TALK NERDY TO ME

INSIDE THIS ISSUE:

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

HOW TO USE A PASSWORD MANAGER AND VIRTUAL CARDS FOR ZERO-RISK HOLIDAY SHOPPING

Have you ever been concerned about your credit card or personal data getting stolen while shopping online? You're not alone. Each holiday season, as millions of shoppers flock online for convenience, hackers ramp up their activity. The Federal Trade Commission (FTC) has warned that scammers often create fake shopping websites or phishing emails to steal consumers' money and personal information, especially during the holidays.

If you're planning to shop this holiday season, now is the perfect time to boost your online security. Two simple tools, password managers and virtual cards, can make a big difference. But how exactly?

Why People Prefer Password Managers and Virtual Cards for Online Shopping

Shopping online is quick, easy, and often cheaper than going to physical stores. However, it is fraught with security risks. Many people now use password managers and virtual cards for safer transactions.

A password manager creates and keeps complicated, distinct passwords for all accounts. This minimizes the chance of unauthorized access and theft. The Cybersecurity and Infrastructure Security Agency (CISA) recommends using password managers to reduce password reuse and protect sensitive data from hackers.

Virtual cards also add an extra layer of protection when shopping online. Although the card numbers are linked to your real credit or debit card account, the merchant never sees your card details. This helps prevent identity theft and financial fraud.

Tips for Using Password Managers and Virtual Cards for Zero-Risk Holiday Shopping

Before you start adding items to your cart, the safety of your money comes first. Here are smart ways to use these tools to improve online security during the holidays.

• Choose a Reputable Password Manager
Select a trusted provider with strong encryption and a solid reputation.

• Create a Strong Master Password
Your master password protects all your other passwords and should be the most secure.

• Turn On Two-Factor Authentication (2FA).
Even if hackers steal your password, they can't access your account without your verification code.

• Generate Virtual Cards for Each Store
This way, if one store is compromised, only that temporary card is affected your main account stays safe.

• Track Expiration Dates and Spending Limits
Virtual cards often expire after a set time or after one purchase. Set spending limits as well, as this helps with budgeting and prevents unauthorized charges.

• Shop Only on Secure Websites
Be sure to purchase only from websites you are familiar with.

Common Mistakes to Avoid for Safer Online Shopping

Even with the best security tools, simple mistakes can put your data at risk. Here are some common pitfalls to watch out for when shopping:

• Reusing Passwords
One hacked password can put all your accounts at risk.

• Using Public Wi-Fi for Shopping
Hackers can easily monitor public Wi-Fi networks, making them unsafe for any online activity.

• Ignoring Security Alerts
If your bank, password manager, or virtual card provider alerts you to suspicious activity, act immediately. Follow their instructions to protect your data.

• Saving Card Details in Your Browser
If hackers access your browser, your saved cards are compromised.

Need help improving your cybersecurity before the holiday rush? We can help you protect your data with smarter, easy-to-use security solutions. Stay safe, stay secure, and shop online with confidence this season. Contact us today to get started.

LUME CUBE EDGE LIGHT 2.0

Elevate your workspace with the Lume Cube Edge Light 2.0.

This sleek, clamp-on LED desk lamp features edge-lit technology for soft, flicker-free lighting, 270° rotation, USBA/C charging ports, and adjustable brightness and color temperature which makes it perfect for work or video calls.

Whether you're tweaking a design, snapping the perfect photo, or jumping on a video call to pitch your idea, the Edge 2.0 is the go-to desk lamp for getting things done in style.

HOW TO REDUCE WASTE IN MICROSOFT 365 SECURITY AND COPILOT ADD-ONS

Microsoft 365 is a powerful platform that helps a business in many ways. It boosts collaboration and streamlines operations, among other benefits. However, many companies waste money on unnecessary licenses and features that are not fully used.

The good news is that much of this waste can be avoided. With discipline, proper tools, and regulation, you can redirect your budget to a smarter use of Microsoft 365. Below are some of the main strategies to adopt.

Downgrade Light Users

Not all users require an E3 or E5 license. For example, why give your receptionist a complete E5 license with enhanced compliance tools if they're only emailing and using Teams? By monitoring actual usage, you can downgrade such users to E1 or another lower-tiered plan without affecting productivity. Low-usage discovery utilities enable you to downgrade confidently without speculation.

Automate Offboarding of Ex-Employees

By automating onboarding processes, licenses are unassigned automatically once you mark an employee as departed. Use workflow tools like Power Automate linked to HR systems or forms to revoke access, remove group memberships, convert mailboxes, and unassign licenses in one automated process.

Consolidate Overlapping Features

Review your security, compliance, collaboration, and analytics tools to find overlaps. If your plan already offers advanced threat protection or endpoint detection, consider canceling redundant third-party tools. If Copilot addons duplicate other AI or automation tools you already use, streamline them under one system.

Review Group and Shared Mailboxes

Many organizations mistakenly assign premium licenses to shared mailboxes, service accounts, or inactive mailboxes. This doesn't offer any functional benefits. Think about converting them to free shared mailboxes or archiving them to free up license slots. That way, you ensure that your M365 budget is only spent on value-generating users.

Enable License Expiration Alerts and Governance Policies

Avoid wastage in the future by setting up policy checks and notifications and make sure you respond as needed. Note down renewal dates for contracts so you don't accidentally auto-renew unused licenses. Also, track levels of inactivity and flag for review licenses that have passed the threshold.

Make Microsoft 365 Work Smarter for You

Don't let Microsoft 365 licenses and add-ons quietly drain your resources. Take control by reviewing how each license is used. When you match your tools with actual business needs, you save money, simplify management, and improve productivity in your organization.

Optimizing your Microsoft 365 environment means getting full value from what you already have. When you use M365 security and Copilot add-ons responsibly, your business is likely to thrive.

THE SMB GUIDE TO MAKING YOUR WEBSITE AND DOCUMENTS DIGITALLY ACCESSIBLE

Have you ever thought about how many potential customers leave your site because of accessibility issues? A UK survey found that 69% of disabled internet users leave inaccessible websites. For small and medium businesses, this is a significant missed opportunity. This guide will show you simple, actionable steps to make your website and documents welcoming to everyone.

Make Your Visuals and Documents Accessible for All

Visual accessibility is often overlooked. Millions have visual impairments. Text should clearly stand out against its background, with a contrast ratio of at least 4.5:1. Use free tools like WebAIM's Contrast Checker for verification. When creating and sharing a PDF, ensure it is tagged with structured information (headings, paragraphs, tables) for screen readers. Add alt text to images and ensure a logical reading order. A simple accessibility test can ensure readability.

Make Reading Easier and Reduce Mental Effort

Use plain language, avoiding complex sentences or jargon. Break writing into short paragraphs with explanatory subheadings. Sans-serif fonts like Arial or Verdana are easier to read on screen; choose at least 14 points for body text and avoid all caps or italics. For deaf visitors, offer captions or transcripts for video and audio. For users with limited mobility, ensure your website is fully accessible with only a keyboard. Avoid features requiring fine motor control.

Make Accessibility Part of Your Brand

For SMBs, accessibility is a smart investment in reputation and customer relationships. It also protects against legal risks, as accessibility standards like the Americans with Disabilities Act (ADA) apply to many websites. Beauty and accessibility can coexist with intentional design choices.

5 ESSENTIAL RULES TO GOVERN CHATGPT AND AI

Managing ChatGPT and other AI tools isn't just about staying compliant; it's about keeping control and earning client trust.

Follow these five rules to set smart, safe, and effective AI boundaries in your organization.

1. Set Clear Boundaries Before You Begin
2. Always Keep Humans in the Loop
3. Ensure Transparency and Keep Logs
4. Understand How Intellectual Property and Data Protection Works
5. Make Governance a Continuous Practice

These rules work together to create a solid foundation for using AI responsibly. As AI becomes part of daily operations, having clear guidelines and governance keeps your organization on the right side of ethics and the law.

PRIVACY COMPLIANCE CHECKLIST 2025

- Data Collection: Be clear about what data you collect.
- Consent Management: Consent must be active, recorded, and reversible.
- Third-Party Disclosures: Be honest about what third parties process your user's data.
- Privacy Rights and User Controls: Outline users' rights to their data, and objection to its processing.
- Cookie Management and Tracking: Clearly disclose tracking tools and refresh them regularly.
- Compliance Assurance: If you have international customers, be GDPR, CCPA/CPRA, and other privacy laws compliant.
- Contact and Governance: Your privacy policy should have the name of a Data Protection Officer or privacy contact point.
- Policy Update: Add a "last updated" date to your privacy policy.
- Automations and AI: Platforms used must be revealed.

WHAT TO REVIEW BEFORE INTEGRATING A THIRD-PARTY API

There can be hidden risks linked to using third-party API integrations. Before connecting, complete a thorough app and security vetting process using this checklist:

- Ensure the application provider holds recognized certifications.
- Review the app documentation, security policies, or compliance certifications to ensure that all data in transit is encrypted with strong protocols.
- Confirm that the app uses modern authentication standards or token based methods like JWT.
- Check if the vendor has proper logging in place by reviewing their documentation and security policy.
- Verify that the API provider maintains versioning, guarantees backward compatibility, and communicates deprecation schedules.
- The app should support rate limiting & quotas.
- Insist on contractual terms that allow you to audit their security practices.
- Understand where the third-party stores and processes data.
- Ask the vendor how they handle downtime, redundancy, fallback mechanisms, and data recovery.
- Request a list of upstream libraries and dependencies used by the vendor.