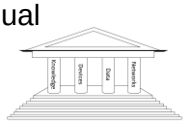
Cybersecurity Tips from John Bandler

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 "security dial" and where it should be, manage risk on a prioritized basis, and aim for continual improvement. Security and efficiency can go together.

Security dial



Improve your security using Bandler's Four Pillars of Cybersecurity

1. Better security starts with each individual's **knowledge and awareness**. Untrained or unaware individuals can essentially let a cybercriminal into the home or business, bypassing security measures. They are susceptible to "social engineering" (con artistry). Increased knowledge, awareness, and experience are what give us necessary common sense.
Sending or receiving funds? Confirm all wiring instructions by phone.

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 access them. 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.

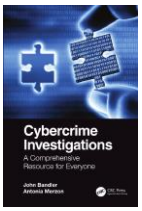
5. Continual vigilance and improvement is key. Organizations need policies and procedures.

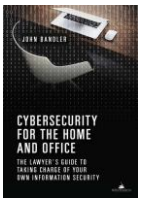
I offer additional free resources, because only so much can fit onto this single page.

From short articles to my two books, start by visiting my website at https://johnbandler.com/articles

Cybersecurity for the Home and Office*: The Lawyer's Guide to Taking Charge of Your Own Information Security*

Cybercrime Investigations*: A Comprehensive Resource for Everyone*





Articles include:

- *Policies, Procedures, and Governance of an Organization*
- *Cybersecurity, Privacy, You, and Your Organization*
- *Email Based Funds Transfer Frauds*
- *Ransomware*
- *Data Breaches*
- *New York Cybersecurity Requirements and the SHIELD Act*
- *Privacy, You, Your Organization, and the New NIST Privacy Framework*
- *Cybercrime and Fraud Prevention for Your Home, Office, and Clients*
- *Prepare for and Plan Against a Cyberattack*
- *Cybersecurity and Working from Home*

Organizations and individuals may need professional assistance. Contact me to discuss.

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