Secure Data Exfiltration

A walk-through of safe(r) data exfiltration recommendations.

This guide will provide practical advice for multiple threat-levels.

Threat	Description
Level 1	Primary Considerations
Level 2	Quick And Liable Methods
Level 3	Safer(Not Risk Free) Methods
Level 4	Release Protocols

Disclaimer:

- We are not lawyers, and this is not legal advice.
- Technology is constantly evolving, and this information could be outdated.
- Following this advice does not guarantee protection against every threat.
- You accept responsibility for your actions and the repercussions of following this advice.

We believe all individuals should have awareness in regards to any potential data exfiltration actions, and opsec is extemely important. You will go to jail.

Level 1 - Are You Sure You Want To Do This?

Leaking confidential documents is a violation of all the things. You should assume that you will be prosecuted to the fullest extent possible. You will be fired, expelled, blacklisted, demonized by the media, singled out, exiled, arrested, harmed, detained, etc. Even whistle-blower protection laws will not save you if you expose the wrong people.

That being said, there may be times when a person may need or feel obligated to release information. If those people want to do so without ruining their lives, that information should be free and accessible. The scope of that decision is much broader than this guide. This guide expressly does NOT encourage anyone to participate in any illegal or unethical activities.

The Courage Foundation

“The Courage Foundation is an international organisation that supports those who risk life or liberty to make significant contributions to the historical record. We fundraise for the legal and public defence of specific individuals who fit these criteria and are subject to serious prosecution or persecution. We also campaign for the protection of truthtellers and the public’s right to know generally.”

Courage Foundation Homepage (https://www.couragefound.org/)

Level 2 - Webmail/Email/IM

TL;DR – Don't use webmail, email, or IM to exfiltrate or release data/documents.

At your school, workplace or organization you should always assume everything you do using company owned devices is being monitored. You have ZERO expectations of privacy while using company owned devices, on company property, on a company owned network, or on a company owned connection.

There is usually remote monitoring and management software present. They can run in stealth mode operating like a rootkit. Every keystroke could be logged. Screen-shots/video can be viewed. Every bit of traffic you transmit can be logged by multiple network appliances.

We have personally seen people fired without notice for activities they had no idea were being watched. Sometimes they will not jump on you right away, so you feel more comfortable and push your limits. Law enforcement is also known to let you operate after detection to build a more airtight case.

Even if they aren't actively monitoring, the digital paper trail will still be easily tracked back to you if you use one of these methods.

Level 3 - Removable Media

If your computer has a USB drive, copying files to a removable thumb drive and removing the data from the property before release is a safer way to go. There are still risks of your activity being monitored. There is always risk.

Another way is to use a cell phone or camera to take photos of the documents, then strip the metadata before release through a secure channel.

You can remove physical documents from trashcans or dumpsters and scan those in later.

Level 4 - Release

Follow **NetP Wiki – Browsing: Level 4 (http://wiki.shadowlinkit.com/browsing/#level4)** recommendations.

These sites offer guides to leaking data:
Submit documents to WikiLeaks (https://wikileaks.org/#submit)
How to leak to The Intercept (https://theintercept.com/2015/01/28/how-to-leak-to-the-intercept/)
How to leak to Gawker (http://gawker.com/how-to-leak-to-gawker-anonymously-1613394137)

Also check out:
WikiLeaks: Tips for sources (https://wikileaks.org/#submit_help_tips)
WikiLeaks: After submitting (https://wikileaks.org/#submit_help_after)