BREACH SECURE NOW

Newsletter: July 2025

WEARABLE TECH SECURITY

Uncovering the hidden risks of wearables and smart devices

THIS MONTH'S TOPICS:

Wearable Tech Security Risks

Are Your Wearables Spying On You?

Protect Yourself

Wearable Security Best Practices

Scam of the Month:

Malicious Browser Extensions

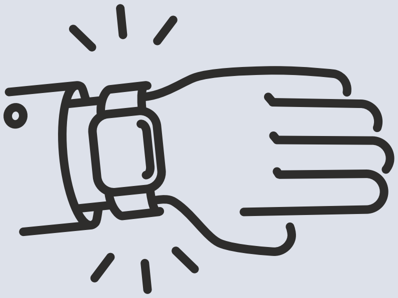
What The Future Holds

The Next Wave of Wearable Threats

As technology continues to shrink and blend into our daily lives, the devices we wear, carry, and even forget about are quietly collecting, transmitting, and storing vast amounts of data. From smartwatches and fitness trackers to smart rings and AR glasses, wearable technology is revolutionizing convenience, but it’s also introducing new and often overlooked cybersecurity risks.

In this newsletter, we’ll take a closer look at how these tiny devices impact security in a big way, both personally and professionally. Let’s dive into the unseen side of tech and learn how to protect what’s always on.

Wearable Tech Security Risks



1

ALWAYS CONNECTED = ALWAYS EXPOSED

Wearables often rely on Bluetooth, Wi-Fi, or cellular connections to sync with smartphones or cloud apps. If those connections aren't secured, cybercriminals can intercept data, spoof devices, or inject malware. Some devices even stay connected 24/7, making them attractive targets for attackers.

2

MORE DATA THAN YOU REALIZE

Wearables gather more than fitness metrics. They can track:

- Location and movement patterns
- Sleep habits and stress levels
- Audio or voice commands
- Health and biometric data
- App usage and behavioral trends

If stolen or leaked, this data could be used to re-identify individuals, profile behavior, or enable social engineering attacks.

3

WEAK DEFAULTS AND POOR UPDATES

Many wearables ship with default passwords, open ports, or insecure pairing modes. Worse, some lack routine security updates or rely on users to install firmware manually. Without automatic patching, vulnerabilities can linger.

4

THIRD-PARTY APP RISKS

Wearable ecosystems often include third-party apps that extend functionality. Think fitness challenges, health coaching, or sleep tracking integrations. But these apps can request overly broad permissions or transmit data to unknown servers, putting users and businesses at risk.

5

THE WORKPLACE THREAT

Employees wearing smart devices in secure areas can inadvertently record sensitive conversations, transmit location data during confidential meetings, and access work apps with minimal authentication. Without proper security awareness, wearable tech can become a quiet insider threat in the workplace.

WEARABLE SECURITY BEST PRACTICES

FOR INDIVIDUALS

Strengthen Your Settings

- Change default passwords and PINs immediately after setup
- Disable unused features, like GPS, Bluetooth, and voice assistants (when not needed)
- Review privacy settings and opt out of unnecessary data collection

Keep It Updated

- Enable automatic updates when available
- Regularly check for firmware updates and companion app patches
- If the device is no longer supported, consider retiring it

UPDATED

Be App-Savvy

- Download only from trusted sources (Apple App Store, Google Play, verified vendors)
- Audit app permissions, especially access to location, camera, microphone, and contacts
- Avoid connecting your wearable to multiple third-party services unnecessarily

FOR BUSINESSES

Update BYOD Policies

- Explicitly include wearable devices in Bring Your Own Device (BYOD) frameworks
- Outline acceptable usage in sensitive areas (e.g., data centers, meeting rooms)
- Require device registration if connecting to corporate WiFi or systems

Train Staff

- Educate employees on how wearables collect and transmit data
- Run simulations or quizzes to identify risky behaviors
- Emphasize that invisibility doesn’t mean harmlessness

Monitor and Audit

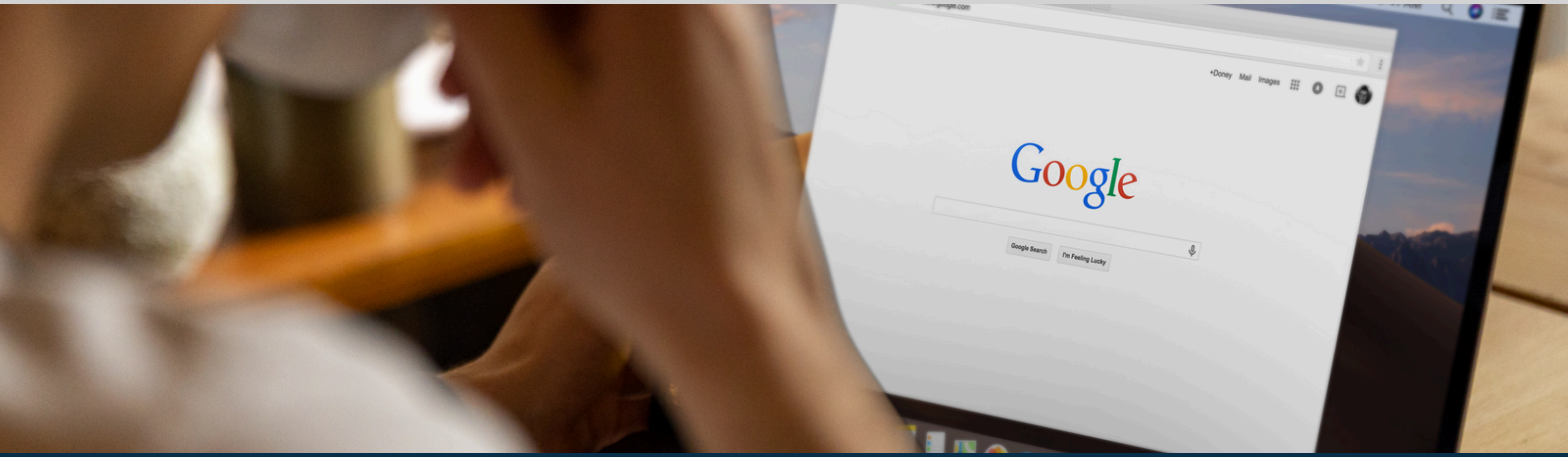
- Use endpoint monitoring tools that can detect unexpected device connections
- Require multi-factor authentication (MFA) for apps accessed via wearable tech
- Periodically review access logs and app integrations

SCAM OF THE MONTH: MALICIOUS BROWSER EXTENSIONS

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

Emma Liu, an Operations Coordinator, installed a Chrome extension called “QuickTab Pro” after reading a blog that claimed it could boost productivity with AI-powered reminders and tab management. The extension had thousands of users and solid reviews, so she didn’t hesitate to grant it full access to her browser data. However, the extension came from an unknown developer with no official website or company affiliation.

Within days, her company’s IT team detected unusual login attempts tied to her account. It turned out the extension was recently hijacked by attackers who updated its code to harvest login credentials, monitor activity, and redirect search traffic to phishing sites. Though no data was stolen, the company spent thousands of dollars investigating the breach, resetting credentials, and tightening browser extension policies.



DID YOU SPOT THE RED FLAGS?

- If an app requests full access, this is a red flag. Having full access means the app can view sensitive information that you type into the browser.
- Never download an extension that comes from an unknown developer and isn’t affiliated with any trusted companies or businesses.

STAY SAFE

HOW TO PROTECT YOURSELF

✓ Be cautious with extensions that ask for full access to your browsing activity or data on all sites. Consult your IT team if you’re unsure.

✓ Only install extensions from well-known developers or trusted companies. Before installing, look for an official website link.

THE NEXT WAVE OF WEARABLE THREATS

01

AR Glasses & Smart Lenses

Augmented reality (AR) glasses and smart contact lenses are poised to revolutionize how we work, communicate, and interact with data. But with built-in cameras, microphones, and location tracking, these devices could covertly capture confidential information in meetings, expose intellectual property, or create new vectors for surveillance and stalking.

02

Smart Clothing & Biometric Sensors

Smart apparel is gaining popularity in healthcare, athletics, and the workplace—monitoring movement, heart rate, posture, and even stress levels. However, this constant collection of biometric data raises serious privacy concerns. Improper storage, unsecured transmissions, or third-party data sharing could result in health data leaks or discrimination risks.

03

Brain-Computer Interfaces (BCIs)

Experimental brainwave-reading wearables are emerging for focus tracking, neurofeedback, and mental health applications. As promising as these sound, neural data is deeply personal, and the idea of it being intercepted or manipulated brings entirely new ethical and security challenges. Could future attackers steal thoughts—or influence attention?

04

Hyper-Connected Environments

Wearables will increasingly interact with smart home systems, workplace networks, vehicles, and public infrastructure. This expanded integration means a vulnerability in one device could ripple across environments—especially if IoT security standards remain inconsistent. Even a hacked smartwatch could trigger far-reaching consequences.

Staying Ahead of the Curve

To stay secure in the wearable future:

- Treat new devices as untrusted until properly vetted
- Limit data access to what's truly necessary
- Stay informed about evolving privacy regulations and industry standards for connected devices.
- Update policies regularly to account for emerging tech and use cases