



TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

How AI Helps Threat Actors
Commit Cyber-Crime.....Page 1

FREE Executive Guide:
Protect Your Data & Preserve
Your NetworkPage 2

Security Corner: SIM Swap
Protection.....Page 3

How To Spot A Scam
Email Now That They
Look Real.....Page 3

Why You Should Scroll
Past The First Result On
GooglePage 4

What To Do When
Microsoft 365 Goes
DownPage 4

September 2026



Kim Nielsen,
CISSP, CCSA
President &
Chief Technology
Strategist at
Computer
Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"



How AI Helps Threat Actors Commit Cyber-Crime

For years, cyber-crime has been framed as a problem for large enterprises, ones with deep pockets and valuable data. Small businesses frequently assumed that they were too small to matter to threat actors.

Now we know that's not true.

Even small businesses have faced a sharp increase in cyber-crime in the past few years, and artificial intelligence plays a major role. This shift has changed who attackers target and how easily they can launch effective campaigns.

In short: Artificial intelligence has definitely lowered the barrier to entry for cyber-crime.

Why AI Changed the Threat Landscape

Tasks that once required technical expertise, time, and resources can now be automated, refined, and scaled with minimal effort. Naturally, threat actors

have adopted it accordingly. More than 60% of organizations experienced AI-driven attacks in the past year.

Why is that? AI tools can...

- Generate convincing phishing emails
- Mimic familiar writing styles
- Analyze previously stolen data for patterns
- Adapt attacks in real time based on user behavior.

These are just a few ways that artificial intelligence fuels more and more cyberattacks! What once took days of preparation can now happen in a matter of minutes.

For small businesses, this means attackers no longer need to go after each individual target. Automation allows them to cast a wide net, and because of that, the volume of attacks often enables success.

Continued on pg.2

Why Hackers Target Small Businesses

Small organizations often rely on fewer security controls, lean IT teams, and limited training resources. At the same time, they still hold valuable data such as customer information, financial records, credentials, and access to larger partners.

AI-driven attacks exploit this imbalance. They personalize phishing messages, create scarily believable fake invoices, and even use deepfaking to make impersonation attempts sound more natural and urgent.

Attackers do not need to breach a large enterprise directly, especially when compromising a smaller business can provide an easier (and still lucrative) path.

Your Awareness Matters

As AI makes attacks more realistic, employees therefore become the primary line of defense. Many AI-driven attacks succeed not because of technical flaws, but because they exploit trust, urgency, and everyday *routine behavior*.

Up until now, phishing often contained obvious red flags that people have been trained to look for. AI has changed our prior assumptions so that now, these messages use proper grammar, the tone matches internal communications, and the context may even reference specific, real work projects. Public company social medias, and details on your own personal accounts, can give hackers enough real details to build a very convincing phishing scheme.

This makes awareness, reporting culture, and simple verification habits more critical than ever.

Preparing for an AI-Driven Threat Era

AI is not inherently the enemy, but it has changed the speed and scale of cyber-crime. Small businesses can't avoid becoming a target simply because of their size.

Reduce risk by understanding the need for...

- Clear security policies
- Regular security awareness refreshers
- Strong multi-factor authentication
- Safe reporting processes

You should feel empowered to pause, question, and report suspicious activity without fear of blame. If that's not the case, then you should take time now to review your company's incident response plan before a real threat strikes.

Conclusion

The rise of AI-driven attacks signals a significant turning point. Small businesses are firmly in the crosshairs, not because they are careless, but because modern tools make them easier to target at scale. Understanding this shift is the first step toward building resilience in an increasingly automated threat climate.

Cybersecurity is no longer just about preventing breaches. You can help protect your private data by recognizing that the threat landscape has evolved, and then responding with the same level of sophistication and awareness.

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems



This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
<https://www.cti-mi.com/protectdata926/>
or call our office at (248) 362-3800

Security Corner

SIM Swap Protection

There's a scam where a criminal takes over your phone number, and once they have it, they can get into a lot of your accounts.

It's called SIM swapping.

The attacker calls your mobile carrier, pretends to be you, and convinces them to move your number to a SIM card they control. Now your calls and texts go to them instead of you. That includes the security codes banks and other services text you, so they can easily reset your passwords and get into your accounts.

The main thing that stops it is a PIN on your mobile account. Every major carrier lets you set one, and then nobody can move your number without it. Call your carrier or check your account settings and turn it on.

It also helps to move your two-factor codes off text messages where you can. An authenticator app or a security key can't be hijacked by taking over your number, so use those for your important accounts.

And if your phone suddenly loses signal for no reason and stays dead while everyone around you is fine, call your carrier from another phone straight away. That's often the first sign someone's stealing your number.

For more information about this topic, call us at 248-362-3800.

How To Spot A Scam Email Now That They Look Real

For years the advice was simple: watch for bad spelling and clumsy grammar. Scammers now use AI to write their emails, so that advice no longer helps. The messages arriving in your team's inbox read as well as anything from a real company.

Why the old advice stopped working

That worked because many scammers were writing in a language that wasn't their own, and mistakes showed. AI removed that. The UK's National Cyber Security Centre says generative AI can now produce convincing phishing without the translation, spelling and grammatical mistakes that used to reveal it. The FBI says the same. Attackers can also feed public details about your company into an AI tool and get back a message with the right names, the right job titles etc.

Why these emails are so convincing now

- The writing is clean. A scam email reads like a normal business email, because a machine wrote it in seconds, in whatever tone the attacker asked for.
- It's personal. Attackers can feed public details about your company into an AI tool, pulled from your website, your team's LinkedIn profiles, or a press release, and get a message tailored to you: the right names, the right job titles, and a believable reason to be in touch.
- There's more of it. AI makes each message faster to produce, so attackers send far more. The FBI's Internet Crime Complaint Center added a section on AI to its annual report for the first time, tied to more than 22,000 complaints and nearly \$893 million in reported losses.

Your spam filter won't catch them all. It's tempting to assume your email security will handle this but a well written, personalized email that asks a normal-sounding question doesn't always look dangerous to a filter, especially when it carries no obvious bad link or attachment. Both the NCSC and the FBI expect AI to push more of these messages through, which is why the last line of defense is a person who knows what to check.

It's not just email anymore

AI has done the same thing to phone calls and texts. The FBI warns that criminals can clone a voice from a short audio clip, enough to leave a voicemail that sounds like your boss or a family member asking for an urgent payment. The same thing that makes AI emails so convincing makes AI phone scams convincing too. The defense is the same: if a call or voicemail asks for money or logins, hang up and call the person on a number you already have.

Here are the signs you should still pay attention to

If you can't trust how an email is written, look at what it's asking you to do:

- It asks for money, gift cards, or a payment to a new account.
- It asks for a login, a verification code, or personal details.
- It creates pressure: a deadline, a threat, or a "do this now."
- It asks you to change the bank details for an invoice or a supplier.
- It comes with a link or attachment you weren't expecting.
- The display name looks right, but the email address doesn't match it.

So, the rule to teach your team is simple: when it is about money, logins, or how you pay someone, slow down before you act.

How to protect your team

- If an email asks you to pay a new account or change a supplier's bank details, call the person on a number you already have.
- Make one rule for payment changes: confirm every change to bank details by phone, even when it's urgent.
- Turn on phishing-resistant MFA or passkeys, so a stolen password is harder to use even if someone gets tricked.
- Make it easy to report a suspicious email and make sure nobody feels silly for checking.
- Remind the team now and then that scam emails look perfect these days. A quick five-minute chat beats a poster nobody reads.

■ Why You Should Scroll Past The First Result On Google

When you search for a program to download or a site to log in to, the first thing you see is usually an ad. Scammers buy those ads on trusted names, so their fake site sits above the real one.

- Scroll past the sponsored results.
- Never download software from an ad. Type the maker's address yourself.
- Bookmark the sites you often log into.
- Check the web address before you type a password into anything.
- Keep browsers and devices

updated, so a bad download is less likely to work.

- Tell your team top results can be a trap. Most have never been warned.
- If someone clicked a bad link, change the password and have the device checked.

■ What To Do When Microsoft 365 Goes Down

In July 2024, a faulty software update crashed around 8.5 million Windows computers in a few hours. It wasn't an attack, just a bad update. When a service you depend on goes down, there's nothing for you to fix. These five steps keep you working while you wait.

1. Check whether it's just you.

Look at the provider's status page or ask whether anyone else has the same problem. If it's a wider outage, there's nothing to fix on your end.

2. Tell your team what's down and what to use instead. Otherwise, someone spends an hour rebooting a laptop that was never the problem.
3. Switch to your backup way to communicate. Move to phone, text, or another app so the team can still coordinate and reach customers.
4. Tell customers if it affects them. If you can't take bookings or payments, say so and tell them when to try again.

A few things that make outages hurt less

- Keep key files available offline. With OneDrive or SharePoint, recent files can sync to the device so you can still open them when the service is down.
- Have a backup way to get online. A mobile hotspot from a phone can get a few key people working again if your main internet drops.
- Know your status pages. It's the fastest way to tell whether the problem is them or you.
- Keep contacts off the cloud. Have your important phone numbers and contacts somewhere that doesn't need the internet.

