CYBERSECURITY AND REMOTE WORK

Defending your digital workspace in the remote era

THIS MONTH'S TOPICS:

Hidden Workspace Threats
Spot Invisible Risks While Working Remotely

Home Office Physical Security
Protect Your Remote Workspace

Scam of the Month:
Fitness Scams

Is Public WiFi Ever Safe?
Think Twice Before You Connect

As remote and hybrid work continue to shape the way we do business, staying secure outside the office has never been more important. This month's newsletter explores the hidden risks that can arise in your home workspace, practical steps to strengthen physical security at home, and the truth about whether public Wi-Fi can ever be considered safe.

With simple best practices and smarter awareness, you can protect your data, no matter where you work. We'll also highlight common mistakes remote workers don't realize they're making and offer easy ways to stay secure without disrupting your daily routine.

HIDDEN WORKPLACE THREATS

Smart Devices Nearby

Threat: Always-listening tech can capture work conversations.
Impact: Sensitive info may be recorded or leaked.
Fix: Mute or unplug devices during meetings; update firmware.

Extensions and Apps

Threat: Extensions may track your activity or read data.
Impact: Logins and browser info can be harvested.
Fix: Remove unused add-ons and review permissions.

Auto-Connect Features

Threat: Devices join unsafe networks automatically.
Impact: Data becomes visible to nearby attackers.
Fix: Turn off auto-connect and manage network lists.

Background Clutter on Calls

Threat: Mail, notes, and personal items visible behind you.
Impact: Attackers gain data for targeted scams.
Fix: Use clean backgrounds or blur features.

Window Visibility

Threat: Screens visible from outside your home.
Impact: Anyone passing by could see confidential info.
Fix: Adjust your desk layout or use blinds/privacy screens.

Home Office
Physical Security

Strong physical security is an essential part of protecting work data at home. These key practices help prevent accidental exposure, unauthorized access, and the everyday risks that come with remote work.

🔒 Secure Your Devices

- Set strong, unique passwords or passcodes for all work devices.
- Enable auto-lock after short periods of inactivity.
- Lock your screen every time you step away — even for a moment.
- Avoid leaving laptops, tablets, or work phones in shared spaces like kitchens or living rooms.

🚪 Control Who Has Access

- Be mindful of home visitors such as cleaners, maintenance workers, or package delivery staff who may pass near your workspace.
- Avoid leaving work materials visible during visits.
- Keep doors closed when working in a dedicated office to limit access from children, pets, or guests.

📄 Protect Printed Materials

- Store sensitive documents in locked drawers or cabinets when not in use.
- Keep paperwork off shared surfaces where guests, family members, or roommates might see it.
- Shred anything you no longer need, especially documents with personal or business information.
- Use a dedicated inbox or file tray to prevent accidental mixing of personal and work materials.

🗂️ Organize Your Workspace Safely

- Keep only the essentials on your desk to reduce the chance of exposing sensitive documents.
- Regularly clean up stray papers, notes, or reminders that could contain confidential information.
- Use designated, secure storage for any removable media (USB drives, external hard drives, etc.).

SCAM OF THE MONTH: FITNESS SCAMS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Jordan was excited to see a new “Company Wellness Challenge” email inviting employees to join a step-tracking competition with prizes. The branding looked perfect, the website appeared professional, and the sign-up process felt familiar. Wanting to participate, Jordan created an account and entered personal details including his home address, birthday, and device syncing permissions, all of which seemed normal for a fitness app.

A few days later, a coworker mentioned receiving two versions of the challenge email. Jordan’s smartwatch had also begun glitching, raising red flags. After reporting it to IT, Jordan learned the fitness challenge was a carefully crafted scam designed to steal employee data and gain access to personal accounts. The experience became a reminder that even friendly, “healthy” opportunities can mask malicious intentions, and that verifying the source is always the safest first step.

DID YOU SPOT THE RED FLAGS?

- A legitimate wellness program wouldn’t require a home address, full date of birth, or direct access to a smartwatch just to track steps.
- Receiving duplicate versions of the same company email from different or unfamiliar addresses is a major warning sign of a scam.

HOW TO PROTECT YOURSELF

- Make sure the email is from your company and confirm with HR before clicking or sharing any information.
- If a program asks for sensitive details or device access, pause and confirm it’s legitimate.

Is Public WiFi Ever Safe?

Public Wi-Fi is everywhere — from airports and hotels to gyms, cafés, and conference centers. While it's convenient, it often comes with serious security risks. Use this **Do/Don't** guide to stay safe wherever you work or travel.

✅ DO

Do use a VPN when possible.
A Virtual Private Network encrypts your traffic, making it much harder for attackers to snoop or steal your information.

Do use your mobile hotspot when you can.
Your phone's cellular connection is significantly safer than most public Wi-Fi networks — especially for work or personal account access.

Do keep firewalls and antivirus tools active.
These tools help block suspicious traffic and detect risky behavior in real time.

🚫 DON'T

Don't log in to sensitive accounts.
Avoid accessing work portals, banking apps, email, and any site that requires a password. Attackers can easily intercept or capture login details on unsecured networks.

Don't assume the network is legitimate.
Cybercriminals often create fake "look-alike" hotspots (called evil twins) that mimic real network names to steal data from anyone who connects.

Don't leave file sharing or Bluetooth turned on.
These settings allow nearby devices to connect to or browse your files without your knowledge.