

# **DOXXING DANGERS:**

***Doxxing Awareness  
and Lessons Learned***

***This project is funded by the U.S.  
Department of Homeland  
Security's Center for Prevention  
Programs and Partnerships,  
opportunity number DHS-24-  
TTP-132-00-99.***

# Doxxing 101

- **What is “doxxing?”**
  - **“Doxxing,” referring to “dropping dox/documents,” is the sharing of someone’s/an entity’s personal and private information on the internet without that person’s/organization’s consent**
  - **Doxxing is associated with intent to cause harm**
  - **Doxxing started in the 1990s as revenge within hacker culture**

# Is Doxxing Illegal?

- **In general, NO**
  - **By itself, doxxing is typically not considered illegal**
  - **Information used in doxxing is most often comprised of publicly available information that the poster feels would be compromising, distressing, or harmful**

# Doxxing Targets

- **Doxxing incidents target information that a poster feels may be harmful if shared, including:**
  - **PII, phone numbers, addresses, emails, employer(s), staff/board members**
  - **Services provided**
  - **Monies received and funding streams**
  - **Previous and/or dead names**
  - **Legal status, criminal records and/or court involvement**

# Doxxing Documents

- **Information used in doxxing are typically publicly available, documents targeted may include:**
  - **Property records**
  - **Phone numbers**
  - **Court documents (name changes, marriage/divorce/custody records, criminal records)**
  - **Information posted on social media**

# **Doxxing Documents cont'd**

- **Information used in doxxing are typically publicly available, documents targeted may include:**
  - **990s**
  - **Annual reports**
  - **Grant and funding award announcements**
  - **News articles, press releases, interviews, etc.**

# Doxxed Populations

- **Some communities, people, and entities may be more vulnerable to doxxing than others, including those with:**
  - **Arrest or criminal records**
  - **Court records (name change, marriage, divorce, custody)**
  - **High-profile individuals and/or organizations**
  - **Property ownership**
  - **Many and/or unsecured online accounts**

# Protecting Yourself

- **Limit your online exposure and presence**
  - **Don't create more accounts than necessary**
  - **Be cautious of what you post and share online**
  - **Never share personal or confidential information via social media or unsecure email**
- **Use multi-factor authentication (MFA) wherever possible, including email and social media**
- **Learn what records may be sealed in your state**

# **If You've Been Doxxed...**

- **Record any incidents of doxxing**
  - **Take screenshots, save emails, and/or keep written or typed logs of any incidents of doxxing**
- **Change passwords on all accounts**
- **Cancel and delete any unnecessary online accounts**

# **If You've Been Doxxed...cont'd**

- **Inform local law enforcement of any threats or perceived threats**
- **Inform your regional FBI office if you feel any doxxing is related to your center or center's work as an anti-LGBTQ incident**

# Has Your Center Been Doxxed?

Please fill out our [CenterLink Safety and Security Incident Report](#)

# Need a Security Consultation?

Email [actionlink@lgbtcenters.org](mailto:actionlink@lgbtcenters.org)

*Complimentary 30-minute consultation  
with CenterLink and TAL Global*

# Resources

- [CISA: Cybersecurity Best Practices](#)
- [CISA: Shields Up: Guidance for Organizations](#)
- [UC Berkeley Citizen Clinic Cyber](#)
- [FBI Field Offices](#)
- [Prevention Resource Finder | Homeland Security](#)
- [Elevating De-Escalation and Community Safety Approaches | Bridging Divides Initiative](#)
- [De-escalation Action Guide](#)