Cybersecurity Tips from John Bandler

Learn about the threats and risks

We are all at risk for cybercrime – each person and organization. We need to learn about the threats, cybercrime, cybersecurity, and technology. We should think about our "cybersecurity dial" and where it should be, manage risk on a prioritized basis, and aim for continual improvement. Security, compliance, and efficiency *can* go together.

Improve your cybersecurity using Bandler's Four Pillars of Cybersecurity

1. Better security starts with improving everyone's **knowledge and awareness**. Untrained or unaware individuals can let a cybercriminal into the home or business, bypassing security measures. They are susceptible to "social engineering" (con artistry). Sending or receiving funds? Confirm all wiring instructions verbally!

2. Next is **device security**. This begins with physical security, keeping physical control of your smartphones, tablets, laptops, desktops, and servers. Good habits pay off. Ensure devices are configured to require a strong password (or thumbprint or other method) to gain access. Keep operating systems and applications updated (patched). For laptops and desktops, run regular malware scans. Review all security and privacy settings periodically and disable or uninstall software and services that you don't need.

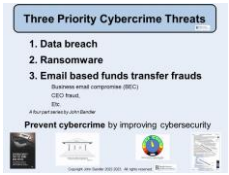
3. Then comes **data security**. Know what data you are storing, and where you are storing it. Consider the sensitivity of each type of data, and the potential consequences if it were stolen or if you lost access to it. Securely delete data you will never need. Backup and securely store important data. Secure email accounts and other important cloud data with strong passwords and two-factor authentication. Consider encryption for sensitive data.

4. Now comes **network and internet security**. Secure your home and office network, starting with the router. The router firmware (operating system) needs to be updated (patched) periodically. Don't use default usernames and passwords. Your Wi-Fi network should be encrypted and require a strong password to gain access. Disable unneeded services and avoid joining public Wi-Fi networks.

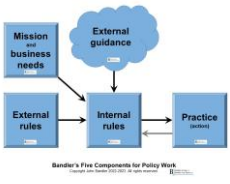
5. **Repeat!** Look for continual improvement. Even small steps can move you forward.

Organizations can follow all the above, and need a cybersecurity program, with a written policy. They need to do certain things to protect themselves, clients and customers, comply with legal obligations, and achieve the mission. I offer **cybersecurity services** for organizations.

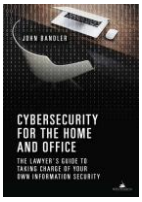
Additional free and valuable resources are on JohnBandler.com
Learn about my books, see short and longer articles, including:



- Three Priority Cybercrime Threats
  - Email Based Funds Transfer Frauds (BEC, CEO Fraud, etc.)
  - Ransomware
  - Data Breaches
- Bandler's Four Pillars of Cybersecurity
- Introduction to Cybersecurity
- Cybersecurity services
- Bandler's Five Components for Policy Work
- Policies, Procedures, and Governance of an Organization
- Cyberlaw
- This one-page tipsheet (check this link for the most current version)
- And many more, including through my reliable information jump-off page/



My books:



Cybersecurity for the Home and Office and *Cybercrime Investigations*

Contact me to discuss professional services.

John Bandler, Bandler Law Firm PLLC and Bandler Group LLC
48 Wall Street, 11th Floor, New York, NY 10005
John@JohnBandler.com johnbandler.com (929) 265-2775