



# TECH TALK

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

## INSIDE THIS ISSUE:

Data Backup Is Not Enough	Page 1	Vulnerability Management for Your Tech	Page 2
Gadget of The Month	Page 1	Tech Tip of The Month	Page 2
Microsoft Forms	Page 2	Windows 8.1 Just Lost All Support	Page 2
Think Twice Before Using Self-Portrait Apps	Page 2	Technology Trivia	Page 2



We love technology and we love helping people. Give me a call today for a quick chat to find out how my team and I can help you secure your data better!

– Diana Scott

Owner – BlueCastle IT Solutions LLC

## DATA BACKUP IS NOT ENOUGH

The need to back up data has been around since floppy disks. Data loss happens due to viruses, hard drive crashes, and other mishaps. Most people using any type of technology have experienced data loss at least once.

There are about 140,000 hard drive crashes in the US weekly. Every five years, 20% of SMBs suffer data loss due to a major disaster. This has helped to drive a robust cloud backup market that continues to grow.

But one thing that’s changed with data backup in the last few years is security. Simply backing up data so you don’t lose it, isn’t enough anymore. Backing up has morphed into data protection.

*What does this mean?*

It means that backups need more cybersecurity protection. They face threats such as sleeper ransomware and supply chain attacks. Cloud-based backup has the benefit of being convenient, accessible, and effective. But there is also a need for certain security considerations with an online service.

Companies need to consider data protection when planning a backup and recovery strategy. The tools used need to protect against the growing number of threats.

Some of the modern threats to data backups include:

- **Data Center Outage:** The “cloud” basically means data on a server. That server is internet accessible. Those servers can crash. Data centers holding the servers can also have outages.
- **Sleeper Ransomware:** This type of ransomware stays silent after infecting a device. The goal is to have it infect all backups. Then, when it’s activated, the victim doesn’t have a clean backup to restore.
- **Supply Chain Attacks:** Supply chain attacks have been growing. They include attacks on cloud vendors that companies use. Those vendors suffer a cyberattack that then spreads throughout their clients.
- **Misconfiguration:** Misconfiguration of security settings can be a problem. It can allow attackers to gain access to cloud storage. Those attackers can then download and delete files as they like.

### What to Look for in a Data Protection Backup System

Just backing up data isn’t enough. You need to make sure the application you use provides adequate data protection. Here are some of the things to look for when reviewing a backup solution.

### Ransomware Prevention

Ransomware can spread throughout a network to infect any data that exists. This includes data on computers, servers, and mobile devices. It also includes data in cloud platforms syncing with those devices.

**95% of ransomware attacks also try to infect data backup systems.**

It’s important that any data backup solution you use have protection from ransomware. This type of feature restricts automated file changes that can happen to documents.

### Continuous Data Protection

Continuous data protection is a feature that will back up files as users make changes. This differs from systems that back up on a schedule, such as once per day.

Continuous data protection ensures that the system captures the latest file changes. This mitigates data loss that can occur if a system crashes before the next backup. With the speed of data

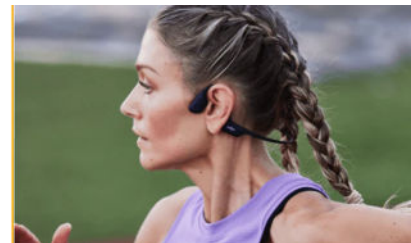
generation these days, losing a day’s worth of data can be very costly.

### Threat Identification

Data protection incorporates proactive measures to protect files. Threat identification is a type of malware and virus prevention tool. It looks for malware in new and existing backups. This helps stop sleeper ransomware and similar malware from infecting all backups.

### Zero-Trust Tactics

Cybersecurity professionals around the world promote zero-trust security measures. This includes measures such as multi-factor authentication and application safelisting.



## SHOKZ OPENRUN PRO

Crush your training goals and stay aware of traffic, pedestrians, cyclists, and more with the OpenRun Pro Premium Bone Conduction Open-Ear Sport Headphones.

Featuring IP55 Water-Resistance to go anywhere.

10 hours of music and calls to keep you powered up through two-a-days or long training sessions.

Featuring a 5-minute Quick Charge for up to 1.5 hours of battery life.

# MICROSOFT FORMS: ONE OF THE HANDIEST FREEBIES IN MICROSOFT 365

Microsoft 365 is one of the most popular cloud platforms in the world, with about 345 million paid seats.

Users get a stable of over 20 different apps, including the core MS Office suite.

With so many different apps, it's not uncommon for some to go unused.

Companies may not even be aware they have access to these other helpful tools.

One of the handiest apps you get with a Microsoft 365 subscription is Microsoft Forms.

## What Is Microsoft Forms?

Microsoft Forms is a drag-and-drop form, quiz, and survey creator. It's simple to use and allows you to send out surveys via a link. Recipients can fill out your form online from any device.

**How to Get Started in Forms:**

1. Visit Forms.office.com and log into your Microsoft account.
2. Choose "New Form" or "New Quiz: from the top menu
3. OR you can choose to explore the built-in templates
4. Click "Add New" to add a new form field. You can choose from field types:

- Choice (i.e., multiple-choice question)
  - Text
  - Rating
  - Date
  - Ranking
  - Likert (a scale that records attitudes/opinions about a topic)
  - Net Promoter Score® (a scale from "not likely" to "extremely likely")
  - Section (separator that can include a title and image)
5. Enter your questions.

6. Once finished, click "Send" at the top. You can distribute the survey using the following options:

- Link to a web form
- Email
- QR code
- Embed in a web page
- Via Facebook or Twitter

7. View responses on the "Responses" tab

## Advantages of Using Microsoft Forms

### It's Included in Microsoft 365 Subscriptions

If you already subscribe to Microsoft 365, then you automatically get access to MS Forms.

### It Saves Time

No emailing attachments back and forth, and Forms collates survey responses automatically.

## Get Charted Results

You can quickly see the results of the survey in meaningful graphs.

## It's Easy to Use

There's a very low learning curve with Microsoft Forms.

The interface is intuitive and simple, so just about everyone can jump in and start using it.

## What Are Some Ways You Can Leverage Microsoft Forms?

- Annual Customer Satisfaction Survey
- Employee Security Awareness Quiz
- Change Readiness Survey
- Event Registrations
- Volunteer Registration Form

## WHY YOU NEED TO THINK TWICE BEFORE USING LENSA AI & OTHER SELF-PORTRAIT APPS

It's a common theme. You begin seeing these amazing CGI images of your friends on Facebook or Instagram.

You think, "How can I make one?"

The latest of these modern vanity marvels to make the rounds is Lensa AI.

You upload about 10 photos so the app can feed that data into its AI algorithm.

Then, once it maps your facial features, it generates several fantasy profile pics.

It sounds like a little harmless digital fun, right?

That's what many companies making apps like this like you to think. Vanity is an easy sell.

But for Lensa AI and several similar self-portrait apps, you're paying more than you know. The cost comes from the data privacy rights you're giving up.

And these can go far beyond the app itself.

### Why Worry About Data Privacy with Lensa AI & Similar Apps?

#### Data Used to Track You

Once you download the Lensa AI app, it can track your phone activity in other apps.

#### Data Collected

By downloading Lensa AI, you permit it to track all kinds of data, including the purchases you make online.

#### Loss of Rights to Your Uploaded Images

Lensa AI Terms require you to grant a sub-licensable license to use, reproduce, modify, distribute, and create derivative works of your user content.

#### Get a Device Privacy Checkup

The more apps you use, the more complicated data privacy can get. Don't leave it to chance.

## EVERY COMPANY IS NOW A TECHNOLOGY COMPANY

Whether you sell shoes or run an accounting firm, you need some type of technology to operate. Today's companies aren't just in the business of selling their own goods and services anymore.

1. Technology Is a Critical Part of Business
2. Customers Expect an Excellent Digital Experience
3. Employees Need Devices to Drive Productivity
4. AI & Automation Help Companies Stay Competitive
5. Information Is Being Generated at a Rapid Pace
6. Vendors/Suppliers Are Leaving Legacy Systems Behind
7. It's Difficult to Grow Without Tech Innovation
8. Business Continuity Needs

## 6 STEPS TO EFFECTIVE VULNERABILITY MANAGEMENT FOR YOUR TECHNOLOGY

Technology vulnerabilities are an unfortunate side effect of innovation. When software companies push new updates, there are often weaknesses in the code. Hackers exploit these.

Software makers then address the vulnerabilities with a security patch. The cycle continues with each new software or hardware update.

61% of security vulnerabilities in corporate networks are over 5 years old.

- Step 1. Identify Your Assets
- Step 2: Perform a Vulnerability Assessment
- Step 3: Prioritize Vulnerabilities by Threat Level
- Step 4: Remediate Vulnerabilities
- Step 5: Document Activities
- Step 6. Schedule Your Next Vulnerability Assessment Scan

## WINDOWS 8.1 JUST LOST ALL SUPPORT. HERE'S WHAT YOU NEED TO KNOW

The latest operating system to lose all support is Windows 8.1.

Microsoft released the OS in 2013, and it was officially retired on January 10, 2023. Microsoft issued the following warning for companies:

*"Continuing to use Windows 8.1 after January 10, 2023 may increase an organization's exposure to security risks or impact its ability to meet compliance obligations."*

### Here are a few facts you should know:

- The OS Will Still Technically Work
- Your System Will No Longer Receive Security Patches
- Options for Upgrading are Windows 10 or 11

### What Happens if you don't upgrade?

- Security & Compliance Issues
- Slowed Productivity
- Incompatibility With Newer Tools

## TECHNOLOGY TRIVIA

Each month you have a chance to win a \$50 Amazon Gift Voucher by being the first person to email us with the answer to our Technology Trivia Question of the Month!

### The Question This Month is:

*In what video game series did Microsoft's virtual assistant Cortana make her debut?*

The first person to email me at info@bluecastleit.com with the correct answer gets a \$50 Amazon Gift Card!

