Dark Web Dangers

The Dark Web is a segment of the Internet that can only be accessed using special tools that anonymize and hide the user's location and identity.

So one might ask, “If I’m not accessing the Dark Web, why do I need to worry about it?” The answer is simple: You don’t need to be on the Dark Web to be adversely affected by the practices being carried out there. Anyone who is online runs a risk of being compromised by activity originating in this hangout for criminals who are constantly looking for new ways to financially benefit by making you a victim of their self-serving plots.

Activities carried out on the Dark Web include…

- Pornography, especially illegal porn like child porn
- Money laundering and related services used by criminals to move money and obscure trails
- Terrorism and communications activities to support terrorist and other criminal activities
- **Phishing and fraud scam sites and services for hire**
- **Market places for stolen data and hacking tools and services**

Those last two items should be of interest to all of us.

Just some of the adverse outcomes we may experience if we become victims of underhanded activities originating on the Dark Web include…

- **Identity Theft** - Internal company information such as employee PII (Personally Identifiable Information), client PII, credit card info, banking info etc. Such breaches can lead to stolen bank accounts, fraudulent purchases, opening new bank accounts to get loans or credit cards, tax return collection by scammers, blackmail, propagation of malware to friends and coworkers, etc.
- **Reputation** - A breach can lead to mistrust and animosity in the marketplace for your company.
- **Cascading Breaches** - Access to one company may lead to access to other companies’ networks.
- **Trade Secret and Intellectual Property Theft** – These may ruin a company’s future.

How do we protect ourselves, our employees, our vendors, our clients, and our companies?

- Apply, check, and verify patches and updates regularly
- Employ strict password policies, including change intervals and complexity
- Use 2 factor authentication (2FA) for networks and systems
- Encrypt data *everywhere* (remember, a chain is only as strong as its weakest link)
- Actively monitor and analyze systems and services using current tools
- Train employees consistently
- Create and execute plans for breach prevention and remediation
- Use data breach attempt detection and Dark Web monitoring services

This may seem like a lot to figure out, but it’s really not. You simply need to have someone at the helm of your digital security efforts who understands how to seamlessly orchestrate these elements into your existing processes. That’s what we do. And we welcome the opportunity to discuss your company’s situation and needs without obligation on your part. We want you to be protected.

Contact us at **385.312.9030** or send us a message through our website at https://sanityworx.com and let’s start the conversation. *We look forward to hearing from you!*