TECHNOLOGY TIMES

Insider Tips to Make Your Business Run Faster, Easier and More Profitably

NOVEMBER 2026



The Hidden Side of AI:
Is Your Business Prepared?

AI is changing the way businesses work. It's also changing the way cybercriminals operate.

The same technology helping businesses improve productivity and security is making scams more convincing, phishing emails harder to detect and sensitive data easier to expose when it's used carelessly.

While businesses are using AI to boost security and productivity, cybercriminals are using the same technology to make attacks more convincing.

AI impersonation: Sounding right isn't enough anymore

Video and audio used to help distinguish someone real from someone trying to scam you. Now, AI lets cybercriminals create realistic voice messages, phone calls and videos that make their requests seem legitimate.

Even if you can spot telltale signs of AI-generated content today, those clues are disappearing quickly. Many of the warning signs people once relied on are already outdated.

Instead of depending on employees to detect a fake, establish verification procedures for sensitive requests such as money transfers or account changes.

AI may be able to imitate a person's voice or appearance, but it can't bypass strong security procedures and multi-factor authentication.

AI-generated phishing: Harder to spot than ever

Phishing messages once contained spelling mistakes, grammatical errors and awkward wording that made them easier to recognize. Typos, generic greetings and urgent language became familiar warning signs.

Today, many phishing emails are well written, personalized and difficult to distinguish from legitimate communication. AI has made these scams more polished and convincing than ever before.

Rather than focusing only on how a message looks, pay attention to what it's asking you to do. Don't trust a message simply because it gets the details right.

Shadow AI: Think before you share sensitive data

When employees use AI tools that haven't been approved by the business, they may unintentionally expose sensitive company information to platforms that haven't been properly vetted.

An AI tool can't read every file in your organization on its own, but it won't stop someone from pasting confidential financial reports, customer information or internal business plans into a prompt and asking for help.

Before employees use any AI tool for work, your business should understand how it handles data, where that information is stored and whether it meets your security and compliance requirements.

A good IT partner doesn't tell you to avoid AI. They help you use it confidently by putting the right safeguards, policies and security controls in place, so your business can embrace new technology without creating unnecessary risk.

HALIFAXTEC

Your Cybersecurity Needs an Immune System, Not a Medicine Cabinet



Most medicine cabinets tell a story. There's cold medicine left over from last winter, vitamins bought in bulk, half-used bottles of cough syrup and a prescription that should probably have been thrown out months ago.

Cybersecurity can end up looking much the same. A new threat prompts one purchase, an insurance requirement leads to another and a vendor recommendation adds something else. Over time, the more useful question becomes whether your business has the right protections in place and if they're doing what they need to do.

Cyber myth: More tools mean better cybersecurity

It's an easy assumption to make. If one security product adds protection, then adding more should make your business even safer. But that's where the myth starts to break down.

Multiple layers of protection can be valuable, but only when each one serves a clear purpose. Adding another product may address a specific concern, but it can also create unnecessary overlap or additional complexity if no one considers how everything fits together.

What matters is whether the right safeguards are in place, properly managed and working together to address the risks your business faces.

Healthy cybersecurity works like a system

Your immune system isn't a shelf of individual remedies. It's a coordinated system designed to recognize problems and respond to them.

Your company's cybersecurity should work the same way, but for many businesses, the pieces don't always come together that neatly.

Tools get purchased to solve specific problems. Employees receive policies and training. New safeguards are added as risks change or requirements evolve. Each decision may make sense on its own, but over time, those individual pieces can become disconnected from the bigger picture.

That's where coordination matters. The right safeguards should complement each other rather than simply coexist.

Security tools are part of that system, but they're most effective when they work as part of a broader approach that still fits the business's needs.

Give your security a check-up

You don't need to understand the technical details of every cybersecurity product your company uses. But you should be able to get clear answers to a few basic questions.

1. What are we currently using, and why?

Someone on your team or a trusted outside partner should be able to explain what your major security protections do and why they're there. If nobody can give you a clear answer, that's worth looking into.

2. Where do our protections overlap, and where are the gaps?

Overlap isn't automatically a problem. Sometimes layered protection is intentional. What matters is knowing whether your security approach was designed that way or simply grew over time without much coordination.

3. Who is making sure everything is working?

A tool can generate alerts around the clock, but that doesn't help much if nobody is reviewing them or knows what should happen next. The important thing is knowing that someone is responsible for the outcome and paying attention.

4. When did we last reevaluate what we need?

Businesses change. People join and leave, new applications get adopted and teams start working in different ways. Cybersecurity that made sense when it was first implemented may no longer fit the business as it exists today.

Cybersecurity Myth Busters:

6 Things Small Businesses Still Get Wrong



Cybersecurity advice is everywhere, but not all of it is accurate. It's worth taking a step back every so often to separate what you know from what you only think you know.

Some have circulated for so long that it's taken on a life of its own, repeated until it sounds like fact even when it's outdated or wrong.

When bad advice goes unchallenged, it creates blind spots. And blind spots are exactly what cybercriminals look for.

The good news is these gaps are simple to close once you know where they are. Here are six myths we hear regularly from small business owners, along with the truth behind each one.

Myth 1: We're too small for cybercriminals to care about

There is no such thing as a business too small for an opportunistic cybercriminal. It doesn't matter if you're a one-person operation, a small business with a dozen employees or a large corporation. If you have exposed accounts or vulnerable systems, bad actors will take advantage of it. A small business offers valuable data, access to bank accounts or entry points to customers and vendors.

Fact: Hackers choose targets based on opportunity, not size.

Myth 2: Employees will recognize a phishing email

Some myths have circulated for so long that they've taken on lives of their own, repeated until they sound like fact even when they're outdated or wrong.

Thanks to AI, it's become harder to catch a scam email from the text alone. Instead, your team needs to think about sender behavior. For example, ask yourself if the supposed sender would:

- Make an unusual request
- Change payment instructions
- Request sensitive information
- Send a new or unusual login link

If anything seems off, double-check before clicking or responding.

Fact: A convincing email can still be a scam.

Myth 3: MFA fully protects our accounts

Multi-factor authentication (MFA) is important, but it's not invulnerable. Hackers use MFA fatigue to their advantage, counting on employees approving requests out of habit. For example, "prompt bombing" floods your phone with requests in hopes you'll approve access just to get them to stop.

continued on page 4 ...

Product Highlight of the Month: DMARC Protection

As cyber security threats increase, so do protections and one newer measure aimed at improving email authentication was implemented by major providers (such as Google and Microsoft) around the globe to help businesses authenticate their domains as legitimate. Bulk email senders (i.e. Constant Contact, Hubspot and other 3rd party sending services) are now required to have DMARC, DKIM and SPF verifications to authenticate their domains and the emails they send.

Halifaxtec's managed DMARC / DKIM / SPF services meet the implementation requirements and monitor activity related to sending email from your domain. They also include reporting, analysis and improved DMARC authentication. DMARC authentication protects your organization's domain from email impersonation, helping reduce spam, prevent financial loss from phishing attacks, and increase the likelihood that legitimate emails reach your customers' inboxes.

If you want to take a step to improve your DMARC / DKIM / SPF coverage reach out to Chris at ckane@halifaxtec or 386-241-0096.

CARTOON OF THE MONTH



"Do you still have regular coffee?"

... continued from page 3

Keep in mind, MFA is a tool, not a shield. Hackers are finding ways to get around weaker authentication methods, which is why MFA needs support from the controls around it.

Fact: MFA should be part of a broader security strategy.

Myth 4: Our backups have us covered

Ask yourself: If your business was hit with a ransomware attack tomorrow, could you restore your data? How long would it take?

A backup is great when you know it's going to work. However, an untested backup isn't something you can rely on during an incident. Knowing how long your business will be down can save you time and money.

Fact: Having backups is not the same as being able to recover.

Myth 5: Cybersecurity is only IT's responsibility

Your IT department does a lot to keep your business safe, but they can't control every click employees make. Cybersecurity decisions happen across every department. It takes only one bad click to open your systems to threats.

Employee security awareness training matters. When everyone knows what to look for and when to ask for help, they become part of your cybersecurity defenses.

Fact: Training employees to make good decisions strengthens your cybersecurity.

Myth 6: We know what to do if something happens

It's Tuesday morning. Several employees suddenly can't access their files. Many teams discover in that moment that nobody has answered the basic questions:

- Should employees shut down their computers?
- Who calls IT?
- What do you do if communication systems are down?
- When does the insurance company get involved?
- Who communicates with customers?

Don't rely on memory in the moment. Have an incident response plan.

Fact: Your recovery plan shouldn't debut during an incident.

Cybersecurity awareness starts with the facts

Strong cybersecurity starts with the facts. Many security gaps come from assumptions that go unchallenged.

If any of these myths sound familiar, it may be time to reassess your cybersecurity strategy. The businesses that stay ahead work with a trusted IT partner to identify gaps, strengthen their defenses and stay ahead of evolving threats.