Office of the Chief Information Security Officer

Doxxing and SWATing

What Is Doxxing?

Doxxing (aka Doxing), slang for "dropping documents," refers to gathering an individual's information such as home address, telephone number and/or email address, and posting it publicly without permission.

This is usually done for malicious purposes such as public humiliation, stalking, identity theft, or targeting an individual for harassment. Doxxing is also used for exposing the internet identity of someone and is generally used as an intimidation technique or for retaliation.

In October 2018, the United States Capitol Police arrested Jackson Cosko, a Congressional intern, for allegedly posting private, identifying information (doxxing) about one or more United States Senators to the internet. He was initially charged with Making Public Restricted Personal Information; Witness Tampering; Threats in Interstate Communications; Unauthorized Access of a Government Computer; Identity Theft; Second Degree Burglary, and Unlawful Entry.

Doxxers are individuals who are experts in gathering and disclosing information, and/or are in it for political or financial gain. Doxxers may target government employees to identify law enforcement or security personnel, demonstrate their own hacking capabilities, or attempt to embarrass the government.

Why Doxxing?

Motivations for these activities include personal quarrels, financial gain, political activism and many other reasons. Many segments of popular culture including social media exploit this.

Doxxing has also enabled the nefarious and dangerous act of "SWATing".

What Is SWATing?

SWATing is an internet prank/crime in which someone finds your address either through your computer's IP address, or because your name and location is known. They then anonymously call 911 and report a fake emergency.

For example, the 'SWATer' calls 911 and says someone is being held at a gun point or someone is going to commit suicide and a SWAT team would be dispatched to the address. Fake reports leading to SWAT team deployments have doubled since 2011.

A particularly severe case took place in Wichita, Kansas, in 2017. Some online gamers were upset with an individual and contacted 911 saying that this individual had killed their father, was holding their mother and sister hostage and was planning to burn the house down with the occupants inside. The address the SWATers had given 911 was the individual's past address and when the new home occupant exited the house, he was fatally shot by Wichita police.

Why SWATing?

Reasons are generally traceable back to an event or interaction between the SWATer and SWATee.

Additionally, the SWATer may seek publicity or other public reaction(s). For SWATing the motives will be part of any investigation.

Have Additional Questions or Need Assistance?

Contact the Texas Department of Information Resources CISO Office at DIRSecurity@dir.texas.gov.

Legality?

Doxxing isn't necessarily illegal if the information exposed is part of the public record. Such information includes arrest records, marriage certificates, major traffic violations, and real estate transactions.

Doxxing can be illegal if someone publishes information that isn't in the public record, such as your bank account information, credit card numbers, or birth certificate.

However, SWATing is a Class A misdemeanor in Texas under Texas Penal Code Sec. 42.0601 and if somebody is hurt during the SWATing it becomes a felony of the third degree.

Exposure

Data That You Provide — It is always a good idea to establish limits on the level of information that you share about yourself on social media and make certain that it is factual and appropriate for sharing.

There are so many social media platforms, and each has its own privacy settings that must be adjusted to best match what one intends to be their level of transparency versus level of privacy.

Additionally, many settings on social media platforms constantly change as new features are added or other changes are implemented.

Users should review their initial privacy settings and then periodically check to make sure that the chosen settings remain aligned with a user's privacy expectations.

If a plan for keeping information confidential relies upon who is in the inner circle, then further deliberation should go into accepting network or friend requests.

There are many bogus profiles out there and some are very well constructed. One useful tool for weeding those out is to use reverse image lookups such as http://tineye.com, Google or similar platforms.

Social Media Platform Security

Here are some popular platforms and their security configuration options and use policy:

Facebook's guidance: https://www.facebook.com/help/325807937506242/

An example of a Facebook privacy setting guide: https://www.techlicious.com/tip/complete-guide-to-facebook-privacy-settings/

Relevant use policy: https://www.facebook.com/policies

Twitter: https://help.twitter.com/en/safety-and-security#hacked-account

Relevant use policy: https://help.twitter.com/en/rules-and-policies/twitter-rules

LinkedIn: https://safety.linkedin.com/staying-safe#Protecting-Yourself

Relevant use policy: https://www.linkedin.com/legal/professional-community-policies

Instagram: https://help.instagram.com/527320407282978

Relevant use policy: https://help.instagram.com/581066165581870

Please refer to the privacy and security guidance for the social media application that you use.

Information That is Public — In addition to social media information, public information can also be added to the mix and used as open-source intelligence.

This information could be used for social engineering, criminal activity, and foreign intelligence recruiting and targeting. The data is not always matched accurately leading to errors and entanglement.

As privacy debates, issues, and laws continue to mature, the next few years might see massive shifts in privacy rights, which will impact how data is handled and what is considered publicly available information.

What is Out There?

There are many public sector and private sector organizations that currently use public data about a person to compose a series of challenge questions that is used for identity authentication.

The information can be which vehicle was owned at one time or an old physical address.

While not an all-encompassing list, there are numerous websites that rely on personal data collection as their business model, receiving revenue by selling your data to marketers, advertisers and others.

These sites scrape data together from various sources and charge a fee for a person to look for their data or another person's data. These companies use open-source intelligence methods, public records, and, at times, data purchases to build a product or service around that.

beenverified.com
cocofinder.com
findermind.com/free-people-search-engines
intelius.com
mylife.com
peekyou.com
pipl.com
radaris.com
skipease.com
spokeo.com
spyfly.com
truthfinder.com
unmask.com
ussearch.com
yasni.com
zabasearch.com

How to Get Rid of It?

While removing 100% of this information may not be possible and may require repeated attempts at removing information, there are many guides on how to scrub this public data, including:
joindeleteme.com/help/diy-free-opt-out-guide

What Can a Victim of Doxxing Do?

Contact your local law enforcement and seek legal counsel. You can also report it immediately to whatever platform may have been leveraged in the dox and ask for its removal.

Some examples:

https://www.facebook.com/help/reportlinks

https://help.twitter.com/en/rules-and-policies/abusive-behavior

https://www.linkedin.com/help/linkedin/answer/37822?lang=en

What Can a Victim of SWATing Do?

First and foremost, comply with the SWAT and law enforcement team and do nothing that could be perceived as a threat.

This is a dangerous time and has resulted in death. Once law enforcement has the scene secured, then discussions and de-escalations can begin.

If you have concerns that you may become a victim of SWATing contact your local law enforcement agency immediately.

Sources

Airaksinen, Toni. "More Than 30 UT Students Doxxed For Crime of Being Conservative" PJ Media. January 13, 2019.

https://pjmedia.com/trending/more-than-30-ut-students-doxxed-for-crime-of-being-conservative/

FBI Cyber Intelligence Section Intelligence Bulletin. "Law Enforcement at Risk for Harassment and Identify Theft through "Doxing". August 2, 2011.

Economist staff author. "Swatting Could Become a Federal Crime." The Economist. January 12, 2019.

https://www.economist.com/united-states/2019/01/12/swatting-could-become-a-federal-crime

Gagne, Ken. "Doxxing defense: Remove your personal info from data brokers." Computerworld. Nov 20, 2014.

http://www.computerworld.com/article/2849263/doxxing-defense-remove-your-personal-info-from-data-brokers.html

Garber, Megan. "Doxing: An Etymology."
The Atlantic. March 6, 2014. http://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/

Tripwire Guest Authors. "Doxxing: What it is
How you Can Avoid It." Tripwire. December 26, 2018.

https://www.tripwire.com/state-of-security/security-awareness/what-is-doxxing-and-how-can-you-avoid-it/

Twitch. "Preventing Doxxing, Swatting and other IRL Harm".

https://safety.twitch.tv/s/article/Preventing-Doxxing-Swatting-and-other-IRL-Harm?language=en_US

Disclaimer: This guidance is not meant to replace legal counsel. One should consult their lawyer or general counsel if they are impacted. Additionally, appearance of an URL or reference to a company does not condone that business practices or meant to show any sort of favoritism and are only used as discretionary examples.

Learn More About DIR:

dir.texas.gov

1-800-ASK-DIR1
1-855-275-3471