



Cyber Safety for Women and Targeted Individuals

By Udit Rai

Using this course

This course is NOT:

- An in-depth guide that takes you through every detail of everything mentioned wherein.

This course IS:

- A comprehensive set of guidance on your threat model, as discussed earlier. When confused in concept or implementation, consult ChatGPT/Grok.

Intro

This course is mainly for:

- Women, due to a special range of threats and concerns against them

But is also for:

- Other cyber-targeted/harassed persons; since many of the threats and defences are shared

This Course is NOT
for you, if you:

Have more than 10K followers

Regularly transact a value of
over \$5000 per day

Are an Escapee of Violence

3 Tiers of Security

Threat Profiling

Threat Modelling

Threat Mitigation

Section 1

THREAT PROFILING

“WHO WOULD WANT TO HURT ME, AND WHY?”



The First
Question:

Who
wants to
harm me?

Strangers: Extremists

These trolls don't really care or affiliate with any cause, they just revel in causing hurt online. Why online particularly?

1. Most major platforms (YouTube, TikTok, Facebook, etc.) use engagement-driven algorithms, so they promote content that triggers strong emotions (anger, fear, tribal loyalty)
2. Guide users toward more **extreme** content over time - because it's “stickier” and keeps users watching/clicking
3. Create **filter bubbles** where users mostly see views they already agree with, deepening polarization



Strangers: Trolls

These trolls don't really care or affiliate with any cause; they just care about hurting people online, as much as possible. It is a sport to them. Why online?

1. They hurt people online since it is easier and might translate to popularity; among their peers and maybe the internet in general.
2. Most social media to an extent run on trolling: It drives drama, a key for viral content. Just try clicking on “feminists roasted” videos on YouTube and see your algorithm change.
3. From YouTube to Instagram to Twitter/X, all social medias love trolls: They boost engagement **massively** by sparking debate, outrage and arguments.



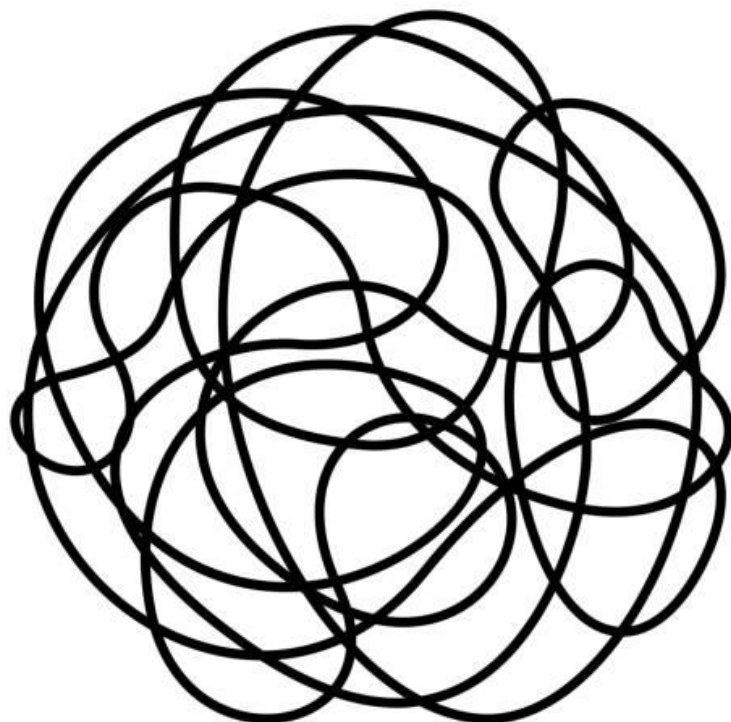
Known Persons

Some people you know—like an ex, someone whose proposal you turned down, or even a seemingly friendly acquaintance—can become a threat.

Why?

1. It's about control. When they can't control your choices, some try to punish you for acting independently. It's less about anger and more about dominance.
2. This dynamic isn't limited to men vs. women—it's common in all bullying patterns. Some people just can't stand others being independent: and it's rarely noticeable.
3. And it doesn't always follow a fight; jealousy mostly starts quietly, during seemingly normal conversations.





The Second
Question:

Why do they
want to harm
me?

Threat Actors: Aggressors

Threat Actors refers to the persons who are the threat. Although there can be many ways a person can harm another, this refers specifically to persons who use calculated attacks on others.

These persons have the following traits:

1. Dominator Complex
2. Externalized Blame
3. Authoritarian Mindset

Victims who succumb

Although many suffer such events, this refers specifically to those victims who “lose” - incurring personal, financial or professional setbacks due to events. These individuals tend to share certain traits:

1. Victim Complex
2. Internalized Blame
3. Dependent Mindset


Victims who grow

Although many suffer such events, this refers specifically to those victims who “win” - managing not only to recover but also end up gaining from the event in either personal, financial, and/or professional terms. These individuals tend to share certain traits:

1. Confident Mindset
2. Genuine Kindness
3. Social Intelligence

Section 2

THREAT MODELLING, I.E. WHAT ATTACKS WILL
COME, AND WHERE FROM?



Where are you targeted?

§ Platforms most known for cyber-bullying (security.org) :

- § Instagram 🏰 : Consistently rated worst for mental health and safety across multiple surveys
- § Youtube (79%)
- § Snapchat (69%)
- § Gaming Communities (57%)
- § Facebook (49%)

The State of Online Platforms

GlobalWitness did an experiment on Social Media Moderation

They uploaded advertisements in 4 most common languages globally

Calling for global mass killing of women regardless of demographic

AI Generated Video Tutorials, Graphic and Filthy language included

All approved for publication on X, Facebook, YouTube and TikTok

Only deleted by GlobalWitness last minute before going live

Types of
Attacks
(Special to
bullied
persons/
women)

Cyber-Stalking

Online Harassment

Non-consensual intimate
image abuse (NCII)

Doxing

Cyber-Stalking

This is mostly exes or rejected persons, or even acquaintances *with you have cordial relations*. Like discussed in the first section, there is not really much rhyme or rhythm to their actions. It is unwanted and persistent contact and tracking of a person.

It does occur with strangers, particularly in cases of Doxxing (explored later), but the overwhelming majority of cases is with known persons.

Online Harassment

This can constitute threats, rumors, spamming, tagging, mean comments; or any other sort of persistent online behavior that is done to significantly hurt your mental health.

This is mostly strangers, and less frequently but still commonly known persons. However, in both cases there will usually be an attempt at anonymity, either using fake IDs or by sticking to gossip and rumors without direct contact.

NCII

For women it is almost always explicit, for men there are multiple possibilities. It is quite prevalent, with a majority of women worldwide reporting some instance of seeing online inappropriate, non-consensual content of them.

While it used to be mostly angry exes, now it also constitutes strangers due to AI generated content, with how easy it is to bypass the AI filters.

Doxxing

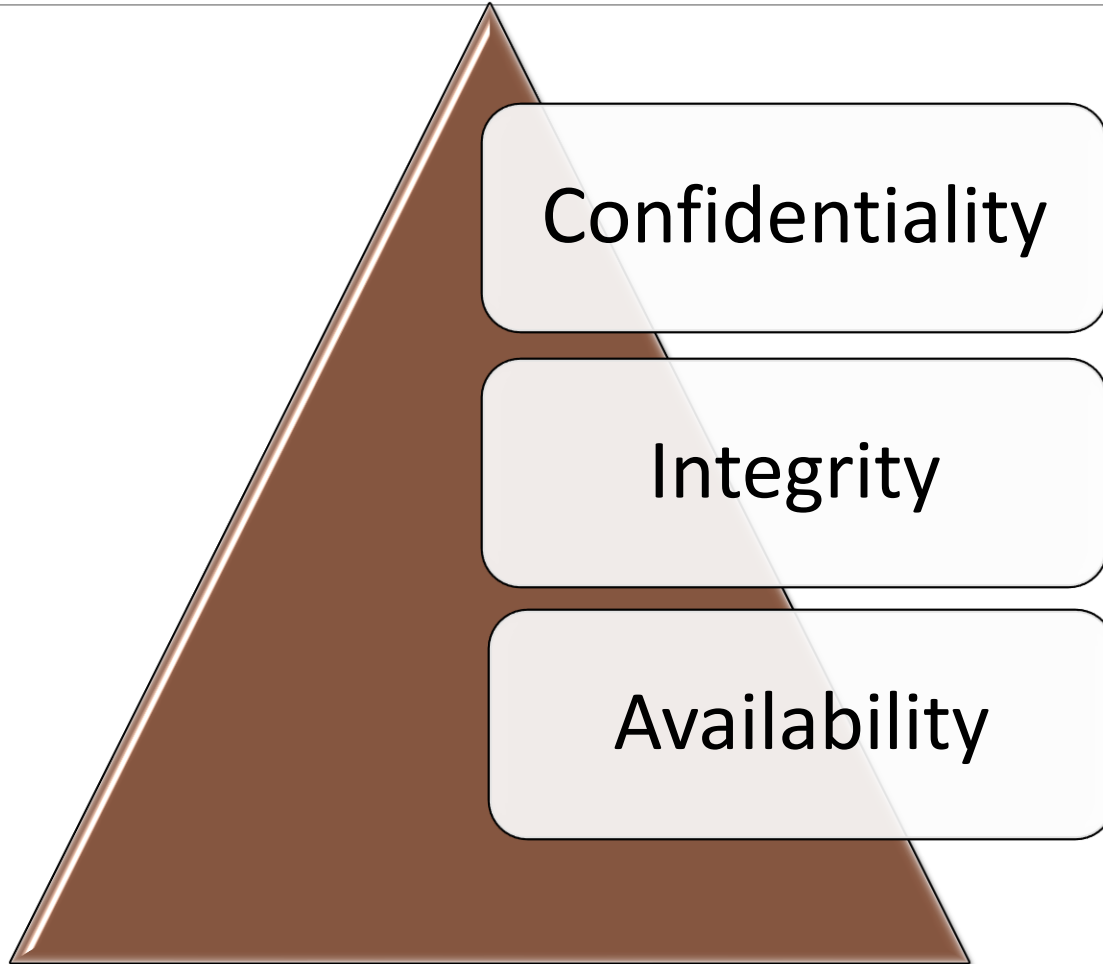
This is most commonly done by strangers on the Internet, less commonly by exes and scorned persons, or persons you have been in a fight with.

It is a public reveal of your private and identifiable information; a full dox ranges across at least 20 points from home address to parent/spouse phone number to your pictures and your social media passwords.

Section 3

THREAT MITIGATION, I.E. THWARTING ATTACKS

Cybersecurity in General



Principle: Privacy



Since we do not have the resources or the time to set up defences for Integrity and Availability; we rely on third party vendors for this, such as Google, Microsoft etc.

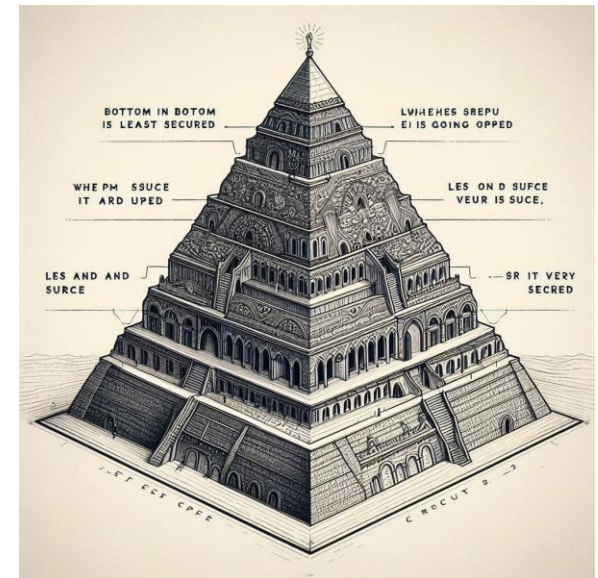
What we have to do is ensure confidentiality; i.e. no one can reach data about us that we do not want. We call it Privacy for individuals.



Principle: Pyramid of Pain

Imagine your data as jewels being left alone in a house. The more windows and doors (open surfaces) you have, the easier it is for someone to find a way in. The more defences, the more money, people and time it takes to crack it; and therefore, the less likely it is to be broken into.

Similarly, we layer defences for bad actors to access your information, the more defences the less likely someone is to find crucial information needed to hurt you.



First Layer of Defence



What is OSINT?

What is OSINT?

OSINT stands for Open Source INTelligence and means collecting publicly available data about a target and using it for analysis.

Examples of OSINT usage:

- Collecting data on US Surveillance Airplanes: [Blog](#)
- Finding people who have gone missing or been kidnapped: [TraceLabs](#)
- Using it for investigation and crime prevention: [Blog](#)

Why to
prevent
OSINT?

Let's take the example of a woman who turned down a friend, and this friend now has had a nervous breakdown; and is sending her texts that directly threaten her physical safety.

Examples of data this man can get via OSINT



Home Address

FROM

People search engines, online govt records etc



Workplace

FROM

LinkedIn, Tagged posts, Google Image results



Daily Route

FROM

Location-Tagged posts, Snapchat



Family Details

FROM

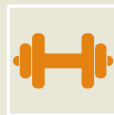
Public family trees, LinkedIn, Tagged Photos



Favorite Shops

FROM

Tagged posts, Reviews left Online



Gym Schedule

FROM

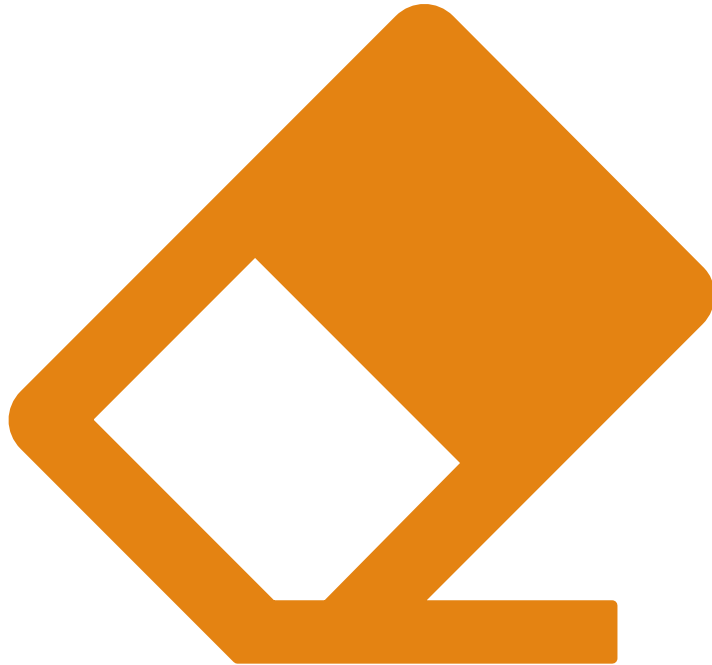
Data leaks in fitness app shares, Group class posts



Securing Yourself



Combined with an attack like
violent tendencies or
defamation, Offensive OSINT
can easily be an open door to
personal disaster



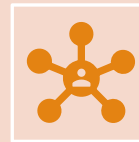
What we can prevent



In today's world, your data is everywhere—and trying to erase all of it is nearly impossible without going off-grid.



You can't delete your old school photos, recover every forgotten account, or monitor every comment your name might show up in.



But what you can do is disconnect your identity from that data—so even if someone finds something, they have no clue it's yours.

How to unlink Data:

- **All** Non-professional accounts: (including review/fitness/delivery etc.)

Use your personal name and personal email ❌

Use a randomized name and randomized email (legitimate) ✅

- **All** Online Provided Phone numbers:

Give your personal number ❌

Only provide a virtual number (under another name) ✅

- **All** Pictures:

Rely on removing metadata ❌

Delete metadata **and** blur your pictures with filters ✅



Good Filter Examples



Bad Filter Examples

What is Privacy Maximization



Providing valid data



On Official Platforms



While ensuring to use

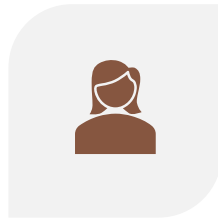


All privacy features built-in

List of Features to Disable



SEARCH ENGINE
INDEXING



PUBLIC PROFILE
VISIBILITY



DISPLAY EMAIL
AND PHONE



HIDE FRIENDS
LIST



Don't hide recommendations



Don't hide pictures of achievement, family or work



Do: hide personal details written in about section etc.



Reason: LinkedIn is a summary of your work life, and that's a matter of pride; hiding may cause mental health risks to you

LinkedIn:
A Necessary Evil

What is Account Security



Preventing unauthorized
access



On your official accounts



By using built-in tools



That are stronger than
password-only



Very strong passwords



2 Factor authentication NOT using SMS/Calling



Account Data Privacy and Security

3 Pillars of Account Security

Strengthening Passwords



USE RANDOMIZED
PASSWORDS



WITH A PASSWORD
MANAGER



DISABLE BROWSER
“ASK TO SAVE
PASSWORD”



CLEAR ALL
BROWSER SAVED
LOGINS



USE AN
AUTHENTICATOR
APPLICATION



FROM A HIGHLY
REPUTED COMPANY



IN WHICH YOU
LOGIN USING EMAIL



AS 2-FA FOR ALL
YOUR OFFICIAL
ACCOUNTS

2 Factor Authentication (Strong)

Data Security and Privacy: What to Disable

Auto-
Synchronization
of Data

Ad
Personalization
and Geo-
Tagging

History (Voice,
Assistant,
Location)

Third Party
Application
Access
(Unused)



What we have achieved

Before buying anything, say a product from Amazon: You will check reviews on multiple websites about it, go onto YouTube and watch a video review of it, and you may also go to the manufacturer website and read more about them before buying.

The first of Cyber-Attacks is a bit similar in that the attacker studies the target and collects data, but the usage of that data is for an attack. Now if the attacker has no knowledge about you; they simply cannot plan a good attack.



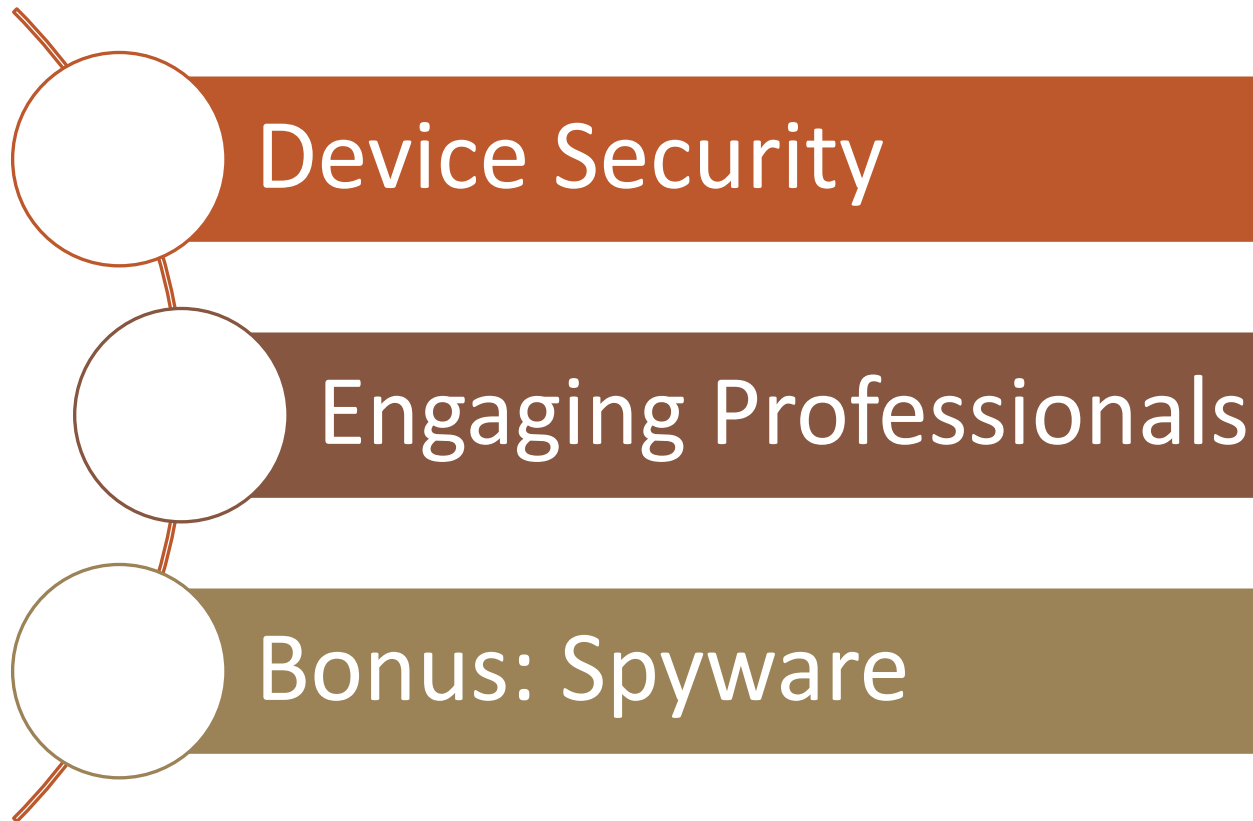
What we will Secure Next

The next layer builds on an assumption: The attacker stumbled upon some data by accident; let's say your yoga trainers' post in which they mention you by name, or an old school photo combined with a scam call to an old friend of yours for your information.

Now, once they have your information; they will try to use some malicious software/device against you for monitoring or to cause hurt.

Let's make sure their attempt doesn't work.

Second Layer of Defence





First Layer: Browser Security



Second Layer: Device Firewall



Third Layer: Anti-Virus

3 Pillars of Device Security



Securing Browsers

While your browser is a personal preference matter, you should do the following:

- 1. Add Extensions:** uBlock Origin, Privacy Badger, Password Manager, HTTPS Everywhere
- 2. Use Built-In Features:** Disable Password Saving, Set Privacy Settings to Max.

Of course, you can avoid doing this manually by using a more secure browser like Brave. (Firefox not recommended)



Device Firewall

1. Enable Firewall: While PC OS like Windows, Linux, Mac have built-in firewalls; you'll need to install one for mobile (I personally love Rethink)

2. Use Built-In Features: Check if firewall is on. If you are not a technical professional, I would not recommend anything beyond this.

Of course, you can avoid doing this manually by using a third-party firewall from a reputed anti-malware provider, e.g. Bitdefender



Anti-Virus

Hardening Antivirus is a bit of a technical task; so just:

1. Go to built-in Antivirus Settings and set everything to ON

AND

2. Get **one** very reputed paid anti-virus across your devices

If you have any office/study files that cause issues with your antiviruses, you can add its folder into exclusions, if you're sure of safety.

Reporting

If **after a cyber threat has been established**; things feel off; for example, finding a lock not in the position you left it, being approached by strangers with strange vibes, signs of spyware, repeated login attempts, or finding leaked info about yourself online etc. -

1. Treat this with the serious-ness it deserves: Moderate. Make a chamomile tea and relax, there's no hit out on you.
2. Engage Law Enforcement **before** anyone else; then go live with a friend/relative/dorm if you want to
3. Engage top-rated private investigators, specialized lawyers, or trusted NGOs for all-around advice if the police recommends a lawsuit, OR things have taken a turn for worse

Anti-Spyware

We have covered enough to ensure that no non-advanced threat can install a malware onto your devices, at least unless you have been careless with your cyber-security.

So what spyware are we talking about?

1. GPS Trackers and similar
2. Specialized Phone Spyware
3. Spy Cameras

Anti-Spyware

1. Get the following apps on your phone-

- Hidden Camera Detector (*By FutureApps*)
- AirGuard (*By Technische Universität Darmstadt*)
- Fing Network Mintor (*By Fing Ltd*)
- Tutorials for each will be provided within app

2. Do the following Checks Weekly (or in hotels)-

- Turn off the lights and check for blinking lights
- Shine a flashlight around all the rooms with the light off, where it shines back – Investigate
- Under your car and in your bag pockets

No Need For Paranoia!

Think of the weekly checks like looking both ways before crossing or adding a salad to your meal - not out of fear, just a smart habit for good mental hygiene.

If you do find something (rare, but possible), don't touch or turn it off. Quickly grab your essentials, add a lock, head to a public place like a café, then go stay elsewhere for 3 days.

Since there is a slight chance someone saw you find the camera, return home later with a group of friends (include a few intimidating ones if possible). Once safe inside, hand the devices to law enforcement as-is.



Thanks
and
Regards

HOPE THIS WAS USEFUL!