CYBERSECURITY AWARENESS DAY 12

Let's talk about
Insider threat

Iwuchukwu Augusta Chioma

→

Insider Threats: The Danger Within

Not every cyber threat wears a hoodie. Sometimes, it’s someone already inside

Iwuchukwu Augusta Chioma

What Are Insider Threats?

An insider threat happens when someone with legitimate access an employee, contractor, or partner misuses it to harm the organization.

This can be:

- Malicious: intentionally stealing data or sabotaging systems.
- Negligent: accidental mistakes that expose sensitive information.

Think of it like someone leaving a door unlocked at home the intention may not be to steal, but danger enters anyway.

Iwuchukwu Augusta Chioma

Why Insider Threats Matter

A single insider mistake can lead to:

- **Data breaches** — exposure of sensitive information
- **Financial losses** — fines, theft, or operational downtime
- **Reputation damage** — loss of trust with clients or the public
- **Legal consequences** — regulatory penalties for mishandled data

Real-Life Example:

In 2020, a Tesla employee was approached by a Russian hacker offering $1M to install malware on Tesla’s network.The malware could have stolen sensitive data and disrupted operations.The employee reported the attempt, and the FBI intervened, stopping the attack.

Lesson:The employee’s choice to report the attempt instead of succumbing to temptation saved the company from potential financial, reputational, and operational damage.Integrity can prevent disasters before technology even detects a threat.

Iwuchukwu Augusta Chioma

Types of Insider Threats

- Malicious Insiders — intentionally steal or damage data
- Negligent Insiders — mistakes that expose systems (e.g., clicking phishing links)
- Compromised Insiders — accounts hijacked by external attackers

Even a single negligent or compromised insider can create far-reaching damage

Iwuchukwu Augusta Chioma

How Organizations Detect Insider Threats (Tech Tools Simplified)

- Microsoft Purview Insider Risk Management — flags unusual file movements or sensitive data access
- Microsoft Sentinel (SIEM) — monitors internal activity patterns for anomalies
- Microsoft Defender for Endpoint — alerts on suspicious device behavior
- Microsoft 365 Audit Logs — tracks file access and modifications

For non-techies: These tools act like digital security cameras and alarms for sensitive information.

Iwuchukwu Augusta Chioma

How to Prevent Insider Threats:

- Enforce least privilege access.
- Educate employees on phishing, data handling, and reporting suspicious activity.
- Monitor data movement and user behavior.
- Foster a culture of integrity and accountability.

The most dangerous threats often come from within but the most powerful defense is awareness, culture, and integrity.

Iwuchukwu Augusta Chioma

Share, like and follow for more Cybersecurity awareness tips

Iwuchukwu Augusta Chioma