CamCop: Keeping Your Privacy Intact by Notifying You Whenever Your (Laptop) Camera is on!

Priyanka Bose, Sam Zierler

Home is supposed to be everyone’s safe space. But is it really “safe”? Almost everyday we hear news about someone’s laptop camera getting hacked and pictures of their intimate settings either being leaked, or them being blackmailed for ransom. Do you not want to be one of those people? Well why fear? CamCop is here. Read on to find out how our application can help keep you one step ahead of the hackers.

Introduction

As the world becomes increasingly interconnected, the threat of cyberbullying looms larger than ever before. From hurtful messages on social media to the theft of personal information, the digital age has opened up a new frontier for bullies to harass and intimidate their victims.

But perhaps the most insidious form of cyberbullying is the unauthorized access of someone's webcam. It's a violation of privacy that can leave people feeling vulnerable and exposed in the very places they should feel safest, like their bedrooms or private offices.

That's where CamCop comes in. With its cutting-edge technology, this innovative project sends an instant notification to your mobile device via Slack every time your laptop camera is turned on. With CamCop, you can rest easy knowing that you have an extra layer of protection against cyber criminals and the potential violation of your privacy.

No longer do you have to worry about hackers lurking in the shadows, waiting to take advantage of your vulnerability. CamCop is here to help you take back control and ensure that your digital life remains your own. So why wait? Sign up for CamCop today and experience the peace of mind that comes with knowing that you're always protected.

Motivation

In our IoT Security and Privacy class, Prof. Danny Huang provided us with research papers to read every week and at the end of the week, we would also discuss the paper in class. It was through these discussions that we were made aware of how bad and scary the problem of IPA: Interpersonal Abuse is.

Background Research

To understand the extent of the problem, we conducted our research about IPA and the following were our findings:

- 1 in 4 women and 1 in 7 men have experienced cyber stalking.
- 1 in 10 teens have been cyberbullied.
- 40% of teens who have been cyberbullied have considered suicide.
- 1 in 5 teens who have been cyberbullied have attempted suicide.

According to a study by the Pew Research Center [1], 41% of Americans have experienced some form of cyber interpersonal abuse. Of those who have experienced cyber interpersonal abuse, 25% have experienced it from an intimate partner.

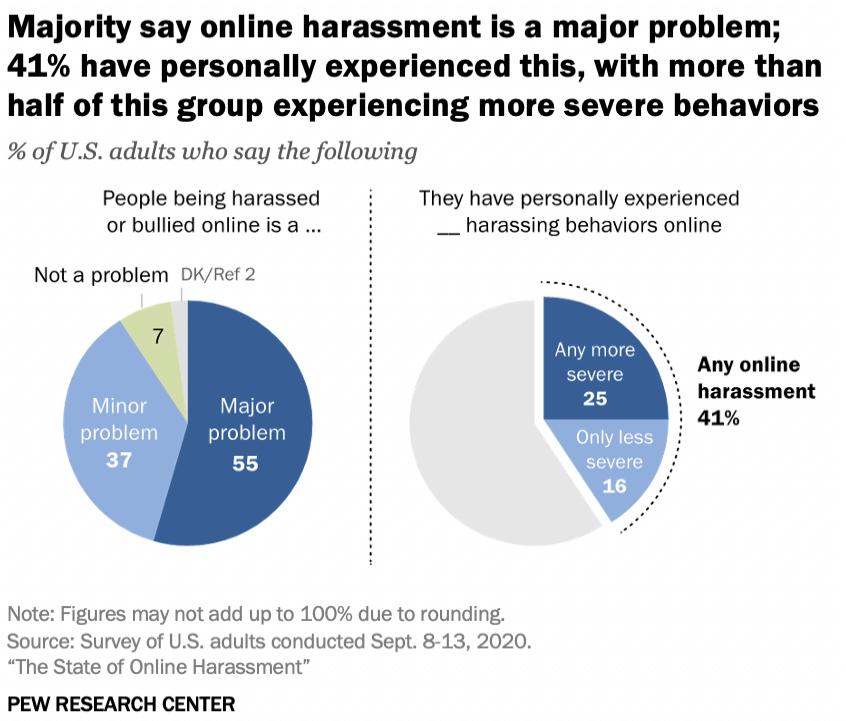


Figure 1 – Survey results of Adults in the US for online harassment according to the study by Pew Research Center.

Additionally we found several news reports about actual instances of spying and abuse using webcams and malware called Remote Administration Tools or Remote Access Trojans (RATs). In some cases this software was installed legitimately and misused by administrators while in other cases it infected remote computers through malicious means [19, 20, 21, 22, 23].

So we decided to create a solution that can help with reducing this form of bullying: the fast growing and more critical than ever Cyber bullying. And IPA is the worst form of cyberbullying, in our opinion, as the hacker uses intimate personal information to threaten their partners. We

found that Cyber IPA is the use of technology to harass, threaten, or control another person. It can take many forms, including:

1. Using technology to track someone's movements and actions
2. Sending unwanted messages or emails
3. Posting embarrassing or humiliating photos or videos online
4. Spreading rumors or lies online
5. Hacking into someone's social media accounts
6. Using technology to control someone's access to money or resources

Hence, we started working on CamCop, as we found that cameras getting hacked is not a rarity. In 2020, there were an estimated 10 million webcam hacking incidents worldwide. And, an average laptop camera is hacked once every 18 months. Hackers can use webcams to spy on people, steal their personal information, and eventually blackmail them.

Then, we outlined our idea: we knew here that we were going to build an application that would notify users as soon as their camera laptop turned on. This would allow them to take appropriate measures as soon as possible. Then, we worked with Danny to understand and expand the scope of our project and fine tune our idea.

Method

We use the basic idea that every process that runs on your laptop can be accessed from the terminal or the command line. With this in mind, first we decided on what operating systems we wanted to work with.

Device Selection

For our project we chose to work with macOS and Windows. We did this because most of the people we talk to everyday, irrespective of their background, usually use one of these two. In our research we also found that, as of April 2023, Windows is the most used operating system on laptops, with a market share of 69%. macOS is the second most popular operating system, with a market share of 17%. Chrome OS is the third most popular operating system, with a market share of 3.2%. Linux is the fourth most popular operating system, with a market share of 2.9%.

Here is a breakdown of the market share of the top 5 operating systems on laptops:

Operating System	Market Share
Windows	69%
macOS	17%
Chrome OS	3.2%
Linux	2.9%
Other	8%

Figure 2 – Market share of operating systems for laptops. [4]

So we focused our efforts on developing solutions for users of these platforms, primarily.

Application Development

For the scanning functionality of CamCop, we employed native logging tools provided by both the macOS and Windows operating systems. This approach was inspired by a similar technique utilized by Oversight, a third-party application for macOS that monitors for microphone and camera events [2]. To identify our logger conditions, we collected an unfiltered session of system logs during which we activated several camera applications. These logs were scanned for relevant events and the content was used to test various iterations of the filter. We also included details like device name, collected from system applications like *device manager* or *system profiler*.

```
log stream
  --predicate 'subsystem=="com.apple.cmio"'
  --predicate 'sender contains "appleh13camerad"'
  --predicate 'composedMessage contains "CMIOExtensionProperty"'
```

Figure 3 – Some examples of filter properties tested for detecting camera events.

When the user launches CamCop, the application will first deploy python to the system if it is not previously installed, as this is an underlying requirement for triggering our response actions. If an event occurs while CamCop is running, a script file is called to generate the notification. The file is passed along the event log contents from which it can determine the state change and application name that caused the activation. To provide a more informative alert, these details are embedded in the message sent to the user's device.

```
os_ = sys.platform
# on mac
pid = sys.argv[6]
process_info = subprocess.run('ps -p ' + pid, stdout=subprocess.PIPE, shell=True)
app_ = ' '.join(sys.argv[8:])
```

Figure 4 – The script file inside CamCop can parse information from the event log contents and make a system call to identify the responsible application from its process id (PID).

We designed CamCop to support two methods of delivery for the mobile alerts. During development we used Pushover [3], which relies on an established connection between your phone and their notification services. This was suitable for our purposes, however they limit users to a 30-day trial period before requiring a paid subscription. For our user testing we also created a Slack workspace where notifications were aggregated to expedite the demonstration of CamCop.

The source code for CamCop is open source and can be found at this Github link.

User Testing Framework

Once the development was done, we wanted to test our application out. For this, we wanted to talk to people who were from different backgrounds – technical as well as non-technical. For the non-technical background, we talked to people who are from different schools with NYU - like from NYU SPS, NYU Steinhardt, NYU Wagner, etc. This included people who hadn't used command line tools before. It was while working with them that we realized that our code should handle the Python installation as well – since none of them had it previously installed. In total we tested with six participants.

The general process for each session was to:

1. Configure the user's machine (if necessary)
2. Download and run CamCop files
3. Interact with "camera" applications to try and trigger events
4. Conduct post-interaction survey where we asked several open-ended questions;
    a. Are you aware of the problem we are trying to address?
    b. What does security and privacy mean to you?
    c. Do you think this solution (CamCop) might be helpful?
    d. Do you have suggestions for alternative solutions?

Results

Development Testing

From our development testing we found a significant difference in our ability to successfully capture camera events across macOS and Windows. Specifically, with macOS, all ten of our tested applications triggered calls to the same subsystem, meaning they were captured by our listener filter and triggered a mobile alert. Windows was far less reliable, only managing to capture events stemming from the native Camera application. We tried filtering with a variety of related strings and found no improvement or new events discovered. We believe this is due to how the Windows operating system implemented its own system logger, which CamCop relies on for functionality.

What applications did we test?

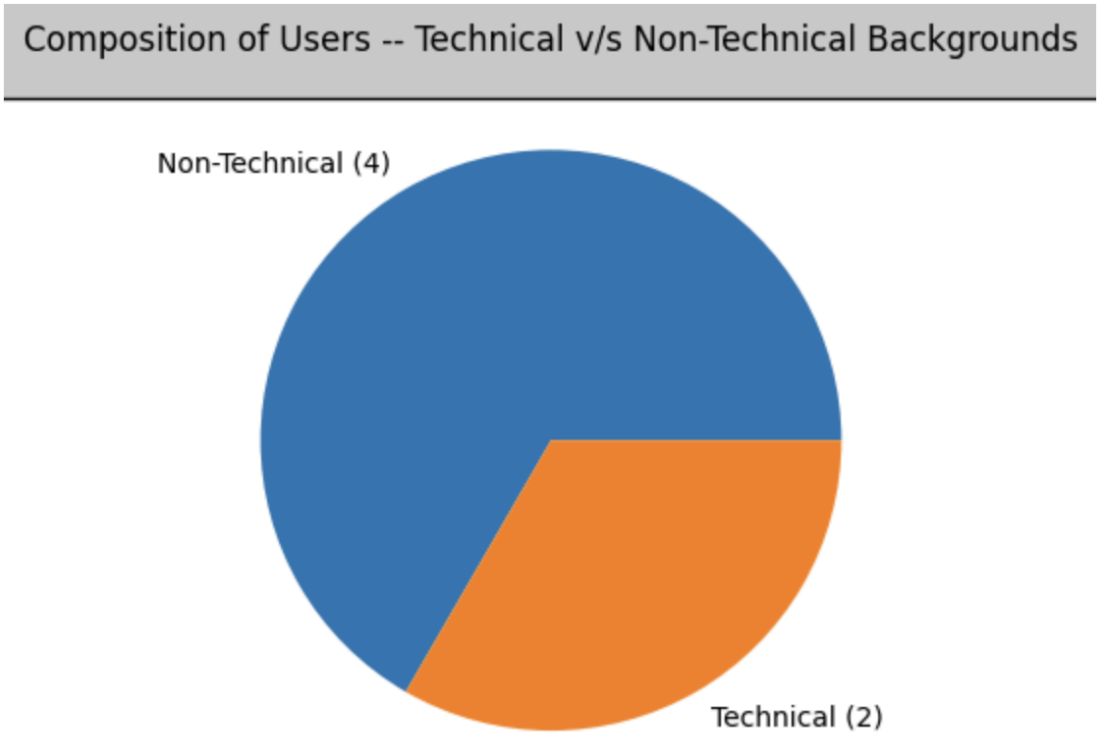
✔ application successfully triggered CamCop; ✘ application failed to trigger CamCop; – not tested on operating system

Application	macOS (10/10)	Windows (3/9)
FaceTime	✔	–
PhotoBooth	✔	–
Camera	–	✔
“Settings”	–	✘
Firefox	✔	✘
Chrome	✔	✘
Safari	✔	–
Discord	✔	✘
Zoom	✔	✘
Microsoft Teams	✔	✘
Quicktime Player	✔	–
Terminal	✔	–
Cmd	–	✔
Powershell	–	✔

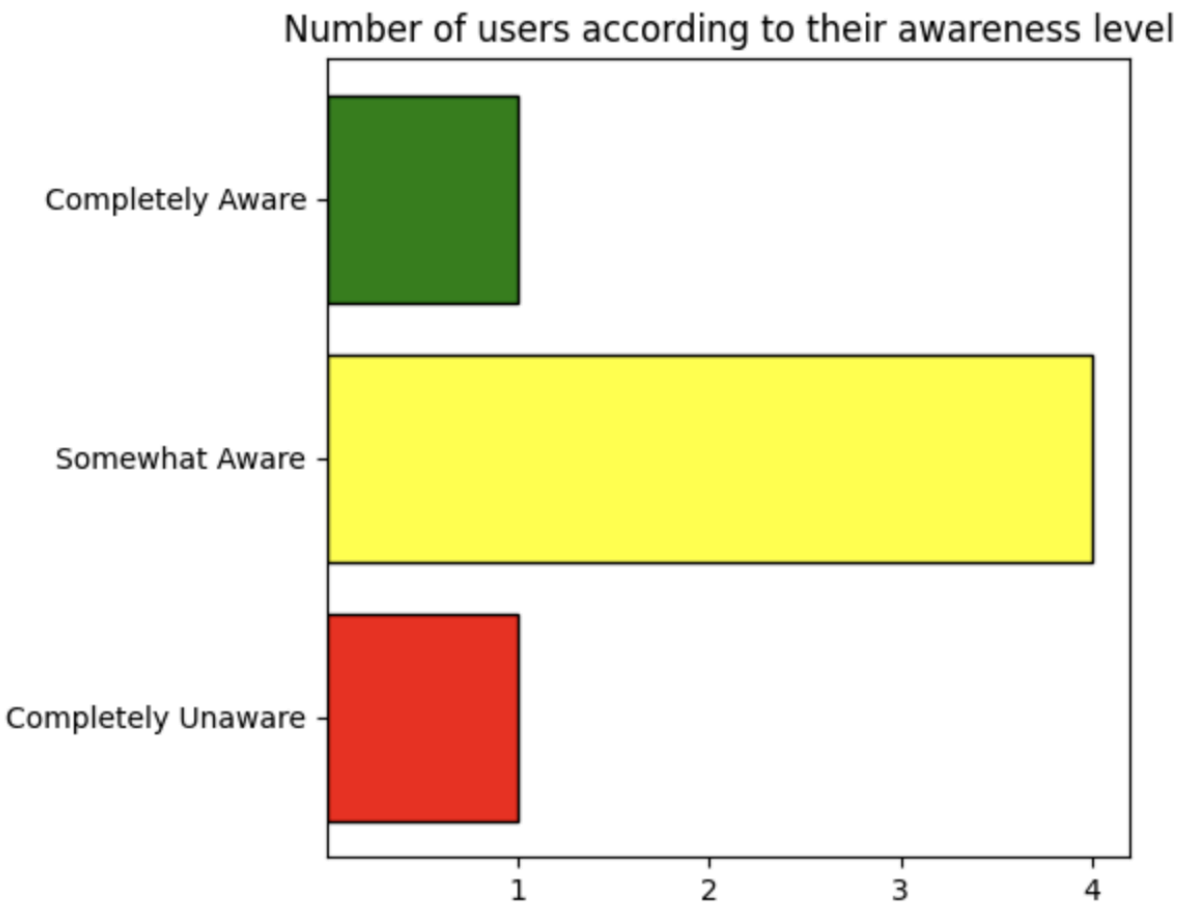
User Testing

Before we get on to the details of our user testing details, we wanted to present some caveats that the user must keep in mind before fully absorbing the results as presented. Since we had about a week to put towards our testing efforts, we reached out to close friends. We did 6 interviews, between the both of us. Hence, we wanted to point out that there might be potential bias involved.

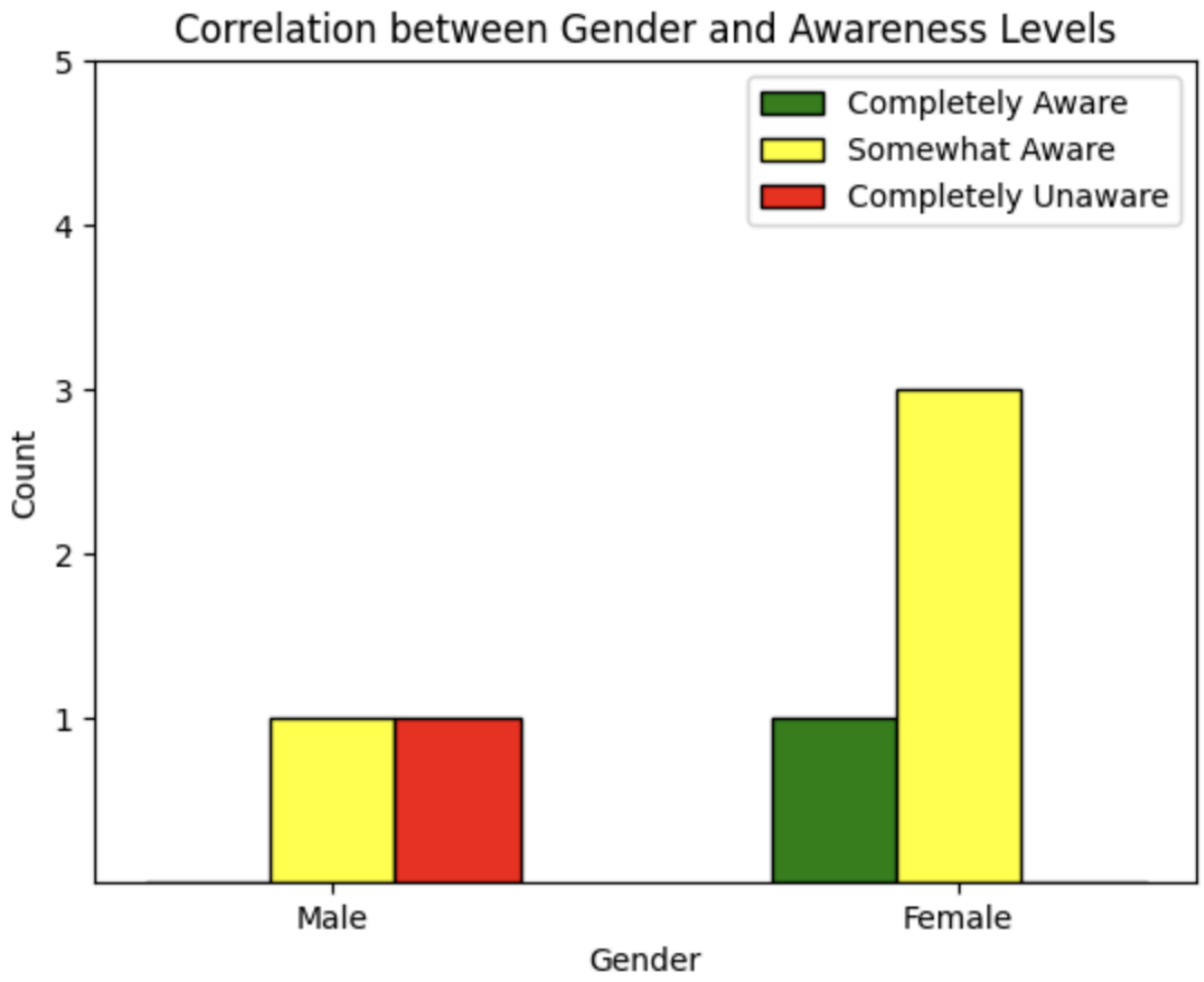
We wanted to make sure that our users came from diverse backgrounds. The composition of our user group is summarized in the pie chart below:



We also wanted to understand if our users were actually aware of Webcam hacking being an issue in the real world. Based on the answers we received from all of them, we were able to categorize them in the following 3 categories:



We also observed a trend between the users' gender as well as their awareness level in terms of this privacy breach issue:



We noticed that women in our dataset in general had more awareness of this issue, as compared to their male counterparts. However, we need a bigger dataset to confirm our findings.

In general, with respect to CamCop, our user testing experience yielded several key takeaways. More than half the participants indicated that they were not aware of the problem presented. This is concerning as related studies have demonstrated the prevalence of webcam attacks and the consequences of personal data exposure. Encouragingly, all six users expressed interest in CamCop as a tool and believed it could operate as an effective solution. Positive features mentioned by testers included, "*ease of deployment*", "*hands-off monitoring*", and "*real-time updates*."

Related Work

Previous work regarding webcam vulnerabilities has been conducted in both the academic and professional security space. Some studies have looked broadly; performing a global assessment of exposed devices through Shodan [6], or conducting an awareness study

supported by real world examples of abuse [7]. Others have focused on specific devices, running exhaustive testing to discover potential issues. Brocker and Checkoway exhibited a method for disabling the indicator light of Macbook iSight cameras [12]. Bondi et al. showed how a motion sensing from an IP camera could be abused to track a victim's movements [13]. Work from security and cyber research firms have uncovered major data leaks in the past, typically relating to unsecured databases of user information [14, 15, 16]. Popular video conferencing applications like Zoom and Microsoft Teams have also been found to have exploitable weaknesses that could jeopardize user's privacy [17, 18].

Bug researcher Ryan Pickren has twice identified vulnerabilities in macOS that allowed attackers to take control of a user's webcam through a seemingly innocuous website or image link. While his threat methods have since been patched, the work highlights the ability for malicious actors to disguise their intent behind common interactions [10, 11].

Through google searches we found a number of articles and blog posts that make recommendations for users interested in protecting themselves and their webcams. These tended to include common sense behaviors like using antivirus software, not visiting unsafe websites, and purchasing camera covers [8, 9].

Future Work

There are several limitations to our project that could be addressed in future work.

Windows Event Discovery Failures – The results of our development testing on Windows were disappointing and the inability to discover any additional sources of microphone or camera related events in the system logs means that this state of CamCop cannot deliver equal support across both operating systems. Despite our efforts to find relevant sources for filtering and to replicate the registry entry technique described by Zachary Stanford, [5] we could not improve our detection results. An alternative approach for future work could be to try and decompile any of the advertised software tools online that claim to monitor Windows media devices, or to investigate how Windows triggers its on-screen delivery (OSD) notifications for webcam events.

Mobile Notification Delivery Methods – We tested two means for sending notifications to users of CamCop. Pushover has the convenience of linking uniquely with your phone, maintaining greater privacy, however it has an initial barrier of setup and a limited trial period of 30 days. Slack is a free service, however the testing workspace is shared by all users that join it. A solution might be to integrate the generation of a custom slack workspace when CamCop is first initialized, thereby creating a private environment for users to receive their notifications.

Further User Testing – Our user survey had only open ended questions to assess general sentiment on the experience and therefore is difficult to quantify into results. If we were to conduct further testing, it would be ideal to include some other forms of questions, such as using a Likert scale.
Also, we would want to recruit more folks who weren't friends or family members to try out

CamCop. More diversity would be required in the user group to get a better understanding of CamCop's impact.

References

[1] Duggan, M., Rainie, L., & Smith, A. (2021, January 13). The state of online harassment. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

[2] "OverSight" Objective-See, https://objective-see.org/products/oversight.html

[3] Pushover, https://pushover.net/

[4] Desktop Operating System Market Share Worldwide - April 2023, "https://gs.statcounter.com/os-market-share/desktop/worldwide"

[5] Z. Stanford, "Can you track processes accessing the camera and microphone on Windows 10?," DFIR Review, https://dfir.pubpub.org/pub/nm5b39ae/release/1

[6] J. Bugeja, D. Jönsson, and A. Jacobsson, "An Investigation of Vulnerabilities in Smart Connected Cameras," in 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2018, pp. 656–661. https://www.diva-portal.org/smash/get/diva2:1409755/FULLTEXT01.pdf

[7] Jones, A. & Gagneja, Kanwalinder. (2016). Preventing Covert Webcam Hacking in the Civilian and Governmental Sectors. 993-998. 10.1109/CSCI.2016.0190. https://courses.csail.mit.edu/6.857/2014/files/03-jayaram-lui-nguyen-zakarian-preventing-covert-webcam-hacking

[8] H. Staff, "How to tell if your Mac camera has been hacked (2023)," HowToiSolve, https://www.howtoisolve.com/how-to-tell-if-your-mac-camera-has-been-hacked/

[9] David Cook, "Hackers can access your mobile and laptop cameras and record you – cover them up now," The Conversation, https://theconversation.com/hackers-can-access-your-mobile-and-laptop-cameras-and-record-you-cover-them-up-now-135933

[10] "Webcam Hacking ," Ryan Pickren, https://www.ryanpickren.com/webcam-hacking

[11] "Hacking the Apple Webcam (again) ," Ryan Pickren, https://www.ryanpickren.com/safari-uxss

[12] M. Brocker and S. Checkoway, "Iseeyou: Disabling the MacBook webcam indicator led," JScholarship Home, https://jscholarship.library.jhu.edu/handle/1774.2/36569

[13] P. Biondi, S. Bognanni and G. Bella, "Vulnerability Assessment and Penetration Testing on IP camera," *2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, Gandia, Spain, 2021, pp. 1-8, doi: 10.1109/IOTSMS53705.2021.9704890. https://ieeexplore.ieee.org/document/9704890

[14] *Adorcam leaks thousands of webcam accounts*. RedPacket Security. (2021, February 15). https://www.redpacketsecurity.com/adorcam-leaks-thousands-of-webcam-accounts/

[15] Cyber Research Team. (2019, September 16). *Risk: Is this your webcam? you're being watched*. WizCase. https://www.wizcase.com/blog/webcam-security-research/

[16] Palmer, D. (2021, August 17). *Critical IOT security camera vulnerability allows attackers to remotely watch live video - and gain access to networks*. ZDNET. https://www.zdnet.com/article/critical-iot-security-camera-vulnerability-allows-attackers-to-remotely-watch-live-video-and-gain-access-to-networks/

[17] A. Chailytko, "Zoom-zoom: We are watching you," Check Point Research, https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/

[18] P. Tavares, "Hacking microsoft teams vulnerabilities: A step-by-step guide," Infosec Resources, https://resources.infosecinstitute.com/topic/hacking-microsoft-teams-vulnerabilities-a-step-by-step-guide/

[19] C. Moss, "Hacker who 'sextorted' miss Teen USA gets 18 months in prison," Business Insider, https://www.businessinsider.com/jared-james-abrahams-gets-18-months-in-prison-2014-3

[20] M. Plummer, "California Computer Technician Trevor Harwell Suspected of Spying on Women," ABC News, https://abcnews.go.com/US/california-computer-technician-trevor-harwell-suspected-spying-women/story?id=13806697

[21] "LMSD: Initial LANREV system findings," Scribd, https://www.scribd.com/doc/30891576/LMSD-Initial-LANrev-System-findings

[22] N. Bilton, "Rented computers captured customers having sex, F.T.C. says," The New York Times, https://archive.nytimes.com/bits.blogs.nytimes.com/2012/09/26/rented-computers-captured-customers-having-sex-f-t-c-says/

[23] N. Anderson, "Meet the men who spy on women through their webcams," Ars Technica, https://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/