the adversary intercepts the session cookie and can use it to authenticate to the web service as the user, even if the user changes their password, gaining access to the user's mailbox and other sensitive data, leading to business email compromise (BEC) and other attacks.

Once inside your email account, attackers typically work fast. They'll scan your inbox and sent items to understand your business relationships, ongoing projects, and payment processes. They're looking for invoices, wire transfer instructions, and conversations about money. Many will set up email forwarding rules to silently copy future emails to themselves, extending their access even after the stolen session expires.

Business email compromise is often the next step. Attackers might impersonate you to request urgent wire transfers, change payment details with vendors, or trick employees into sharing sensitive information. Because the emails come from your actual account—not a spoofed address, they're incredibly convincing.

Some attackers also use compromised accounts to move laterally through your organization. They'll access shared documents, cloud storage, and internal systems. If your email account has admin privileges or access to other business applications, those become targets too.

Why Traditional Defenses Miss This Attack

The reason session hijacking is so effective is that it bypasses the security measures most businesses rely on. You had a strong password—didn't matter. You used MFA—still got compromised. Even changing your password after the attack won't kick the attacker out, because they're using your session cookie, not your credentials

Traditional security tools often miss this activity because, from the system's perspective, it looks like you're legitimately logged in. The attacker is using valid authentication tokens, so there's no failed login attempt to trigger an alert. They're accessing your account from a different location or device, but many businesses don't have monitoring in place to catch those anomalies.

Protecting Your Business Beyond the Login Screen

The good news is that session hijacking can be detected and prevented with the right approach.

Modern security tools can monitor for suspicious session behavior—like a user suddenly accessing their account from two different countries simultaneously, or unusual patterns of email forwarding and deletion.

This is why regularly monitoring your business email is important, auditing logs regularly to spot new location log ins, policy changes or odd patterns.

Session timeout policies matter more than you might think. Shorter session durations mean stolen cookies expire faster, limiting the attacker's window. Some advanced security solutions can also bind sessions to specific devices or network conditions, making stolen cookies useless when used from a different context.

How Can Employee Training help?

Employee training needs to evolve beyond "don't click suspicious links." Your team should know to verify the actual URL before entering credentials, watch for subtle signs that a login page might be fake, and report anything unusual immediately—even if they're not sure.

Who Monitors Your Business Email

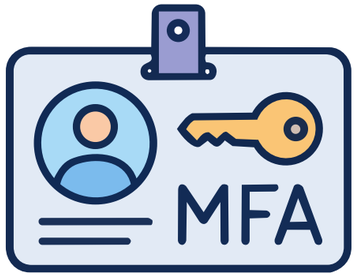
Regular security audits of email accounts can catch the telltale signs of compromise: unexpected forwarding rules, unfamiliar devices with active sessions, or access from unusual locations.

The sooner you catch these indicators, the less damage an attacker can do. having a live team monitoring and your business email can help.

Your team should be meeting with you regularly to stay on top of email vulnerabilities, improve staff training and suggestung regular improvements.

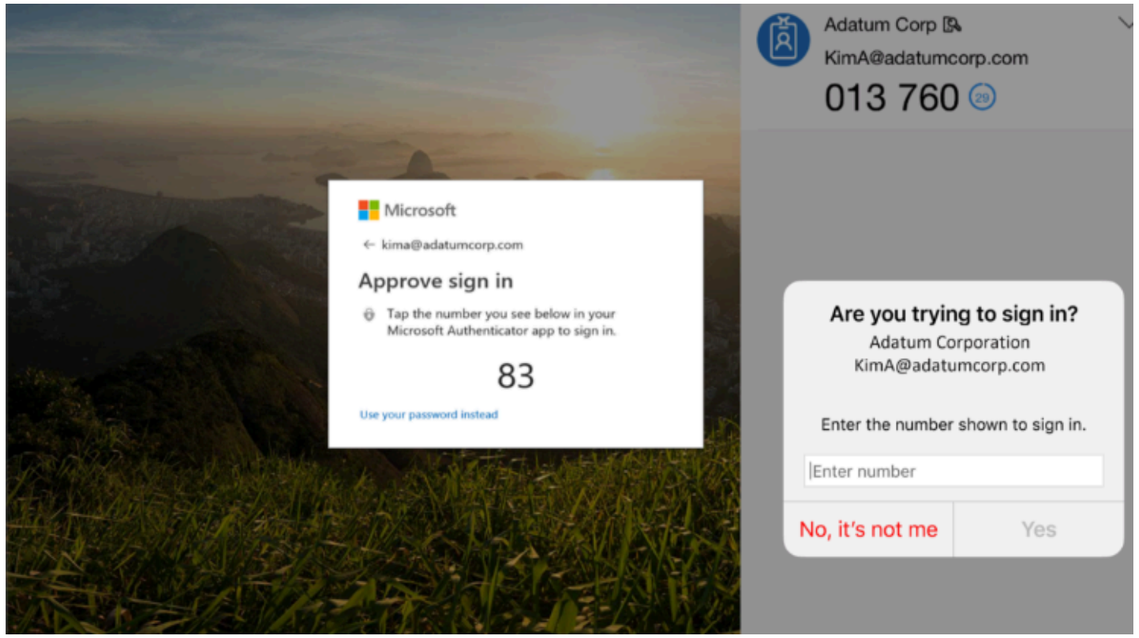
Getting Help With Modern Authentication Threats

Session hijacking and MFA bypass attacks represent a new generation of threats that require a new generation of defenses. If you'd like help assessing your current authentication security, implementing session monitoring, or training your team to recognize these sophisticated attacks, contact us. We help businesses like yours stay protected against threats that evolve faster than traditional security can keep up.



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

AFTER THE LOGIN: WHAT HAPPENS WHEN MFA GETS BYPASSED



Multi-factor authentication is supposed to be the lock on your digital front door. But what happens when an attacker finds a way around it—not by breaking the lock, but by walking in right behind someone who just unlocked it?

Session cookie hijacking lets attackers do exactly that, and the real damage begins after they're already inside your systems, moving through your business undetected.

How Attackers Steal the Keys After You've Already Unlocked the Door
The technique is called Adversary-in-the-Middle (AiTM), and it works like a digital pickpocket.

According to Cloudflare, these attacks involve "intercepting and relaying authentication requests and session cookies between the user and the legitimate service, allowing them to steal the session cookie after the user has successfully authenticated, including MFA, and then use that cookie to impersonate the user."

Think of a session cookie as a backstage pass your browser receives after you log in successfully. It tells the system "this person already proved who they are, let them through."

When an attacker steals that pass, they don't need your password or your phone for MFA—they just walk in as you.

The attack typically starts with a phishing email that looks legitimate. When you click the link, you're taken to a fake login page that looks identical to the real one. But here's the twist: when you enter your credentials and complete MFA, you're actually logging into the real service—the attacker's fake site is just sitting in the middle, passing everything through while copying your session cookie for themselves.

What Attackers Do Once They're Inside

This is where things get serious. The Microsoft Security Blog notes that "once a user enters their credentials and completes MFA.

NMA
NORTHUMBERLAND MANUFACTURERS' ASSOCIATION

ATTITUDE IT
Keeping Your Technology On Course

CYBERSECURITY IS THE NEW WORKPLACE SAFETY

9AM - NOON ● ***Wednesday, July 15*** ● ***Venture13, Cobourg***

For decades, manufacturers have built strong workplace safety cultures through training, awareness, procedures, and accountability. These efforts help prevent incidents, reduce risk, and keep operations running safely.

Cybersecurity threats can disrupt production, delay shipments, impact customers, and create significant business interruptions. **Just like workplace safety, cybersecurity is no longer the responsibility of one department—it's everyone's responsibility.**

Join us for an engaging and practical workshop that explores how manufacturers can apply proven health and safety principles to create a stronger culture of cyber safety across their organization.

What You'll Learn

- How cybersecurity has evolved over the past 15 years
- Why manufacturers are increasingly targeted by cyber criminals
- The similarities between workplace safety programs and cybersecurity programs
- How to recognize common cyber threats and scams
- What to do if you click on a suspicious email or link
- Why reporting cyber "near misses" is just as important as reporting safety near misses
- How to build an effective incident response plan
- Artificial Intelligence opportunities, risks, and workplace best practices
- Steps every department can take to help reduce risk

Key Takeaway
A strong safety culture doesn't happen by accident. Neither does a strong cybersecurity culture.

Who Should Attend?
This workshop is designed for all manufacturing employees, including:
Leadership and management ● Operations and production teams ● Health and safety professionals
Human resources ● Finance and administration ● Customer service and sales
Information technology staff

We encourage manufacturers to send employees from multiple departments to gain a shared understanding of today's cyber risks and how to respond effectively as a team.

$30+HST per trainee
Register at www.thenma.ca

HOME OFFICE SECURITY DEFAULTS EVERY REMOTE WORKER NEEDS

Working from home has blurred the line between personal and professional space, but your security posture shouldn't blur with it. Whether you're in a dedicated home office or working from the kitchen table, establishing baseline security defaults protects both your company's data and your own peace of mind.

Core defaults to implement immediately

- Lock your computer screen every time you step away—even for 30 seconds to grab coffee or answer the door
- Set your computer to auto-lock after 5 minutes of inactivity as a backup to manual locking
- Store all physical documents with sensitive information in a locked drawer or filing cabinet when not actively in use
- Remove sticky notes containing passwords, Wi-Fi credentials, or access codes from your monitor and desk area
- Position your monitor so it's not visible through windows or to anyone passing by your workspace
- Clear your desk of client files, financial records, and proprietary documents at the end of each workday
- Use a privacy screen filter if you work in shared living spaces or areas with foot traffic
- Shred sensitive documents rather than tossing them in household trash or recycling
- Keep work devices physically separate from personal devices and family members' access
- Establish a dedicated charging station for work devices that's out of reach of children, guests, or household visitors

Canadian Government Get Cyber Safe website: www.getcybersafe.gc.ca

emphasizes that you should "ensure that sensitive information is not left unattended or visible to unauthorized individuals.

This includes physical documents, sticky notes with passwords, and information displayed on computer screens." The same principle applies whether unauthorized individuals are external threats or simply family members who shouldn't have access to confidential business information.

These defaults aren't about distrusting your household—they're about building habits that protect you regardless of circumstance. A locked screen prevents your curious teenager from accidentally seeing employee salary data. A clear desk means the plumber who's fixing your sink doesn't glimpse client contracts. Physical security measures create layers of protection that complement your digital safeguards.

The 4-Step Legacy IT Debt Audit Your Business Needs

Legacy systems and outdated technology create hidden costs that drain your budget and slow your business down. If you're running software that hasn't been updated in years, relying on hardware past its prime, or patching together workarounds to keep things running, you're carrying technical debt.

Here's how to conduct a practical audit of your legacy IT systems.

- **Inventory Your Current IT Assets.** Start by creating a complete list of every system, application, and piece of hardware your business uses. Include the age of each asset, its current version, the vendor's support status, and who depends on it daily. This isn't just about servers and computers—document your software licenses, cloud subscriptions, and any custom applications built years ago that still run critical processes.

- **Assess Business Impact and Risk.** For each item in your inventory, evaluate how it affects your operations. Ask: What happens if this system fails tomorrow? Does it handle sensitive customer data? Is it connected to other critical systems? CIO.com emphasizes that "assessing the impact of technical debt on business operations" and "prioritizing remediation efforts based on risk and value" are essential steps in managing technical debt effectively. Systems that pose security risks or could halt business operations should rise to the top of your priority list.

- **Calculate the True Cost of Keeping It.** Legacy systems cost more than their maintenance contracts. Factor in the staff time spent on workarounds, the productivity lost to slow performance, the security vulnerabilities that put you at risk, and the opportunities you're missing because your systems can't support new capabilities. Compare these ongoing costs against the investment required to modernize or replace the system.

- **Create a Prioritized Remediation Roadmap.** Based on your risk assessment and cost analysis, build a realistic plan for addressing your technical debt. Some systems may need immediate replacement, while others can be phased out gradually. Budget for both quick wins that deliver immediate value and longer-term projects that address foundational issues. Set clear timelines, assign ownership, and establish metrics to track your progress.