Basic Cyber Investigations: Understanding Digital Footprints

This course introduces learners to the concept of digital footprints and best practices in protecting personally identifiable information (PII). Topics include limiting an individual’s digital footprint, protecting privacy on social media, and the consequences of oversharing personal information; as well as steps to take after becoming a target of doxing.

**Current landscape.** Emerging technology and trends that can aid criminals in the commission of identity theft, credit card theft, child exploitation, and production of counterfeit documents.

**Personally identifiable information (PII).** Learn what PII is, why it can threaten individuals’ safety, and the scams and exploits criminals use to obtain it.

**Minimizing your digital footprint.** Learn how and why you should remove PII, and how to find where information may be located. Instructors demonstrate how to secure digital devices and request removal of data from a website.

**Social media.** Use security and privacy settings to control the amount of available information on multiple platforms.

**Resources.** Identify resources that can help victims of identity theft, doxing, and other related crimes.

To register, visit our training site at:

**www.nw3c.org**

Questions? Call 877-628-7674

To register, visit our training site at:

**www.nw3c.org**

Questions? Call 877-628-7674

"This project was supported by Grant No. 2018-MU-BX-K001 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice’s Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice."