

TECH TIPS

TECHNOLOGY INSIGHT THAT BUILDS BUSINESS



HODGSON
CONSULTING & SOLUTIONS

June 2025

INSIDE THIS ISSUE

Shadow IT: How Employees Using Unauthorized Apps Could Be Putting Your Business At Risk |1

Why Your Business Needs Regular Network Pen Tests |2

Is Your Printer The Biggest Security Threat In Your Office? |3

Don't Fall For This Travel Scam |4

Vacation Smarter, Not Harder With These Savvy Tech Tools |4

SHADOW IT:

How Employees Using Unauthorized Apps Could Be Putting Your Business At Risk

Your employees might be the biggest cybersecurity risk in your business—and not just because they're prone to click phishing e-mails or reuse passwords. It's because they're using apps your IT team doesn't even know about.

This is called Shadow IT, and it's one of the fastest-growing security risks for businesses today. Employees download and use unauthorized apps, software, and cloud services—often with good intentions—but in reality they're creating massive security vulnerabilities without even realizing it.

What Is Shadow IT?

Shadow IT refers to any technology used within a business that hasn't been approved, vetted, or secured by the IT department. It can include things like:

- Employees using **personal Google**
- **Drives or Dropbox** accounts to store and share work documents.

- Teams signing up for **unapproved project management tools** like Trello, Asana, or Slack without IT oversight.
- Workers installing **messaging apps like WhatsApp or Telegram** on company devices to communicate outside of official channels.
- Marketing teams using **AI content generators** or automation tools without verifying their security.

Why Is Shadow IT So Dangerous?

Because IT teams have no visibility or control over these tools, they can't secure them—which means businesses are exposed to all kinds of threats.

- **Unsecured Data-Sharing:** Employees using personal cloud storage, e-mail accounts, or messaging apps can accidentally leak sensitive company information, making it easier for cybercriminals to intercept.

continued on page 2...

This monthly publication is provided courtesy of Robert Zehnder, President of Hodgson Consulting & Solutions.



OUR MISSION:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

...continued from cover

- **No Security Updates:** IT departments regularly update approved software to patch vulnerabilities, but unauthorized apps often go unchecked, leaving systems open to hackers.
- **Compliance Violations:** If your business falls under regulations like HIPAA, GDPR, or PCI-DSS, using unapproved apps can lead to noncompliance, fines, and legal trouble.
- **Increased Phishing And Malware Risks:** Employees might unknowingly download malicious apps that appear legitimate but contain malware or ransomware.
- **Account Hijacking:** Using unauthorized tools without multifactor authentication (MFA) can expose employee credentials, allowing hackers to gain access to company systems.

Why Do Employees Use Shadow IT?

Most of the time, it's not malicious. Take, for example, [the "Vapor" app scandal](#), an extensive ad fraud scheme recently uncovered by security researchers at IAS Threat Lab.

In March, over 300 malicious applications were discovered on the Google Play Store, collectively downloaded more than 60 million times. These apps disguised themselves as utilities and health and lifestyle tools but were designed to display intrusive ads and, in some cases, phish for user credentials and credit card information. Once installed, they hid their icons and bombarded users with full-screen ads, rendering devices nearly inoperative. This incident highlights how easily unauthorized apps can infiltrate devices and compromise security.

Employees often turn to these unauthorized apps because:

- They find company-approved tools frustrating or outdated.
- They want to work faster and more efficiently.
- They are unaware of the risks.
- They think IT approval takes too long, so they take shortcuts.

Unfortunately, these shortcuts can cost your business BIG when a data breach happens.

How To Stop Shadow IT Before It Hurts Your Business

You can't stop what you can't see, so tackling Shadow IT requires a proactive approach. Here's how to get started:

1. Create An Approved Software List

Work with your IT team to establish a list of trusted, secure applications employees can use. Make sure this list is regularly updated with new, approved tools.

2. Restrict Unauthorized App Downloads

Set up device policies that prevent employees from installing unapproved software on company devices. If they need a tool, they should request IT approval first.

3. Educate Employees About The Risks

Employees need to understand that Shadow IT isn't just a productivity shortcut—it's a security risk. Regularly train your team on why unauthorized apps can put the business at risk.

4. Monitor Network Traffic For Unapproved Apps

IT teams should use network-monitoring tools to detect unauthorized software use and flag potential security threats before they become a problem.

5. Implement Strong Endpoint Security

Use endpoint detection and response (EDR) solutions to track software usage, prevent unauthorized access, and detect any suspicious activity in real time.

Don't Let Shadow IT Become A Security Nightmare

The best way to fight Shadow IT is to get ahead of it before it leads to a data breach or compliance disaster.

Want to know what unauthorized apps your employees are using right now? Start with a Network Security Assessment to identify vulnerabilities, flag security risks, and help you lock down your business before it's too late. ■

HODGSON CONSULTING & SOLUTIONS

Why Your Business Needs Regular NETWORK PEN TESTS

A Network Penetration Test (Pen Test) is the **ONLY** way to find out what hackers can access in your environment.

- Simulates what a **HACKER** could do in your network.
- Accurate view of **actual risks** rather than supposed risks.
- Test your current **IT Team** to see what they could be doing to put the company & you at **RISK!**
- Exploits any found **security vulnerabilities** to see the impact of a breach.
- A deeper **evaluation** of your security systems and vulnerabilities.
- Identify and prioritize **remediation actions** more accurately based on risk levels.

PROACTIVE CYBERSECURITY STARTS HERE.

Call To Schedule Your Network Penetration Test at **(847) 906-5005** or visit www.hodgsonconsulting.com/discovery

IS YOUR PRINTER THE BIGGEST SECURITY THREAT IN YOUR OFFICE?



If I asked you to name the biggest cybersecurity threats in your office, you'd probably say phishing e-mails, malware, or weak passwords. But what if I told you that your office printer—yes, the one quietly humming in the corner—could be one of the biggest vulnerabilities in your entire network?

It sounds ridiculous, but hackers love printers. And most businesses don't realize just how much of a security risk they pose—until it's too late. In 2020, Cybernews ran what they called the "Printer Hack Experiment." Out of a sample of 50,000 devices, they successfully compromised 56% of the printers, directing them to print out a sheet on printer security. That's nearly 28,000 compromised devices—all because businesses overlooked this "harmless" piece of office equipment.

Wait, WHY Target Printers?

Because printers are a goldmine of sensitive data. They process everything from payroll documents and contracts to confidential client information. And yet, most businesses leave them wide open to attack.

Here's what can happen when a hacker gains access to your printer:

- **Printers store sensitive data:** Every time you print, scan, or copy a document, your printer keeps a digital copy. Many printers have built-in hard drives that store years' worth of documents, including payroll files, contracts, and employee records. If a hacker gains access, they can steal or even reprint those files without your knowledge.
- **Default passwords are a hacker's dream:** Most printers come with default admin logins like "admin/admin" or "123456." Many businesses never change them, making it easy for cybercriminals to take control.

- **They're an open door to your network:** Printers are connected to your WiFi and company network. If compromised, they can be used as an entry point to install malware or ransomware, or steal data from other devices.
- **Print jobs can be intercepted:** If your print jobs aren't encrypted, hackers can intercept documents before they even reach the printer. That means confidential contracts, legal documents, and even medical records could be exposed.
- **They can spy on your business:** Many modern printers have built-in storage and even scan-to-e-mail features. If a hacker compromises your device, they can remotely access scanned documents, e-mails, and stored files.
- **Outdated firmware leaves the door wide open:** Like any device, printers need security updates. But most businesses never update their printers' firmware, leaving them vulnerable to known exploits.
- **Data mining from discarded printers:** Printers that were improperly disposed of can be a goldmine for cybercriminals. Residual data stored on discarded printers can be mined for sensitive information! This can result in potential security breaches. Printers need to have their storage wiped clean to avoid being vulnerable to data breaches and legal liabilities.

How To Protect Your Printers From Hackers

Now that you know printers can be hacked, here's what you need to do immediately:

1. **Change The Default Password** – If your printer still has the default login credentials, change them immediately. Use a strong,

unique password like you would for your e-mail or bank account.

2. **Update Your Printer's Firmware** – Manufacturers release security patches for a reason. Log into your printer settings and check for updates, or have your IT team do this for you.

3. **Encrypt Print Jobs** – Enable Secure Print and end-to-end encryption to prevent hackers from intercepting print jobs.

4. **Restrict Who Can Print** – Use access controls so only authorized employees can send print jobs. If your printer supports PIN codes, require them for sensitive print jobs. You can also add a guest option.

5. **Regularly Clear Stored Data** – Some printers let you manually delete stored print jobs. If yours has a hard drive, make sure it's encrypted, and if you replace a printer, wipe or destroy the hard drive before disposal.

6. **Put Your Printer Behind A Firewall** – Just like computers, printers should be protected by a firewall to prevent unauthorized access.

7. **Monitor Printer Activity** – If your IT team isn't already tracking printer logs, now is the time to start. Unusual print activity, remote access attempts, or unauthorized users printing sensitive documents should be red flags.

Printers Aren't Just Office Equipment—They're Security Risks

Most businesses don't take printer security seriously because, well, it's a printer. But cybercriminals know that businesses overlook these devices, making them an easy target.

If you're protecting your computers but ignoring your printers, you're leaving a huge hole in your cybersecurity defenses.

DON'T FALL FOR THIS TRAVEL SCAM

Cybercriminals are exploiting travel season by sending fake booking confirmations that look like legitimate e-mails from airlines, hotels, and travel agencies. These scams steal personal and financial information and spread malware.

How The Scam Works

1. A Fake Booking Confirmation Lands In Your Inbox

- Appears to be from travel companies like Expedia, Delta, or Marriott.
- Uses official logos, formatting, and fake customer support numbers.
- Subject lines create urgency, such as *"Your Flight Itinerary Has Changed—Click Here For Updates."*

2. Clicking the Link Redirects You To A Fake Website

- E-mail prompts you to log in to confirm details, update payment info, or download an itinerary.
- The link leads to a fraudulent website that steals your credentials.

3. Hackers Steal Your Information And/Or Money

- Entering login credentials grants hackers access to your airline, hotel, or financial accounts.
- Providing payment details leads to stolen credit card information or fraudulent charges.
- Clicking malware-infected links can compromise your entire device.

Why This Scam Works

- **It Looks Legit** – Uses real logos, formatting, and familiar-looking links.
- **It Creates Urgency** – "Reservation issues" or "flight changes" cause panic, making victims act fast.
- **People Are Distracted** – Busy travelers often don't double-check e-mails.
- **It's A Business Risk Too** – If employees handling company travel fall for it, businesses face financial loss and security breaches.



How To Protect Yourself And Your Business

- **Always Verify Before Clicking** – Visit the airline or hotel's website directly.
- **Check The Sender's Address** – Scammers use slightly altered domains (e.g., "@delta.com.com" instead of "@delta.com").
- **Educate Your Team** – Train employees to recognize phishing scams.
- **Use Multifactor Authentication (MFA)** – Adds an extra security layer.
- **Secure Business E-mail Accounts** – Block malicious links and attachments.

VACATION SMARTER, NOT HARDER WITH THESE SAVVY TECH TOOLS



You've earned your vacation—don't let travel stress ruin it! These smart tech tips will keep you organized, secure, and stress-free.

Logistics Made Easy

Road Trips: Apps like Roadtrippers help you easily add 20+ stops (you can only add nine in Google Maps). Plus, you can plan trips in advance in the app.

Itineraries: Skip the e-mail digging—apps like TripIt or TripCase automatically compile travel details into one master itinerary.

Travel Prices: Apps like Hopper predict when to book for the best deals on flights, hotels, and car rentals. For bus or train travel, use

comparison apps like Wanderu.

Accommodation: Stick to trusted platforms like Vrbo or Airbnb and keep payments and communications within the platform so customer support can step in if something goes wrong.

Local Deals: Find local discounts on excursions, spa treatments, and restaurants through apps like Travelzoo.

Pack Smart

Digital packing assistants like PackPoint create lists based on your destination, activities, and trip length so you pack only what you need. In crowded areas, a phone lanyard can also be a lifesaver. For extra security, an RFID-blocking wallet can protect your credit cards and passport from electronic pickpocketing.

Protect Your Data

We would be remiss if we didn't mention data protection. Update your devices, enable multifactor authentication, and if you'll rely on public Wi-Fi, use a VPN to encrypt your connection. Bon voyage!



CARTOON OF THE MONTH



"I WON'T TRULY BELIEVE IN AI UNTIL IT FALLS FOR A PHISHING SCAM."