AUG 2025

McLaren Strategic Solutions

Newsletter

Beyond the Office: Securing Hybrid Work

Introduction

The pandemic didn't just change where we work, it rewired how we're targeted. Hybrid is the new normal, and attackers know it. They've shifted from hardened office networks to our living rooms, latching onto weak home WiFi, personal devices, and café hotspots. One reused password, one tap on a fake MFA prompt, one free wifi login – that's all it takes.

The attack surface has expanded beyond the office and now spans home networks, personal and company devices, cloud logins, and the public networks we use while traveling. The human element is involved in about two thirds of breaches, and the average breach now costs millions. Will you be the next victim, or the person who prevents the headline by locking down the basics wherever you work?

Here are a few real incidents that make the point clear.

Weak home network becomes the back door

An engineer working from home never changed the ISP router's admin password and hadn't updated firmware in years.

Attackers scanning the internet logged in remotely, hijacked DNS, and invisibly redirected the engineer to look-alike login pages for email and VPN. The credentials, and later MFA approvals, fell right into their hands. The campaign quietly targeted SOHO routers for nearly two years, proving how living room hardware can redraw a company's perimeter. This was the ZuoRAT campaign disclosed in June 2022 (North America and Europe).

Device theft on public transport

On a weekday evening commute, a healthcare worker's backpack disappeared between two stops. The company laptop inside was password protected but not encrypted

Within hours, the thief removed the drive and browsed cached documents and a local mail archive. The organization had to notify patients because protected health information was likely exposed. If full disk encryption and mobile device management had been enforced, a stolen chassis would have been an inconvenience, not a breach. This incident was reported by TimeDoc Health in March 2024.

No MFA turns one old password into a breach

Credentials stolen from home and contractor laptops by info-stealer malware were reused to access Snowflake customer accounts that did not require MFA.

Because these were password-only SaaS logins, attackers could authenticate from anywhere and immediately begin bulk exports. Investigators said about 165 organizations were notified as potentially affected. This hit Snowflake customers in April to June 2024 (global).

Public WiFi “evil twin” harvests logins

Travelers and café goers saw a familiar free network name pop up and connected without a second thought. In reality, a nearby attacker had set up a spoofed hotspot, an “evil twin,” to capture traffic and credentials from anyone who joined.

Police later alleged the operator used the fake WiFi in public places, including on flights, to steal personal data from unsuspecting victims. A VPN and turning off auto-join would have ruined the con. This was an Australian Federal Police case in 2024 (Western Australia).

Why this matters right now?

These incidents are happening every day, and most of us never hear about them. If we do not follow secure remote work practices, we are never far from a breach. So what exactly counts as “secure remote work,” and how do we keep our network, devices, and data safe?

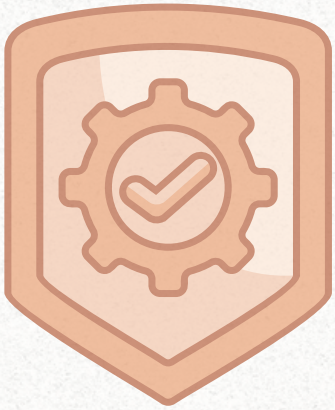
Start with the data

Everything comes back to one thing: the data - its criticality, where it lives, and who can touch it. Organizations should classify data, identify where highly sensitive information is stored (cloud apps, laptops, shared drives, backups), and make sure only authorized people and devices can access it. That means least-privilege access, strong authentication, encryption at rest and in transit, and monitoring that actually alerts when something unusual happens.

The CIA triad, applied to remote work

Confidentiality means your data stays private. No unauthorized person or device should be able to read company or customer data. In remote settings, that looks like MFA everywhere, managed and encrypted devices, secure home routers, and avoiding password reuse or saving work passwords in personal browsers.

Integrity means your data cannot be altered without approval. For remote teams, that includes patching and EDR on endpoints, controlled change workflows, versioning in your cloud tools, and safeguards against malware that tampers with files or email rules.



Availability means authorized people can get the information they need when they need it. Practically, this requires resilient connectivity, reliable VPN or zero-trust access, tested backups and restores, and clear incident processes so downtime is short and controlled.

Secure Remote Working Practices

Accounts and access

Always turn on multi-factor authentication (MFA) for every work account. MFA means even if someone learns your password, they still can't get in without the second step (like a code, a prompt, or a security key). If you ever receive an MFA prompt you didn't trigger yourself, deny it and report it- that's a sign someone is trying to log in as you.

Use a password manager to create and remember long, unique passphrases; this avoids reusing the same password in multiple places.

Devices: use managed, keep them healthy

Work on a company-managed device whenever possible. Managed devices have full-disk encryption, approved antivirus/EDR, and automatic updates turned on - so if a laptop is lost, stolen, or infected, IT can remote-wipe or block access quickly. Set your device to auto-lock after 5 minutes and lock it every time you step away. Only install approved software and browser extensions; random tools can introduce malware or data leaks. Don't let family or friends use your work device - accidental actions can still put company data at risk.

Home network hygiene

Your home Wi-Fi is part of the security perimeter now. Make sure it uses WPA2 or WPA3 encryption and change the router's admin password (this is different from the Wi-Fi password). Check for and apply router firmware updates, and turn off features attackers abuse, like WPS, UPnP, and remote administration. Put smart home and visitor devices on a guest network so they're isolated from your work laptop. When you're away from home or whenever the network isn't fully trusted, use the company VPN / Zero-Trust model and, if available, set it to auto-connect.

Public Wi-Fi and travel

Public Wi-Fi is convenient but risky because fake or insecure hotspots are common. The safest option is your phone's personal hotspot; if you must use public Wi-Fi, connect the VPN before opening work apps, and disable auto-join for open networks so your device doesn't connect by itself. Captive portals sometimes offer "updates"- never install software from a Wi-Fi login page. Keep sensitive conversations and on-screen data to a minimum in public spaces, and be mindful of who might be watching or listening.

Handling company data

Treat company data like it's valuable - because it is. Create, store, and share files only in the approved cloud (e.g., [OneDrive/SharePoint/Google Drive]); that way, data is backed up, access-controlled, and recoverable if something goes wrong. Share links with least-privilege permissions (view-only by default, grant edit only when needed) and respect any data-loss prevention (DLP) prompts that appear. Whenever possible, use the web versions of apps—that keeps data in the secure cloud instead of downloading copies to your device.

Phishing and social engineering

Most attacks start with a message that looks routine. Be cautious with unexpected links or attachments - even if they come from someone you know, because their account could be compromised.

Verify the sender's email by expanding the full address and confirming the exact domain name, including subdomains and the top-level domain; watch for lookalike characters, added words, or a Reply To address that differs from the From address. If anything seems questionable, validate the request using a trusted phone number or corporate chat rather than replying to the message.

Do not sign in or open documents from links in email; instead, open a new tab or the official application, navigate to the service directly by typing the URL or using a trusted bookmark, and enter any reference or security code there.

Physical security at home and on the go

Choose a private space to work. Position your screen so shoulder-surfing isn't possible, and consider a privacy filter if you're near windows or in shared areas. Lock your screen whenever you step away, and never leave devices unattended in cars, cafés, or conference rooms. If you must transport your laptop, keep it out of sight and with you at all times.

Conclusion

At McLaren Strategic Solutions, secure remote work comes from pairing convenience with disciplined habits. Focus on strong access hygiene, well managed devices, trusted networks, careful handling of company data, and a healthy skepticism toward unexpected messages, links, and prompts. Small lapses can have large consequences, but consistent everyday precautions reduce risk across our people, processes, and technology. If something does not feel right, pause, verify through a trusted McLaren channel, and report it promptly to the Security team or the Helpdesk so we can respond quickly and keep our clients and colleagues protected.