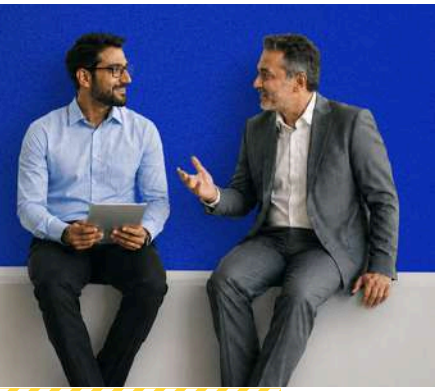
DIAMOND TIMES
A Technology Management Company

6 QUESTIONS

Smart Companies Ask Their IT Provider Every Quarter



If you're talking to your IT provider only when you renew your contract, you're doing it wrong. Technology isn't a "set it and forget it" part of your business. It's constantly evolving and so are the threats that come with it. That's why quarterly IT check-ins are non-negotiable if you want your business to stay protected, productive and competitive.

But here's the thing: Most business owners don't know what to ask. These are the questions your IT provider should be ready to answer every single quarter without tech-speak or vague promises.

Question 1: What security problems do we need to address?

Every business has vulnerabilities. The important question is whether your IT provider is actively identifying and addressing them before they become costly.

Ask them:

- Are there systems that need security patches?
- Have there been any unusual login attempts or suspicious activity?
- Are there users, devices or processes creating unnecessary risk?

You want specifics, not a generic "you're protected" response. A good IT provider should be able to explain where your biggest risks are today and what's being done about them.

Question 2: Have you tested our backups recently?

A backup is valuable only if it works when you need it. That sounds obvious, but many businesses assume they're protected simply because backups exist. Then a server fails, ransomware hits or someone accidentally deletes critical data, and suddenly nobody's sure how quickly systems can be restored.

Ask:

- When was the last full recovery test?
- How long would restoration realistically take?
- Are backups stored securely and separately from our primary systems?
- Are cloud applications included in backup coverage?

You don't want guesses during an outage. You want a process that's already been tested under pressure.

Question 3: Where is our technology slowing us down?

Most productivity issues don't look dramatic enough to trigger an IT emergency. They show up when your team loses momentum throughout the day.

An employee waits 15 seconds for an application to load dozens of times before lunch. A sales call freezes halfway through a proposal. Someone avoids using a system altogether because it's become unreliable and frustrating.

...continued on page 3

WHAT'S NEW

AI is moving at lightning speed. In just one month, our DIAMOND AI platform went from 70+ models to 80+ – and the pace isn't slowing down. The same is true on the risk side: scams are only getting more sophisticated, sharper, and harder to spot (see page 2 and page 4).

That's exactly why AI adoption needs a plan – and a platform that puts security first. DIAMOND AI gives your team access to 80+ AI models in one place – your data stays private and under your control. No shadow AI. No data leaking to free tools. Just a structured path forward which has birthed our mantra: Crawl, Walk, Run.

Curious about DIAMOND AI Platform? Join our August 20th Early Adopters webinar — **Register HERE**. This won't be recorded. Miss it and miss your edge.

Dedicated to your Success,

Team Diamond

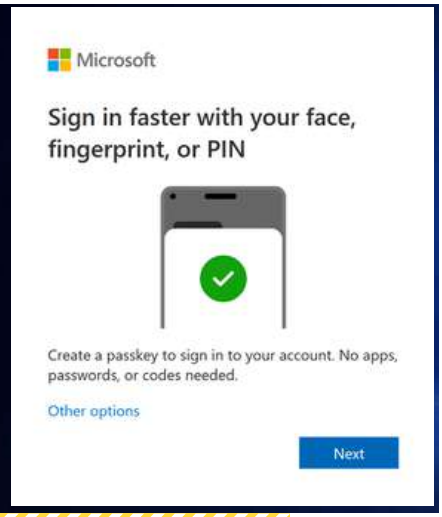
This monthly publication is provided courtesy of Cora Park, President of Diamond Business Communications.

OUR MISSION:

To help connect clients with expertise necessary to incoporate the diverse and emerging technologies needed for today's business, while providing a collaborative first-class support platform to allow them to achieve great things.

HELLO PASSKEYS GOODBYE SMS CODES

Here's What This Means for You



What's Changing

Microsoft is retiring text message (SMS) and phone call verification for Microsoft 365 accounts. Starting September 1, 2026, you may be prompted to set up a new login method called a passkey. By February 1, 2027, this becomes required — accounts still relying on a texted code will be blocked until a passkey is set up.

What is a Passkey?

A passkey replaces the SMS/text code with something simpler and more secure: your device verifies it's really you using your fingerprint, Face ID, or PIN — then signs you in automatically. No code to wait for, nothing to type.

Most users will set this up through the Microsoft Authenticator app on their smartphone. Windows users may be prompted to use Windows Hello instead, which uses your computer's fingerprint reader or camera. Either way, setup takes about two minutes, and day-to-day sign-ins actually become faster.

What You'll See

After September 1st, you may notice a new screen during your normal Microsoft sign-in asking you to set up a passkey. This is expected and legitimate. You can skip it for a while, but not after February 1, 2027.

What You Should Do

1. Install the Microsoft Authenticator app on your phone if you haven't already (search "Microsoft Authenticator" in the App Store or Google Play).

2. Don't panic when the prompt appears — it's a normal part of your sign-in and your IT team is expecting it.

3. Wait for instructions from your IT team. We'll send step-by-step guidance before each deadline.

4. When in doubt, call us before clicking anything unfamiliar.

What Won't Change

Your email and Microsoft 365 apps aren't going anywhere. Outlook, Teams, Word, Excel, SharePoint - all of it stays exactly the same. The only thing changing is how you prove it's you at login. Think of it like getting a new key for the same door. The office hasn't moved - you've just got a better lock.

This Is What "We've Got You" Looks Like

If you're a Diamond client, we're managing every step. Not a client yet? That's exactly the kind of support we offer. You shouldn't navigate tech transitions alone — that's what a trusted IT partner is for.

🚨 Watch Out for the "ClickFix" CAPTCHA Scam!

Cybercriminals are using a clever trick called ClickFix to get you to install malware on your own computer — without you even realizing it.

It starts with a webpage that looks like a normal "Verify you're human" CAPTCHA check. When you click it, a hidden malicious command is silently copied to your clipboard. The page then instructs you to press a keyboard shortcut (like Win + R), paste with Ctrl + V, and hit Enter — telling you it's just part of the verification. It isn't. You've just run malware yourself.

Once executed, it silently steals saved passwords, browser data, and login credentials. There's no warning. Your device looks completely normal.

The golden rule: Real CAPTCHAs never ask you to leave your browser. If a page tells you to open a system tool or paste anything into Windows, close the tab immediately and copy a harmless piece of text to clear your clipboard.

Stay sharp, trust your instincts, and fall back on your security awareness training — it exists for exactly these moments!

EARLY ADOPTER DIAMOND AI WEBINAR

AI Is Here. The Question Is: Is Your Organization Ready?

Join our Early Adopters Webinar and get a first look at how nonprofits and SMBs can embrace AI securely, strategically, and productively. Gain insight into:

- How to prevent employees from unknowingly exposing sensitive data
- Ways to save time by automating repetitive tasks and workflows
- How to bring AI tools under one secure, managed approach
- What a practical AI adoption strategy looks like for SMBs and nonprofits

To Reserve Your Spot for the FREE Early Adopters August 20th Webinar, click HERE.

CARTOON OF THE MONTH

"We're seeing a lot of consistency"

...continued from page 1

Ask your provider:

- Are there recurring performance problems?
- Are we outgrowing our current hardware or software?
- What systems generate the most complaints internally?
- Is there anything we should optimize or replace?

Technology should help your team move faster, not train them to tolerate inconvenience.

Question 4: Are we still compliant with industry regulations?

Compliance regulations change constantly, whether you're dealing with HIPAA, PCI-DSS, GDPR, cybersecurity insurance requirements or other industry-specific standards.

A company that was compliant last year can easily drift out of alignment without realizing it.

Ask:

- Have any compliance requirements changed recently?
- Are there gaps in our documentation or policies?
- Do we need additional employee training?
- Are there security controls we should strengthen?

The cost of noncompliance usually extends far beyond fines. It affects insurance claims, legal exposure and customer trust.

Question 5: What should we be budgeting for next quarter?

Good IT planning eliminates surprises. Your provider should be tracking aging hardware, expiring warranties, software license renewals, upcoming infrastructure upgrades and security investments worth planning for.

Quarterly reviews should help you make decisions early, spread costs out intelligently and avoid emergency purchases that wreck budgets.

Question 6: Where are we falling behind that's leaving us exposed?

This is the question too many IT providers avoid because it requires strategic thinking, not just technical fixes.

Ask them:

- Are there new tools or automations we should consider?
- Are we lagging behind in any security protocols or performance benchmarks?
- What are other businesses our size doing that we aren't?
- Have cybersecurity standards changed in ways that affect us?

Technology moves fast, but cybercriminals move faster. A good IT partner helps you stay ahead of both.

Silence is a red flag

If your IT provider isn't meeting with you quarterly or can't answer these questions, it's time to ask why. The right partner helps you stay ahead of problems, reduce risk and make smart technology decisions.

THE MOST DANGEROUS RISKS IN YOUR BUSINESS

Don’t Swim On The Surface

On the surface, the water looks calm.

That’s what makes Shark Week fascinating every year. The danger is rarely visible right away. It’s what’s already moving underneath.

Cybercriminals operate the same way. The threats businesses face are designed to blend in with normal operations until the moment something breaks, money moves or systems go down.

During the summer, when schedules shift, employees travel and oversight gets thinner, attackers know businesses are often paying less attention.

Here are three ways they’re circling right now.

1. Fake invoices and vendor impersonation

Attackers don't need to hack anything.

They need just one believable email. Business email compromise (BEC) works by impersonating a vendor, supplier or executive your team already trusts. The email arrives looking normal, someone pays the "vendor," and by the time anyone realizes it wasn't legitimate, the damage is done.

These attacks spike during vacation season. When the person who normally approves payments is out, requests get rerouted to people who don't know what normal looks like. Temporary stand-ins are less likely to question urgency.

To ward off attackers, build a verification process for any financial request via email. A quick confirmation call to a known number stops most of these before they go anywhere.

2. Phishing attacks that target distracted employees

Phishing works because it's engineered around how people behave when they're busy. A distracted employee sees a password reset and clicks. Someone gets a text from "IT." An email arrives before a meeting requesting urgent approval.

Nobody stops to verify because stopping feels like losing time.

To fix this, employees need to feel comfortable slowing down when something seems off — an unexpected login, a payment instruction out of nowhere or a link they weren't expecting. Speed is a weapon attackers use against you. Slowing down is how you take it away.

3. Third-party risks that travel fast

When a vendor with access to your systems is compromised, the threat travels directly into your environment. This supply chain exposure is often far greater than businesses realize.

Software tools, service providers with credentials and contractors with lingering access all present paths most owners have never mapped. Outsourcing a service doesn't outsource accountability.

Answer these three questions:

- Which vendors can access your data or systems?
- What are they connecting to?
- Who is responsible internally for managing those relationships?

If those answers aren't clear, your exposure is increasing your risk.

CRISIS AVERTED

Three Close Calls. Zero Disruptions.

Hackers are working in overdrive. This month alone, three clients faced cyber incidents that could've been major headaches. Thanks to our advanced threat detection and rapid response protocols, we identified and isolated each one early – shutting it down before it became a nightmare. The right precautions were in place. The right tools were watching.

Don't wait for your close call to become a crisis. Give us a call today at 609-642-9300.

1542 Kuser Road B1
Hamilton, NJ 08619