According to the U.S. Computer Emergency Readiness Team (US-CERT), many of the safety practices that are used to guard home and work computers apply to your portable devices as well. They include:

- Restricting access to your wireless network, by only allowing authorized users access to your network.
- Changing any pre-configured default passwords to ones that would be difficult for an outsider to guess.
- Keeping your anti-virus software updated.
- Using caution when downloading or clicking on any unknown links.

To address the evolving threats and increased risks of cybercrimes, DHS works directly with public and private partners to enhance cyber security. Through the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of State Chief Information Officers (NASCIO), and the National Governors Association (NGA) Cyber and Electronic Crime Resource Center, DHS works to promote cyber security awareness and digital literacy among all Internet users.

**Resources available:**
- Onguardonline.gov
- Stay safefonline.org
- IDtheftcenter.org

---

**Questions • contact Ken Cameron • 508.373.9452 • Kenneth.Cameron@becker.edu**