE WORK SECURITY STRATEGIES

A secure remote workplace in 2025 is not defined by perimeter defenses. It's powered by layered, intelligent, and adaptable systems. Here are some critical upgrades and strategic shifts your business should adopt now to keep your remote team secure.

- Embrace Zero Trust Architecture
- Deploy Endpoint Detection and Response (EDR) Solutions
- Strengthen Secure Access with VPN
- Automate Patch Management
- Cultivate a Security-First Culture
- Implement Data Loss Prevention (DLP) Measures

- Adopt Security Information and Event Management (SIEM) for Holistic Threat Visibility
- Centralize Your Visibility with a Unified Dashboard
- Standardize Identity and Access Management (IAM)
- Use Automation and AI for Faster, Smarter Threat Response
- Run Regular Security Reviews and Simulations
- Build for Long-Term Agility, Not Just Short-Term Fixes

These advanced tactics not only keep your systems safe but also ensure business continuity, regulatory compliance, and peace of mind.



CLIENT TESTIMONIAL

The biggest benefit to Morsches Builders Mart since moving to Preferred IT group has been moving our server into the cloud. It is easy to maintain and we don't have to worry about cleaning the server hardware. Preferred IT Group is knowledgeable of our systems and always has a quick response to our issues. The cost of the services is worth it for the service you receive.

Jeremy Hammel, Morsches Builders Mart