U.S. Department of Justice
Federal Bureau of Investigation
Office of Private Sector

CYBER AWARENESS

Cyber criminals perpetrate a variety of crimes online, including theft of intellectual property, internet fraud, and financial fraud schemes.

Employers and employees can protect themselves by using easy mitigation strategies. Many businesses have dramatically reduced the risk of credential theft and loss of proprietary data.

CYBER BEST PRACTICES

- Use two-factor authentication to increase security by incorporating login requirements with a password along with a token or PIN code
- Ensure your operating system and software are up to date
- Disable hidden file extensions
- Ignore unsolicited emails
- Cover or tape over webcam when not in use
- Use strong passwords
- Disable automatic logins
- Don't leave your computer on 24/7 - turn it off when you're not using it

Electronic Device Tips:

- Understand your Internet of Things (IoT) devices
- Protect your Wi-Fi networks
- Set up firewalls and use complex passwords
- Use media access control address filtering to limit devices that can access your network
- Separate your computer devices from IoT devices
- Disable the Universal Plug and Play protocol "UPnP" on your router

FBI RESOURCES

InfraGard is an information-sharing and analysis effort with private sector partners who own, operate, and hold key positions within 85 percent of the nation's critical infrastructure. It equips its members to identify and mitigate vulnerabilities, develop incident response plans, and enact security best practices. For more details, visit www.infragard.org

CONTACT US: **For questions or assistance, locate and contact your local FBI field office at www.fbi.gov**