ADVERSARY-IN-THE-MIDDLE ATTACKS: HOW PHISHING SITES STEAL YOUR ACTIVE LOGIN

You click a link, sign in, approve the MFA prompt, and get on with your day, completely unaware that someone else just logged into your account at the same moment.

That scenario surprises many businesses, particularly those that rely on multi-factor authentication (MFA) to protect cloud accounts. But this is exactly how Adversary-in-the-Middle (AiTM) phishing attacks work.
Rather than stealing passwords for later use, these attacks silently hijack an already-authenticated session in real time.

MFA remains a core control, and getting it implemented correctly is still a critical first step for any business.

But AiTM attacks exploit something MFA was never designed to protect: the trusted session that exists after authentication has already completed.

How AiTM Attacks Actually Work

An AiTM phishing site is not a basic replica of a login page. It is a live reverse proxy. The attacker's infrastructure sits between the user and the real authentication service. Every keystroke, redirect, and server response flow through the attacker's system in real time. From the user's perspective, nothing looks wrong.

The page behaves exactly like the real service, with correct branding, working redirects, and a functioning MFA prompt. In most cases, the only clue is a slightly altered URL that goes unnoticed on a mobile screen or when someone is under time pressure.

Session cookies

Session tokens act as bearer credentials. So, whoever possesses the token can access the account, with no password or MFA challenge required.

Once the cookie is stolen, the attacker imports it into their browser and immediately resumes the session. The attacker does not need to log in. They pick up where the legitimate user left off, inside a fully trusted, already-verified session.

What Happens After a Session is Stolen

The aftermath of an AiTM attack tends to be quiet, which is what makes it dangerous.

The attacker is operating inside a legitimate, authenticated session. There are no failed MFA attempts, no unusual login alerts, and nothing in standard sign-in logs to signal a problem.

Research from Proofpoint shows that attackers who gain access through session hijacking commonly create hidden inbox rules to redirect mail, register additional MFA methods to lock in persistent access, monitor email threads for financial conversations, and use the trusted account to launch phishing campaigns against internal colleagues or finance teams.

These follow-on actions are a key reason AiTM attacks are frequently uncovered late, after financial fraud, data exposure, or wider network compromise has already begun.

Stop Protecting Just the Login Screen

Want to review your identity security controls?

Contact us or schedule a consultation to identify the gaps that matter most before an incident does it for you.

HOW "JUST-IN-TIME" ELEVATION HELPS YOUR TEAM HAVE THE SYSTEM CONTROLS THEY NEED

Local administrator rights (the ability to install software, modify system settings, and override security controls) are given to end users far more often than they should. The usual reason is efficiency.

But the practical effect of this often is the opposite: machines that drift from baseline, infections that spread before they are caught, and remediation tickets nobody planned for.

Revoking local admin rights directly removes the root cause of most of those issues.

But I Need to Install Things

The concern about restrictions is legitimate. Users on your network occasionally do need elevated access for specific tasks.

The answer is not to restore permanent admin rights. It is just-in- time (JIT) elevation, where you get temporary elevated access for a defined task. The request is approved through an automated policy or by IT, and the elevation expires automatically once the task is complete.

This keeps users productive and IT informed.

Every elevation request is logged. Unapproved actions do not happen silently. The volume and pattern of requests also become useful data in its own right, revealing exactly which tasks genuinely require escalation and which ones users were performing only because nothing was stopping them.

What Standard Users Can Already Do

Standard accounts support normal application use, browser activity, printing, file access, and the vast majority of day-to-day tasks without any escalation at all.

The friction you may anticipate is usually larger than the friction you actually experience once the change is made and a robust JIT process handles the edge cases.

PROTECTING ACCOUNTS PAYABLE FROM AI FRAUD

Use these tips to strengthen your Accounts Payable (AP) defenses against sophisticated impersonation attacks.

1.Implement Out-of-Band Verification:
Always confirm requests to change bank details or approve urgent payments through a secondary, independent channel.

2.Don't Rely on "The Look":
Assume that a convincing appearance alone is no longer proof of a legitimate request.

3.Be Wary of Voice Cloning:
Require secondary verification for any verbal payment approval.

4.Standardize Verification Habits:
Create a culture where staff feel safe pausing high-risk actions to verify details.

5.Use Layered Access Controls:
Enforce MFA and restrict access to financial systems.

THE PASSKEY MIGRATION CHECKLIST

Transitioning to a passwordless environment doesn't have to happen overnight. Use this checklist to guide your team through a secure and efficient passkey migration.

• Audit Your Platform Support:
Identify which of your current tools already support passkeys natively.
• Prioritize High-Risk Users:
Begin your rollout with administrators and power users.
• Implement a Parallel Authentication Phase:
Allow users to authenticate with passkeys on enrolled devices while keeping passwords as fallback.
• Bridge Gaps with Password Managers:
For tools that do not yet support passkeys, utilize a password manager.
• Establish Recovery & Sync Protocols:
Ensure users understand how passkeys sync across their ecosystem (such as iCloud Keychain or Google Password Manager).

ATTITUDE CHRONICLE

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

Ontario Manufacturers Industry Insights Three essential reads: Cybersecurity · AI & Automation · Cyber Insurance

THE REAL ENTRY POINT

Most cyberattacks do not start with a sophisticated intrusion. They start with a click on a personal email, a reused password, or a file uploaded to a familiar cloud service because the approved option felt slower.

The Verizon DBIR found that **68% of breaches involve the human element** — not a zero-day exploit, but ordinary human behaviour on an ordinary working day.

> *"The risk doesn't disappear. It moves somewhere harder to see."*

For Ontario manufacturers running cloud-based workflows across multiple devices, the personal and professional overlap is now the rule.

PERSONAL HABITS & EXPOSURE

Personal inboxes and social media are where phishing thrives — harder to filter, easier to spoof, and loaded with emotional triggers. When those channels share a device with business systems, a single click crosses the boundary instantly.

CREDENTIAL STUFFING

When a personal account is breached, attackers automatically test those credentials against business systems.

Unique passwords + MFA break the chain.

WHY BLOCKING DOESN'T WORK

Blanket restrictions rarely stop risky behaviour — they relocate it. Users find workarounds. Unapproved tools move to personal devices. IT loses visibility into exactly what it was trying to manage.

The goal is managing the overlap without breaking how people work.

WHAT ACTUALLY REDUCES RISK

- **Separate contexts, not people.**
  Separate browser profiles, clear guidance on where business accounts should be accessed, and identity boundaries reduce exposure without restricting personal time.
- **Design for credential failure.**
  Enable MFA. CISA reports it makes accounts 99% less likely to be compromised — even when the password has already been stolen.
- **Make secure behaviour easier.**
  If the approved tool is harder than the workaround, people will use the workaround. Reducing friction is one of the highest-leverage investments you can make.

QUICK CHECKLIST

- ✓ Enable MFA on all accounts
- ✓ Use a password manager
- ✓ Separate work & personal browsers
- ✓ Train staff on phishing awareness
- ✓ Review device policies annually

THE COST OF A BREACH

Manufacturing is the **#1 targeted sector** for cyberattacks three years running. The IBM 2024 report puts the average breach cost at **$4.88M USD**.

$4.88M average cost of a data breach
21 days avg. downtime after ransomware
$1.5M+ avg. ransom for mid-market firms
$100K max PIPEDA fine per violation

OT/IT CONVERGENCE RISK

PLCs, SCADA systems, and CNC machines are now connected to IT networks. A phishing click in the office can stop a production line on the floor.

> *"A phishing click in the office can stop a production line on the floor."*

OT QUICK WINS

- ✓ Segment OT from corporate IT
- ✓ Require MFA for OT remote login
- ✓ Map all OT devices on network
- ✓ Audit vendor access quarterly

CYBERSECURITY — CONTINUED

SECURITY CULTURE

Annual training alone doesn't change behaviour. In manufacturing, operators are focused on throughput — a suspicious email isn't top of mind when a line is behind. What works:

- **Short, frequent toolbox talks.** Five-minute cyber touchpoints beat annual two-hour sessions every time.
- **Simulated phishing with feedback.** Immediate, non-punitive coaching after a click improves retention significantly.
- **No-blame reporting culture.** If people fear punishment for mistakes, they won't report incidents.

5-STEP ROADMAP

1. **Know What You Have** Inventory every device, OT system, cloud service, and vendor portal.
2. **Secure Your Identities** MFA + unique passwords. Remove unused credentials.
3. **Train for Reality** Short, role-specific training. Easy incident reporting.
4. **Segment & Contain** Separate OT from IT. Limit access between systems.
5. **Plan for When, Not If** Document your incident response plan. Test backups. Know your PIPEDA obligations.

REAL-WORLD SCENARIOS

Phishing stopped a line

An employee clicked a link on their personal phone. By morning, attackers had reached the SCADA system — output halted 18 hours.

Reused password, vendor access

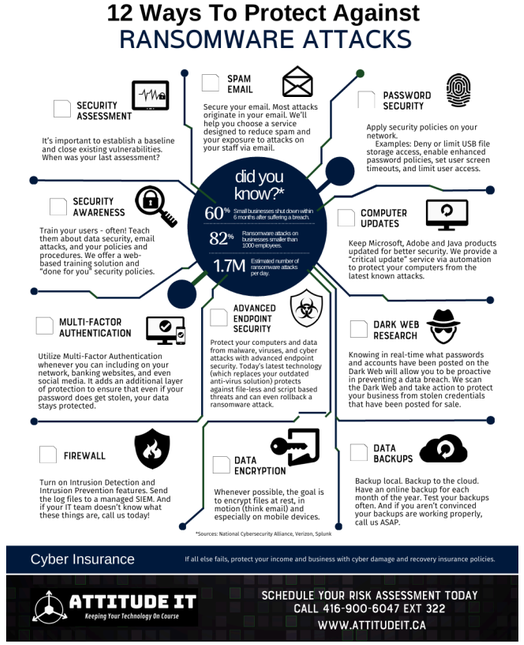
A maintenance tech reused a password across a gaming site and a vendor portal. When the gaming platform was breached, attackers accessed the plant network.

"In each case, the entry point was human — not a technical flaw."

68% of breaches involve the human element

99% less likely compromised with MFA

#1 Phishing — top attacker entry point



02 AI & Automation on the Shop Floor

76% manufacturers plan to adopt AI by 2027

22% productivity gain from automation

#1 Labour shortage: top automation driver

BEYOND THE HYPE

The most impactful automation for Ontario manufacturers isn't the flashy stuff. It's practical, proven, and increasingly affordable — driven by labour shortages, falling hardware costs, and accessible cloud AI tools.

WHERE TO START

1. **Predictive maintenance** Sensors on critical equipment detect failure patterns before breakdown. ROI typically within 12–18 months.
2. **Vision inspection** Machine vision inspects at line speed. Defect rates drop; inspection labour shifts to higher-value roles.
3. **Scheduling AI** Optimizes scheduling based on machine availability, order priority, and material status — reducing changeover time.

GENERATIVE AI APPLICATIONS

- **Maintenance documentation.** AI drafts and updates SOPs and maintenance procedures — saving engineers hours per week.
- **Technical troubleshooting.** Operators describe a symptom; AI provides structured diagnostic guidance from equipment manuals and maintenance history.
- **Procurement analysis.** AI reviews supplier quotes, flags anomalies, and summarizes contract terms faster than manual review.

"Generative AI won't run your machines — but it will save your engineers hours every week."

DATA SECURITY NOTE

Never input into AI tools:
× Customer names or contracts
× Proprietary process parameters
× Employee personal information
Use enterprise AI with data privacy commitments.

HOW TO BEGIN — 5 STEPS

1. **Find your pain point** Don't ask 'where can we use AI?' Ask 'what is our most expensive problem?'
2. **Assess data readiness** Most AI needs data. Do you have sensors, ERP data, quality records?
3. **Pilot before scaling** One application, one area, clear metrics.
4. **Choose manufacturing vendors** Domain expertise matters more than tech credentials.
5. **Plan for your people** Training and communication determine success.

WHY PROJECTS FAIL

Automation investments underperform for predictable reasons. Understanding them before you start is more valuable than any technology selection guide:

- **Automating a broken process.** Automation amplifies whatever is already there — including inefficiency. Fix the process first, then automate it.
- **Underestimating integration complexity.** Connecting a new system to your ERP, MES, or legacy equipment is almost always harder than the vendor demo suggests. Budget time and expertise for it.
- **Skipping operator training.** The people closest to the process need to understand, trust, and own the new system. Without their buy-in, utilization stays low and ROI disappears.
- **Choosing on price alone.** A vendor without manufacturing domain expertise will deliver a technically functional system that doesn't fit how your operation actually runs.
- **No defined success metrics.** If you can't measure it before and after, you can't prove it worked — and you can't improve it.

"Start with the pain point, not the technology."

FUNDING RESOURCES FOR ONTARIO MA

NRC IRAP — direct funding & advisory for AI/automation projects at Canadian SMEs
AMTEC / CME Ontario — automation readiness assessments & advisory programs
Ontario Centres of Excellence — R&D partnership and co-investment programs
SDTC & NRC CHAI — clean tech and advanced manufacturing grants

AUTOMATION & YOUR WORKFORCE

The most common objection to automation is job loss. The data tells a more nuanced story: automation changes jobs far more often than it eliminates them.

In manufacturing, the most common outcome is redeployment. Workers move from physically demanding, repetitive tasks — material handling, manual inspection, basic assembly — to roles that require judgment, problem-solving, and technical skill. These roles typically pay more and carry less physical risk.

"Automation is no longer just a cost strategy — it's a capacity strategy."

The labour shortage makes this reframing even more important. When you cannot hire the people needed to run a second shift, automation enables additional output without additional headcount. When experienced machinists retire, automated systems can encode and preserve their process knowledge.

COMMUNICATING THE CHANGE

Manufacturers who handle automation rollouts well share one habit: they involve their workforce early. Not to seek permission, but to build understanding. The people closest to the process often identify implementation risks that leadership misses entirely.

WORKFORCE TRANSITION CHECKLIST

- ✓ Communicate the project before it starts
- ✓ Involve operators in process design
- ✓ Define new roles before go-live
- ✓ Provide hands-on training time
- ✓ Create a feedback loop post-launch
- ✓ Recognise early adopters publicly

The manufacturers most competitive in five years are investing in automation today — not to replace their workforce, but to do more with it.

TECHNOLOGY TRIVIA TIME

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:

What video game was inspired by a pizza with one slice missing?

The first person to email me at emma@attitudeit.ca with the correct answer gets a $50 Amazon Gift Card!

Last month's answer was ***Radar***