The Hidden Threat: Unmanaged Devices and Unsafe Browsing

In today's fast-paced digital world, convenience often comes at a cost. Two common yet serious cybersecurity risks facing organizations are the use of unmanaged devices and browsing blocked or unsafe websites. Both can create hidden entry points for attackers, putting sensitive data, company systems, and reputations at risk.

⚠️ Unmanaged Devices: A Silent Security Hole

What are unmanaged devices?

These are laptops, phones, tablets, or personal computers that connect to the company's network but aren't monitored or controlled by the IT department.

Why are they dangerous?

🦠 No Security Updates: Unmanaged devices often lack the latest patches or antivirus software, leaving them open to malware and ransomware.

🔓 Data Exposure: Without encryption or secure storage policies, company data can be easily leaked or stolen.

🕵️Access Abuse: If an attacker gains access to an unmanaged device, they can use it as a backdoor into the corporate network.

Real-world impact:
Many major data breaches begin with an employee logging in from an unsecured personal laptop or mobile device. Even a single compromised endpoint can expose the entire company.

Best practices:
Only use company-approved and managed devices for work.
Enable multi-factor authentication (MFA).
Report any suspicious device activity immediately to IT.

🚫 Browsing Blocked or Unsafe Websites

Why companies block certain sites:

Blocked websites often host malware, phishing content, or inappropriate material that can harm the organization's network and reputation.

Risks of ignoring restrictions:

💀 Malware Downloads: Many blocked websites are designed to infect your system silently.

🧩 Phishing Attacks: Fake login pages can steal credentials, giving hackers full access to company systems.

📉 Policy Violations: Accessing restricted sites can lead to disciplinary action and loss of trust from your employer.

Remember: If a website is blocked, there's a reason. Circumventing restrictions using VPNs or proxies is not only unsafe, but also a direct violation of company policy.

✅ Stay Secure, Stay Smart

- Use only managed devices for any company work.
- Report security concerns or suspicious websites to the IT department immediately.
- Remember: cybersecurity isn't just IT's job; it's everyone's responsibility

Keep your BS (be skeptical) meter on, use the PAB when in doubt or forward any suspicious email to PAB@phl.org. Feel free to reach out to the InfoSec team at infosec@phl.org if anything happens or if you have any questions or concerns.

Protect the company. Protect yourself. Stay cyber aware.