Sussex IT Firm Says Email Scams Are Costing Wisconsin Small Businesses More Than Ransomware

Powerful IT Systems founder: the attacks are hitting every kind of business, not just the obvious targets

Sussex, WI - April 16, 2026 - Ransomware gets the headlines. But Nazar Loshniv, founder of Sussex-based Powerful IT Systems, says the cyberattacks actually draining money out of Wisconsin small businesses are almost all email scams, and they're hitting industries nobody used to worry about.

"When I get a call about real money being lost, it's almost never ransomware. It's an email," Loshniv said. His firm provides managed IT and cybersecurity services to small businesses across the Milwaukee metro and Southeast Wisconsin.

The category is called Business Email Compromise, or BEC. The FBI has been calling it the most expensive cybercrime in the country for years now, and Loshniv said what he's seeing in Wisconsin tracks with that.

What's changed, he said, is who's getting hit. A few years ago the targets were predictable: law firms, medical offices, anyone who moved big money around. Now it's coffee shops. Landscaping companies. Mortgage offices. Nonprofits. Contractors. "I had a client recently who never thought of themselves as a target. Twenty employees, nothing flashy. Lost a wire to a fake vendor email. The money was gone in two hours."

He described four versions of the attack he keeps running into:

Fake vendor invoice swaps. Someone gets into a vendor's email, watches a thread for a few weeks, then jumps in at the right moment to ask for a banking change. The wire goes to the attacker. Loshniv said this is probably the most common one he sees, and the hardest to spot, because the email thread is real.

Owner impersonation. A bookkeeper gets an urgent email that looks like it's from the boss. Wire this, buy gift cards, do it before end of day. "The whole thing is built around urgency. If somebody's rushing you, that's the moment to slow down."

Account takeover. This is the one Loshniv said scares him the most. The attacker doesn't spoof an employee, they actually get into the real inbox through a stolen password. Every email they send is technically legitimate. "Your spam filter has nothing to flag. The email is coming from your coworker. Because it is."

Payroll diversion. HR gets a polite note that looks like it's from an employee, asking to change direct deposit info. Next paycheck lands in the attacker's account. The employee usually doesn't find out until they check their bank.

Loshniv said the frustrating part is that most of these attacks succeed because of process gaps, not security gaps. Most of the businesses he works with already have decent tools in place. What they don't have is rules.

"If your bookkeeper can change a vendor's banking info off an email, you're one bad day away from a problem. Doesn't matter what firewall you have."

His advice for Wisconsin businesses that want to actually reduce their risk:

- Pick up the phone. Any change to banking, wire, or payroll info should require a voice confirmation to a phone number you already had on file. Not the number in the email.
- Turn on multi-factor authentication. Specifically on Microsoft 365 and Google Workspace accounts. This is free and stops most account takeovers.
- Talk to your team about urgency. The single biggest tell on a BEC email is that it's pushing you to move fast. Train people to slow down when something feels rushed.
- Check email forwarding rules every few months. After attackers get into an inbox, they usually set up hidden forwarding rules to cover their tracks. Most people never look.

"None of this costs money. It just takes somebody actually sitting down with their team and having the conversation. And in my experience, most small businesses haven't."

About Powerful IT Systems

Powerful IT Systems is a managed IT and cybersecurity provider based in Sussex, Wisconsin. The company works with small and midsized businesses across the Milwaukee metro and Southeast Wisconsin.

Media Contact: Nazar Loshniv Founder, Powerful IT Systems
nazar@powerfulitsystems.net