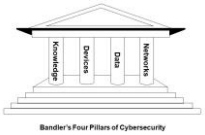
Cybersecurity Tips from John Bandler

Apply solid principles for risk and decision making

We need to learn, assess facts, weigh options, and make good decisions.

We are all at risk for cybercrime – each person and organization. We need to learn about threats, cybercrime, cybersecurity, and technology. Security, compliance, and efficiency *can* go together.

We should think about our Cybersecurity Dial and where it should be, manage risk on a prioritized basis, and aim for continual improvement.



We should apply Bandler's Four Pillars of Cybersecurity as outlined next.

Improve your cybersecurity using the Four Pillars of Cybersecurity.

1. Improve knowledge and awareness. This applies to you and others in your home or organization. Unaware individuals can let a cybercriminal into the home or business, bypassing security measures. They are susceptible to "social engineering" (con artistry). Learn the Three Priority Cybercrime Threats. If sending or receiving funds, confirm all wiring instructions verbally!

2. Protect and secure computer devices. 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) for 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. Protect and secure data. 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. Protect and secure networks and internet usage. 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.

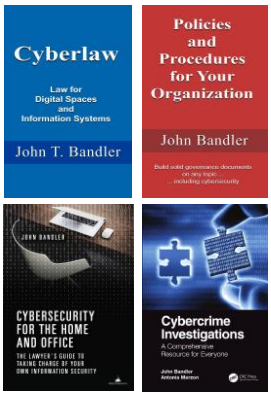
5. Repeat. Aim for continual improvement and know that small steps can move you forward.

This is just a start: See my website articles for more details, my books for even more.

Organizations can follow all the above, plus my Five Components for Policy Work. Build a cybersecurity program with a written policy. Protect the organization, employees, clients and customers, comply with legal obligations, and achieve the mission. See my cybersecurity services.

See my website JohnBandler.com for articles and about my books:

- Three Priority Cybercrime Threats
  - Email Based Funds Transfer Frauds (BEC, CEO Fraud, etc.)
  - Ransomware
  - Data Breaches
- Bandler's Four Pillars of Cybersecurity
- Bandler's Five Components for Policy Work
- Introduction to Cybersecurity
- Cybersecurity services
- This one-page tipsheet at johnbandler.com/cybersecurity-tips-from-john-bandler (check for a more current version)
- And many more resources, including through my reliable information jump-off page



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