black hat USA 2021

August 4-5, 2021

BRIEFINGS

A survivor-centric, trauma-informed approach to stalkerware

Lodrina Cherne & Martijn Grooten

https://bit.ly/blackhatstalkerware

About us

Lodrina Cherne

@hexplates

she/her

Martijn Grooten

@martijn_grooten

he/they

Resources:

https://bit.ly/blackhatstalkerware

Content warning: this presentation will discuss intimate partner violence and gender-based violence.

National Domestic Violence Hotline:

1-800-799-7233

or

www.thehotline.org

Or similar hotlines around the world

NATIONAL
DOMESTIC
VIOLENCE
HOTLINE

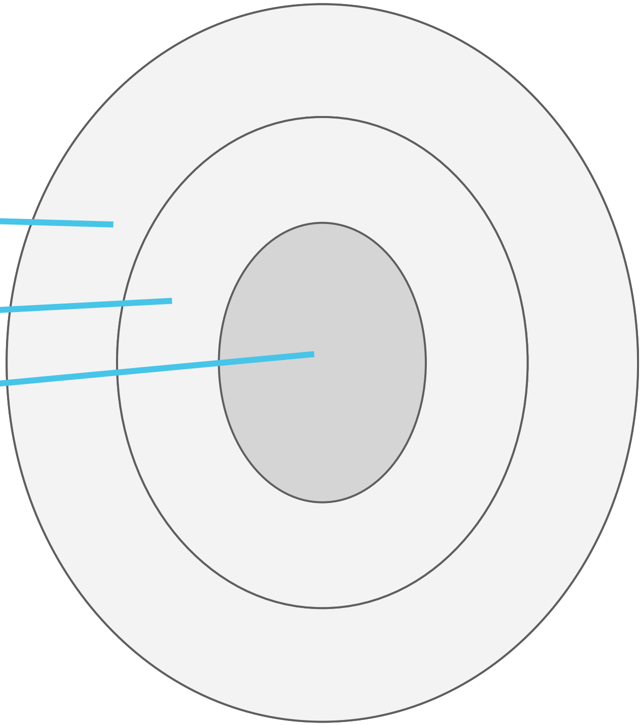
Agenda

Intimate Partner Violence and Gender-Based Violence

Tech Abuse

Stalkerware

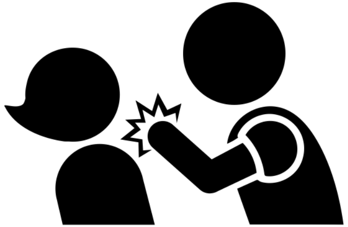
- how does it work?
- how to support someone?
- what can we all do?



Intimate Partner Violence

Gender-Based Violence

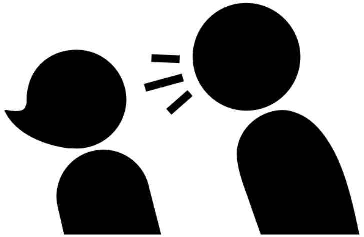
Intimate Partner Violence (IPV)
(also: domestic abuse, domestic violence)



CDC: 1 in 3 women
1 in 7 men
experience physical violence at the hand of an intimate partner

Gender-Based Violence is any violence rooted in exploiting unequal power relationships

Common misconceptions about IPV



Doesn’t always involve physical violence

Not all survivors are women, not all abusers are men

“Why can’t she just leave?”

Tech abuse

Tech abuse

Tech abuse is the use of technology to facilitate IPV

“99.3% of domestic violence practitioners have clients experiencing technology-facilitated abuse”
(WESNET, Australia)

WESNET
The Women’s Services Network

Examples of tech abuse

Remotely-controllable IoT devices

AirTag/Tile and other “Find my” tools

Shared social media and/or email password

Regular device access

Bluetooth LE • Ultra Wideband • AirTag • Designed by Apple in California • Assembled in China

Most tech is not built with the IPV threat model in mind!

Tech abuse resources

CETA (Clinic to End Tech Abuse, Cornell University)

NNEDV’s Tech Safety website

WESNET’s Tech Safety website

Refuge UK’s Tech Safety website

https://bit.ly/blackhatstalkerware

CETA

CLINIC TO END TECH ABUSE

Resources

Stalkerware: how does it work?

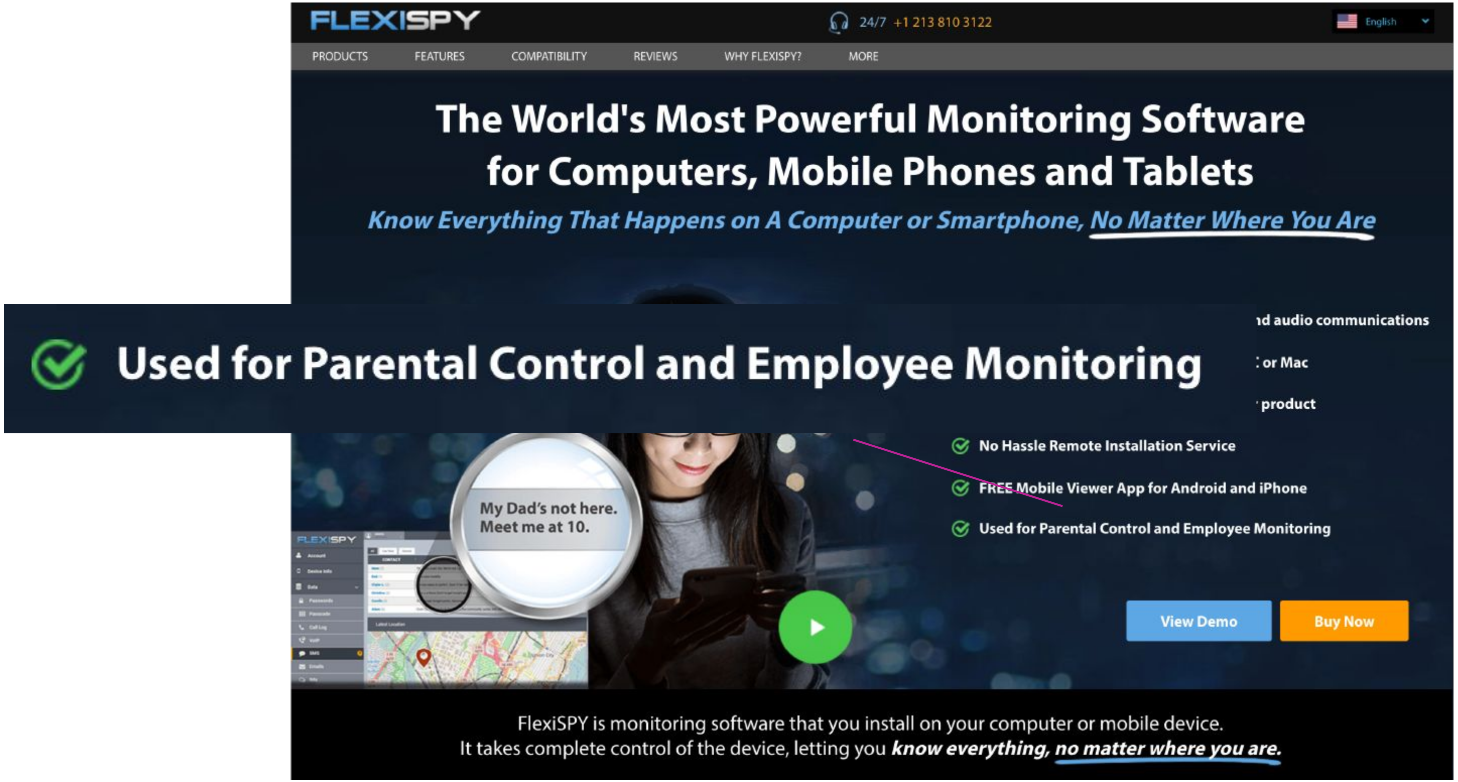
Stalkerware: Tech-Abuse-as-a-Service

Stalkerware is “software, made available directly to individuals, that enables a remote user to monitor the activities on another user’s device without that user’s consent and without explicit, persistent notification to that user in a manner that may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence” (Coalition Against Stalkerware)

excludes government/criminal spyware

one-time consent not enough!

https://bit.ly/blackhatstalkerware



The World's Most Powerful Monitoring Software for Computers, Mobile Phones and Tablets

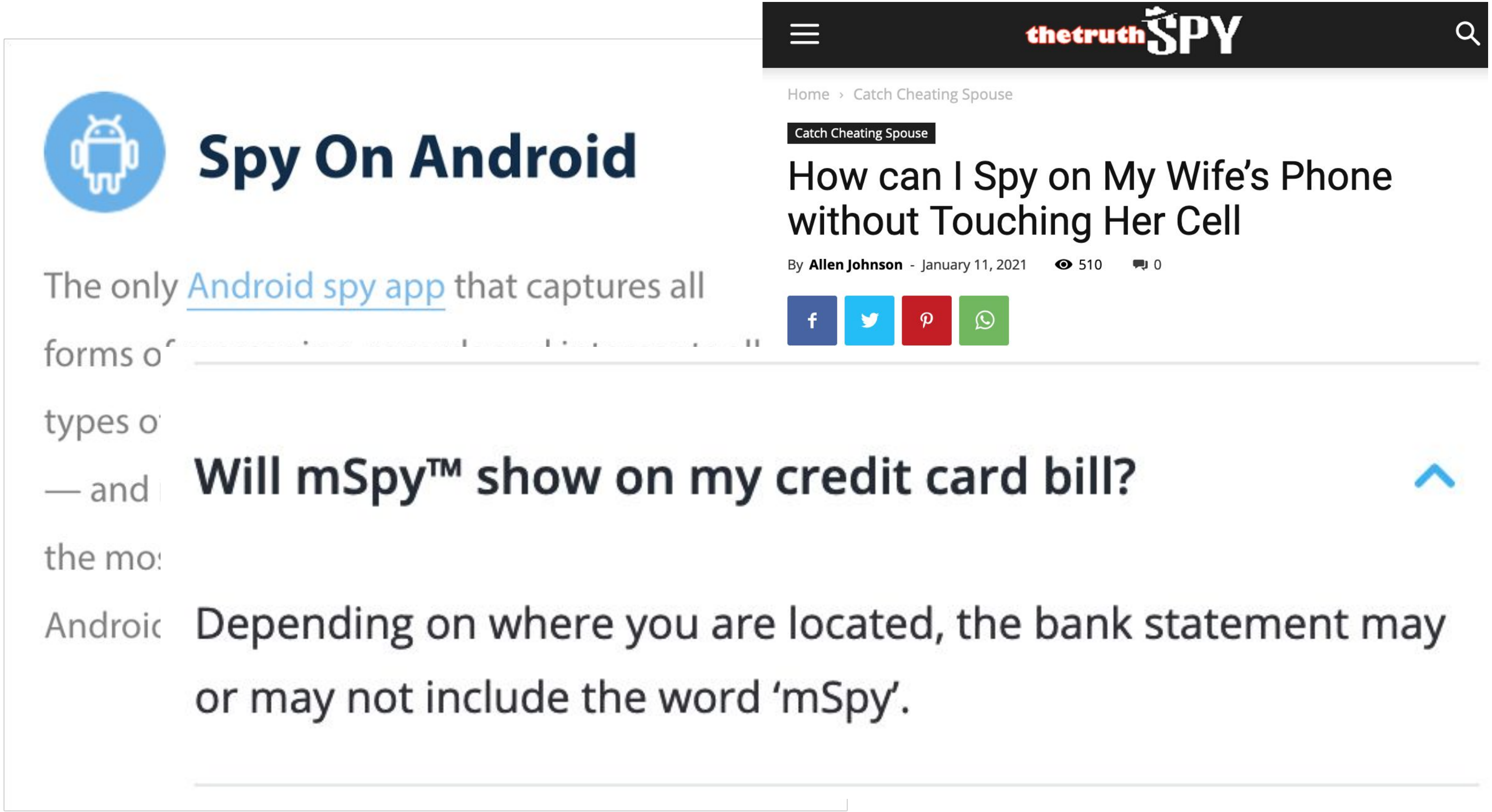
Know Everything That Happens on A Computer or Smartphone, No Matter Where You Are

✓ Used for Parental Control and Employee Monitoring

- d audio communications
- or Mac
- product
- ✓ No Hassle Remote Installation Service
- ✓ FREE Mobile Viewer App for Android and iPhone
- ✓ Used for Parental Control and Employee Monitoring

FlexiSPY is monitoring software that you install on your computer or mobile device.
It takes complete control of the device, letting you ***know everything, no matter where you are.***

https://bit.ly/blackhatstalkerware



thetruthSPY

Home › Catch Cheating Spouse

Catch Cheating Spouse

How can I Spy on My Wife's Phone without Touching Her Cell

By **Allen Johnson** - January 11, 2021 510 0

Spy On Android

The only Android spy app that captures all forms o

types o

— and

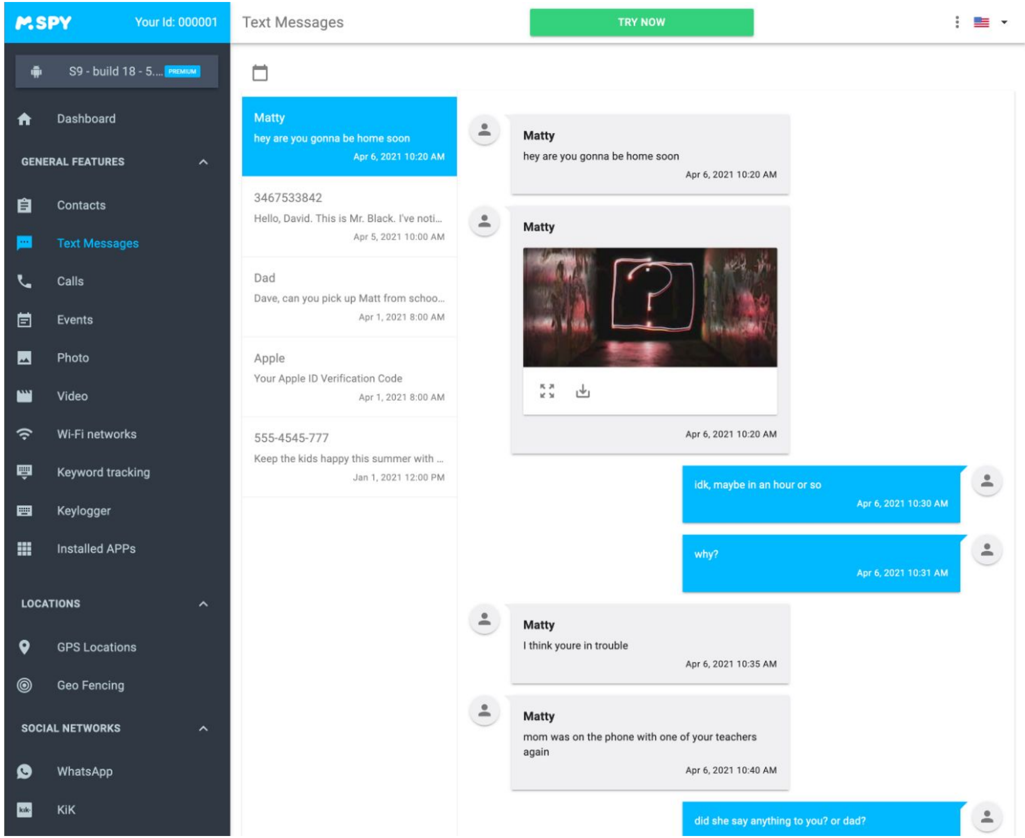
the mo

Androic

Will mSpy™ show on my credit card bill?

Depending on where you are located, the bank statement may or may not include the word 'mSpy'.

https://bit.ly/blackhatstalkerware



Matty
hey are you gonna be home soon
Apr 6, 2021 10:20 AM

3467533842
Hello, David. This is Mr. Black. I've noti...
Apr 5, 2021 10:00 AM

Dad
Dave, can you pick up Matt from schoo...
Apr 1, 2021 8:00 AM

Apple
Your Apple ID Verification Code
Apr 1, 2021 8:00 AM

555-4545-777
Keep the kids happy this summer with ...
Jan 1, 2021 12:00 PM

Matty
hey are you gonna be home soon
Apr 6, 2021 10:20 AM

Matty
Apr 6, 2021 10:20 AM

idk, maybe in an hour or so
Apr 6, 2021 10:30 AM

why?
Apr 6, 2021 10:31 AM

Matty
I think youre in trouble
Apr 6, 2021 10:35 AM

Matty
mom was on the phone with one of your teachers again
Apr 6, 2021 10:40 AM

did she say anything to you? or dad?

https://bit.ly/blackhatstalkerware

Stalkerware 101

Installed through **physical** access to **unlocked** device

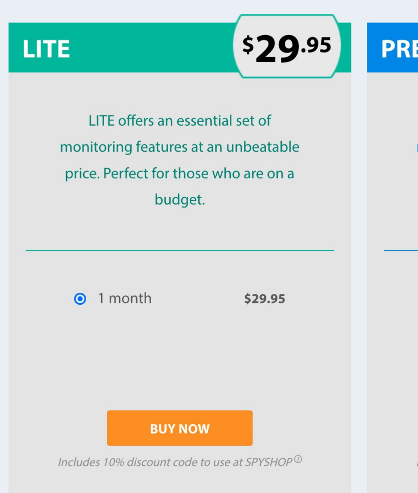
Requires no technical skills or cybercrime connections

Affordable (~US$25/month)

Technically not very advanced

Hidden on device

Can monitor a lot of activity (phone, browser, messages, location, etc.)



LITE $29.95

LITE offers an essential set of monitoring features at an unbeatable price. Perfect for those who are on a budget.

● 1 month $29.95

Includes 10% discount code to use at SPYSHOP

https://bit.ly/blackhatstalkerware

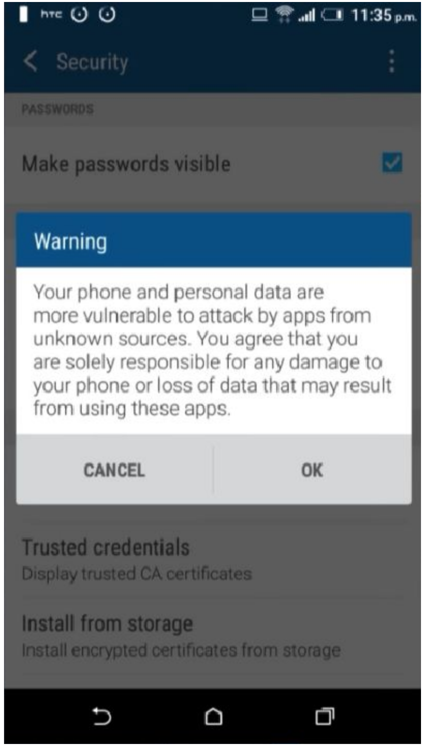
Stalkerware on Android

Stalkerware is most common on Android

Built-in security protections disabled during installation

Occasionally rooted for advanced functionality

Antivirus probably detects it



Warning

Your phone and personal data are more vulnerable to attack by apps from unknown sources. You agree that you are solely responsible for any damage to your phone or loss of data that may result from using these apps.

CANCEL
OK
Trusted credentials
Display trusted CA certificates
Install from storage
Install encrypted certificates from storage

https://bit.ly/blackhatstalkerware

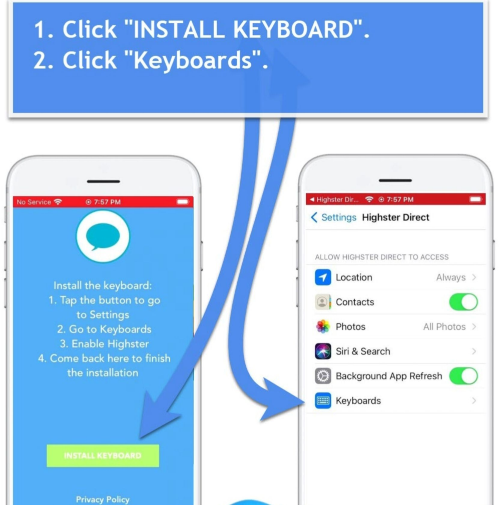
Stalkerware on iOS

Requires jailbreak so only possible on older and/or unpatched devices

Non-jailbreak “stalkerware” possibilities:

- iCloud sync
- iTunes sync
- Custom keyboard with built-in keylogger

Useful tools: Certo, iVerify



1. Click "INSTALL KEYBOARD".
2. Click "Keyboards".

Install the keyboard:
1. Tap the button to go to Settings
2. Go to Keyboards
3. Enable Highster
4. Come back here to finish the installation

ALLOW HIGHSTER DIRECT TO ACCESS

Location: Always
Contacts: on
Photos: All Photos
Siri & Search
Background App Refresh: on
Keyboards

https://bit.ly/blackhatstalkerware

Stalkerware on desktop

Exists, but less common

Device sharing more common for desktops and laptops

RATs have been used for IPV

Stalkerware: how to support someone?

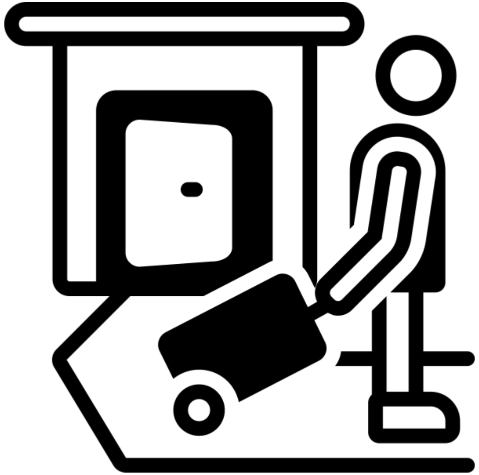
https://bit.ly/blackhatstalkerware

Not a technical problem

Removing stalkerware isn't always safe or desirable

Understand a survivor's threat model

Common prevention measures often aren't feasible



Don’t just focus on stalkerware

The first rule of stalkerware is that it probably isn’t stalkerware

Consider other kinds of tech abuse (or non-tech abuse!) as possible causes of surveillance

CETA resources and checklists can be very helpful!

Understand trauma

Survivors are often traumatized. This could lead to hyper-vigilance and having concerns that you believe aren’t well-founded.

This isn’t about you. And it’s okay for you to ask for help too!

Take survivors seriously and empower them

Stalkerware: what can we all do?

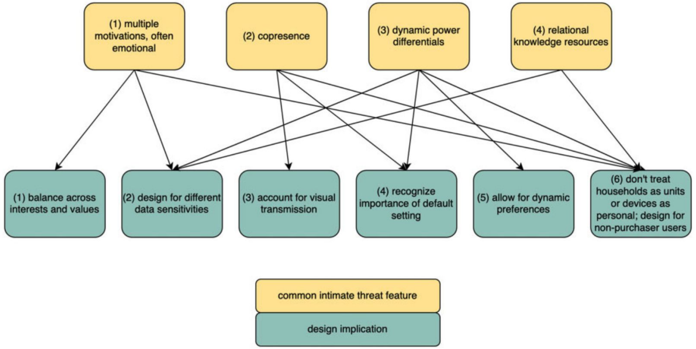
Consider the IPV threat model during product design

Resources:

Privacy Threats in Intimate Relationships (Karen Levy & Bruce Schneier)

Five Technology Design Principles to Combat Domestic Abuse (IBM)

The Inclusive Safety Project website


(1) multiple motivations, often emotional
(2) copresence
(3) dynamic power differentials
(4) relational knowledge resources
(1) balance across interests and values
(2) design for different data sensitivities
(3) account for visual transmission
(4) recognize importance of default setting
(5) allow for dynamic preferences
(6) don't treat households as units or devices as personal; design for non-purchaser users
common intimate threat feature
design implication

https://bit.ly/blackhatstalkerware

Build connections with IPV advocacy groups

You can learn from them. And maybe you can help them too!

Conclusion

Stalkerware is a part of tech abuse, which is a part of IPV

Stalkerware is powerful, affordable and available

It is a very real problem, but don’t ignore other kinds of tech abuse

Understand traumatized survivors. Understand this is not a tech problem

Consider the IPV threat in product design. Build connections!

https://bit.ly/blackhatstalkerware

Thank you!

Eva Galperin, Tara Hairston, NNEDV, WESNET, CETA, Certo Software and all those other people who work together to combat stalkerware, tech abuse and intimate partner violence.

And thank you for listening and caring!

Resources:

https://bit.ly/blackhatstalkerware