Protecting God's Children for Adults

Doxing: What is that?

By Robert Hugh Farley, M.S.

Introduction

On June 20, 2019, the *Washington Post* reported, "Ex-Senate staffer sentenced to 4 years for 'doxing' GOP senators in Kavanaugh confirmation fight." The newspaper article relayed that the offender, Jackson Cosko, 27, had pleaded guilty to "doxing" the senators. Cosko had been fired by one senator and then grew angry at others while watching the Senate hearing that addressed sexual assault allegations against then Supreme Court nominee Brett Kavanaugh. Cosko subsequently doxed the five senators by anonymously editing their Wikipedia pages to add their phone numbers and home addresses.

Some may ask, what is doxing? *Merriam-Webster's Dictionary* defines the word **dox** as slang: to publicly identify or publish private information about (someone) especially as a form of punishment or revenge.

Background

According to *Wired Magazine*, the word dox is the modern, abbreviated form of "dropping docs or dox." Doxing originally was an old-school revenge tactic that emerged from the Internet hacker culture of the 1990s.

Mischievous hackers in the 1990s did not have a lot of options for taking revenge on a rival hacker, so penetrating an enemy's anonymity by posting personal information or documents became a powerful weapon to subject a rival to online harassment (such as on the Internet Relay Chat / IRC portion of the Internet) .

Today, doxing generally refers to the practice of ordinary people, not just hackers, using the Internet to locate and collect someone's personal and private information and then publicly release that information online.

Doxing Problems Today

The aim of doxing is violating one's privacy, resulting in fear, stress and panic. Illegitimately posting a young person's name, photo and cell phone number, for example on Craigslist, can result in the victim being swamped with sexually explicit text messages, sexually explicit images and even threats of violence or sexual assault all of which puts the victim at risk.

Unlike the 1990s, hacking an electronic device or an account today is not a requirement for doxing since an extensive amount of someone's private information is available to the public, if one knows where to look.

Once a person has been targeted by a doxer, a simple Google search starting with just the victim's name can yield a variety of results. Following the Google search, a doxer is able to explore the many social media sites or even professional sites like *Linkedin* to find a treasure trove of personal and private information. Even the background of an innocuous personal posted photo can provide a plethora of information for someone with nefarious intentions.

When the initial doxing process begins, the offender is busy locating and identifying a victim's private or personal information. Examples of doxed information would include: a person's social security number, their home address, telephone number, email address, social media profile names, work history, financial or banking history and the contact details for spouses, partners, relatives and children. Once the essential information has been located and collected, the public doxing of a victim begins by the offender posting the victim's personal information on the Internet.

Most people generally view doxing negatively because it violates privacy and is often fueled by the need for revenge. Doxing is also seen by some as a way to punish someone for perceived wrongs or bring someone to justice by outing a person in the public eye.

People's lives have been ruined by doxing. Some doxing attacks can even lead to a mass campaign of public shaming, which is the online equivalent of the slang workplace term of "mobbing" or workplace bullying. Doxing can cause victims to lose their jobs, their families, their friends and even their homes. Doxing someone actually ratchets cyber-bullying up to the next level.

One of the most disturbing doxing problems is the issue of people on the Internet relentlessly doxing the wrong person. An example of this problem follows the infamous 2017 "Unite the Right" rally in Charlottesville, Virginia. A torch carrying protestor, wearing an "Arkansas engineering" shirt, was identified on the Internet as being Kyle Quinn, a professor at the University of Arkansas.

Unfortunately, the real Kyle Quinn was never at the rally in Charlottesville and had been misidentified by Internet "doxers." That important fact did not stop the "doxers" from spreading misinformation. As a result of the online shaming, the real Kyle Quinn was forced to spend a weekend in hiding. Later, the actual rally protester, a former Arkansas engineering student named Andrew M. Dodson, apologized for the misidentification.

Prevention

A prevention tip to prevent doxing is to increase all of your privacy settings on social media accounts.

- On *Facebook*, edit your profile so it cannot be searched and make your friends list private. Also, be cautious about "friending" colleagues from work as they could one day become rivals.
- On *Twitter, Pinterest* or *Instagram*, edit your security settings and then check who can follow you or view your posts. Additionally, review all of your posted images with the knowledge that an image can easily be copied by somebody and then pasted somewhere else.
- Conduct a review of social media sites that you no longer actively use, to see if profile information or photos are still available online.
- Always use strong passwords or usernames, mixing letters, numbers and symbols
- Lastly, you should consider using a different email address for each social media account. At the very least, you should not use the same email address for both a financial account and a social media account.

Conclusion

Being proactive and taking the time to go online to delete as much private information that can be located is a good first step to prevent one from being doxed. Next, continuing to secure one's online identity can help make it more difficult for one to become a doxing victim in the future.

Technology continues to rapidly change. Parents and all of us who are charged with protecting children must continue our efforts to stay abreast of the many new devices, software programs and the latest apps that may be used by young people and child molesters seeking to manipulate and sexually abuse children.