

HOLY ANGEL UNIVERSITY

Final Requirement

Technology and Human Rights: Rise of Cybercrimes in the Philippines

An ADWEB Final Performance Task
Presented to The Faculty of the
School of Computing



In Partial Fulfillment
of the Requirements for the Course
Advanced Dynamic Web Applications (6ADWEB)

Myra P. Cuyagbo
Jarell Carlo D. Galura
Hans Benedict V. Jardiel
Deidrey Simon Paul L. Mandani
Almond L. Rosos

May 2022

HOLY ANGEL UNIVERSITY**Table of Contents**

	Page
Cover Page	i
Table of Contents	ii
I. Background	1
II. Problems/Issues	1
III. Objectives.....	2
IV. Members and Roles.....	2
V. Mockup Interface Design	3
VI. Final Version of the Web Application.....	8
 References	 15

HOLY ANGEL UNIVERSITY**BACKGROUND**

The Internet has been a common ground for present-day criminals to utilize as a means to mobilize their malicious intentions, otherwise known as cybercrimes. Cybercrimes are illegal activities done using computers or the Internet. Their actors, known as cybercriminals, use different techniques to carry out their crimes, such as phishing, social engineering, and malware as part of their cyber attacks (Latto, 2022). One thing that people should know about such crimes is that they are not happening randomly at a time, cybercriminals are very intelligent, organized, and so professionalized which makes them more dangerous (Latto, 2022). As technology evolves, so do the cybercrimes that happen on the Internet. Cybercriminals have countless creative ways to attack their victims which is why Internet users have a duty and responsibility to stay informed and aware of such crimes to prevent their emergence. According to Carter (n.d.), the most common computer and internet cybercrimes in America include phishing, harassment, ransomware, prostitution, child pornography and solicitation, intellectual property theft, account hacking, drug trafficking, and credit card fraud. Seemingly, the situation on the said country does not fall far behind from the Philippines, and the situation remains alarming even when there is a law enacted to address and penalize cybercrimes (R.A. 10175 or the Cybercrime Prevention Act of 2012).

PROBLEMS/ISSUES

To reinstate, cybercrimes are still a lingering problem in the Philippines at present. Years have passed since the Cybercrime Prevention Act and the Anti-Bullying Act (which covers cyberbullying) were enacted but the problem stays just the same. According to Statista (2021), Region 3 or Central Luzon took the highest number of victims of fraudulent SMS or text scams in 2019, that amounts to approximately 3.4 million individuals. Other cybercrimes noted on the list involved hacking, phishing, and cyberbullying. A report from CNN in 2020 showed that 37% of the top cybercrimes in 2020 were related to online scams. Online libel and cyberbullying were also among the top cybercrimes in the year 2020 and out of 5 cybercrimes that happened, 3 of which are related to cyberbullying (Sonnie, 2022). Given the context, there



HOLY ANGEL UNIVERSITY

really is a need to address the issues on the continuing emergence of cybercrimes here in the country, and it is crucial for the citizens to be aware of such crimes to prevent further damages. Hence, the project addresses the cybercrimes covered by the Cybercrime Prevention Act of 2012, as well as cyberbullying, which are pertinent issues in the Philippine online setting.

OBJECTIVES

The project aims to address the issues on the emergence of the different cybercrimes and instill awareness to the users on how to be vigilant and prevent becoming a victim of such. It will contain necessary information about the root causes and adverse effects of such crimes and the ways on how people should act as a responsible netizen and how to take care of their online profile/identities. The project also focuses on the development of essential skills using Angular that future web developers like us should possess to advance in our chosen careers.

MEMBERS AND ROLES

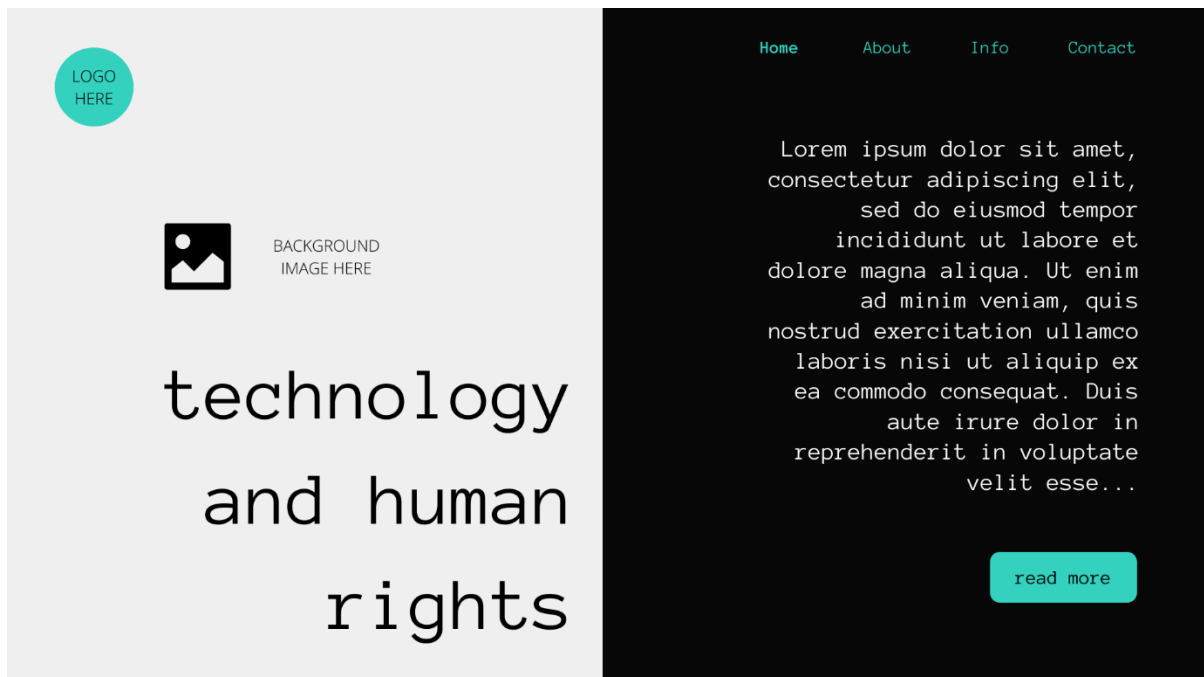
Member	Role
Myra Cuyagbo	Developer, Introduction
Jarell Carlo Galura	Developer, Problems/Issues
Hans Benedict Jardiel	Developer, Researcher, Objectives
Deidrey Simon Paul Mandani	Developer, Researcher, Objectives
Almond Rosos	Project Manager, Introduction, Problems/Issues

HOLY ANGEL UNIVERSITY

MOCKUP INTERFACE DESIGN

For this project, the group has decided to include four pages as the main navigation for the users, and they are the HOME page, ABOUT page, INFO page, and CONTACT page. Screenshots of the design of each page are provided below along with their descriptions. (*Note: the names of the pages are subject to changes until the finalization of the design.*)

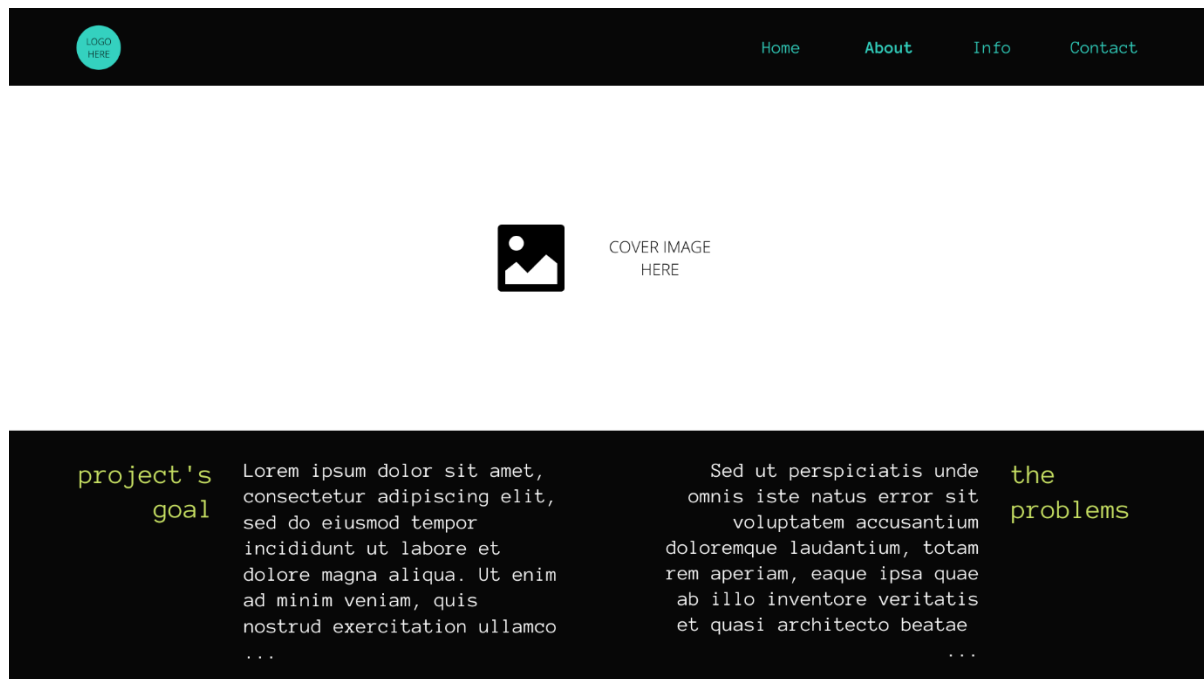
- **Home page**



The home page of the project is straightforward in terms of design language. It consists of the site logo, a cover image, site title, the navigation bar, and a featured text which contains an overview of the site content. The group is yet to decide whether the home page would be a single page with no scrollable content or not. For the sake of the mockup design, we put a button below the featured text to signify that there will be more content for the viewers and users to see/read.

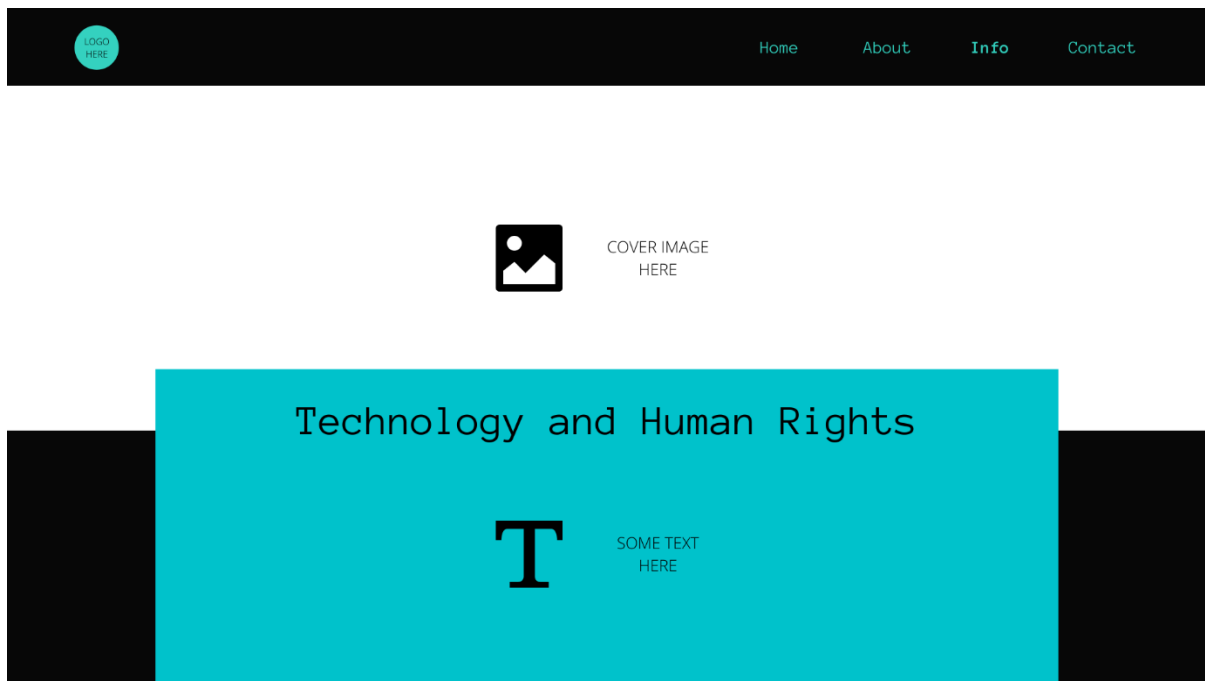
HOLY ANGEL UNIVERSITY

- About page

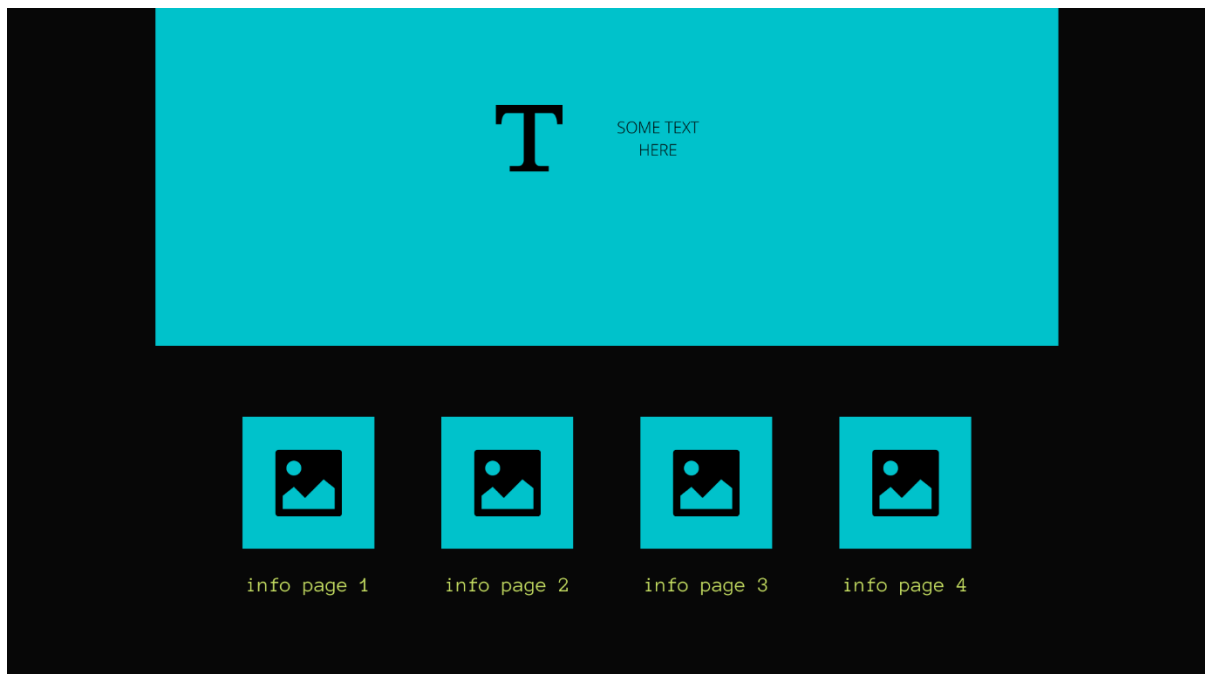


This page will contain the necessary information about the project, its goals, and the people behind the team. The initial design contains a header cover image and other contents such as the project's goal and the issues to be tackled. More content will be revealed in the final stage of the project design.

- Info page



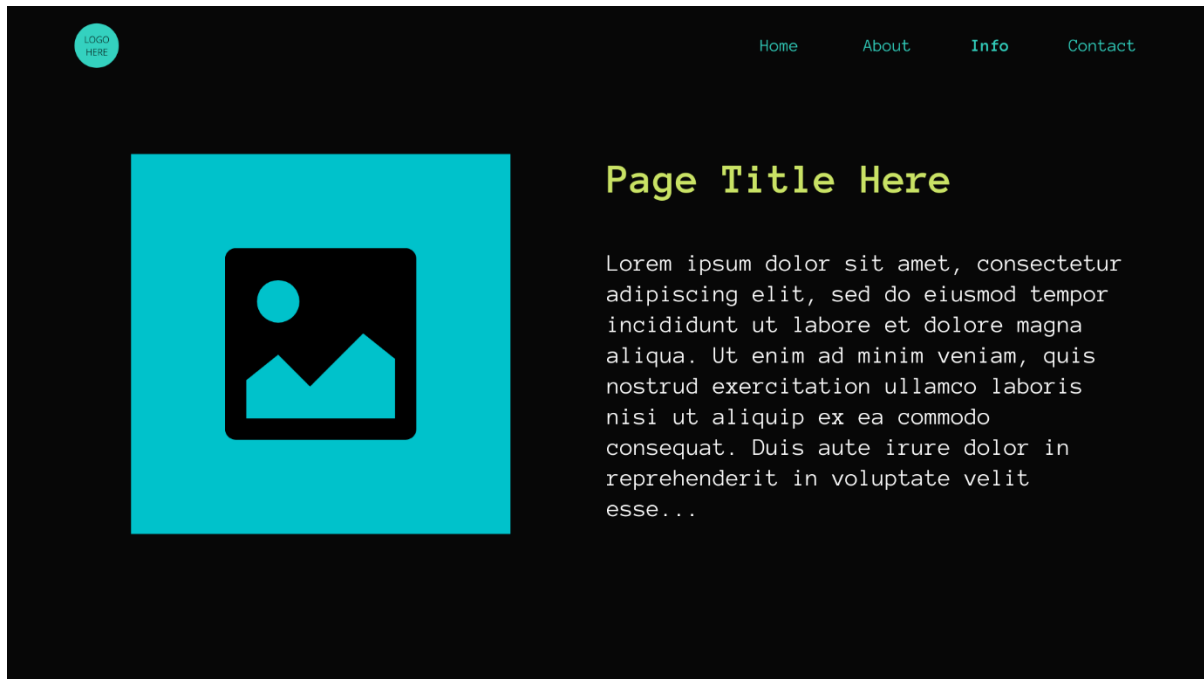
The information page also contains a header cover image, and text card containing the summary/overview of what our advocacy about technology and human rights would be all about.



HOLY ANGEL UNIVERSITY

Below the text card would be a collection of thumbnails that are linked to other external pages with necessary information about the different cybercrimes and laws in the Philippines. More content will be revealed on the final stage of the project design.

- **Sub page for the info page**



This is how the external pages would look like once the users click the thumbnails seen on the information page. It is also simple and contains information about the page.

HOLY ANGEL UNIVERSITY

- **Contact page**

The last main page for the project would be the contact page. It is also simple like the other pages, containing a contact form which users can fill in to reach out to the site owners and creators regarding their concerns. We also plan on providing a footer on each page that contains necessary contact information.

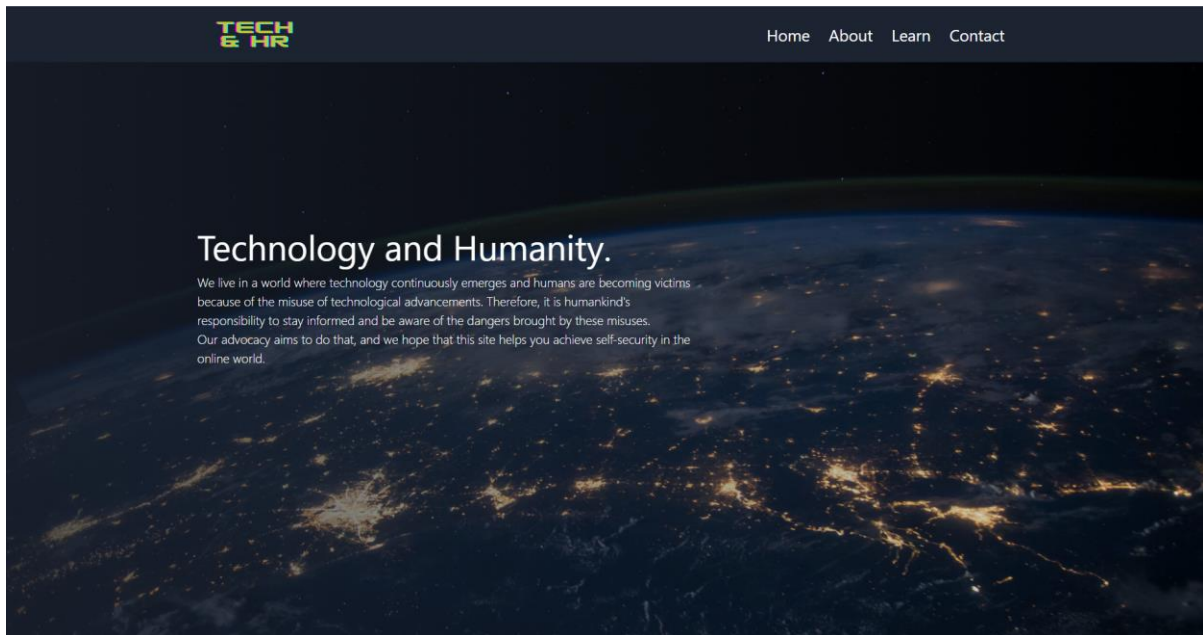
Lastly, we would also like to note that the colors and fonts used on this mockup design are subject to changes depending on what the final consensus would be within the group. To clarify, we chose colors and fonts that we thought would represent technology the most. As for the layout, we opted for a very minimalistic and simple yet intuitive design so that users would get the best information rather than focus on aesthetics and visuals. Of course, there will be other design changes depending on feedbacks and comments that will add more sophistication and appeal to the project's overall look.

HOLY ANGEL UNIVERSITY

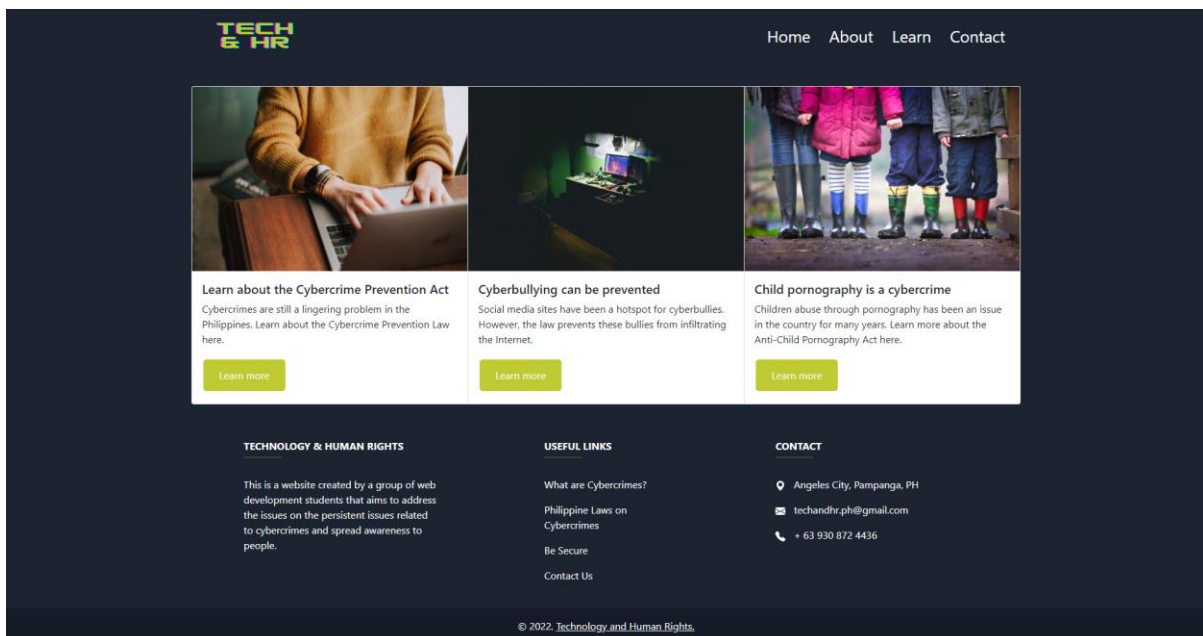
FINAL VERSION OF THE WEB APPLICATION

Here are the screenshots of the final version of our web application:

- **Home page**



- **Footer**



HOLY ANGEL UNIVERSITY

- About page


[Home](#) [About](#) [Learn](#) [Contact](#)




PROJECT'S GOAL

The Internet has been a common ground for present-day criminals to utilize as a means to mobilize their malicious intentions, otherwise known as cybercrimes. Cybercrimes are illegal activities done using computers or the Internet. Their victims – Internet users – have been severely

THE PROBLEMS


Cybercrimes are still a lingering problem in the Philippines at present. Years have passed since the Cybercrime Prevention Act and the Anti-Bullying Act (which covers cyberbullying) were enacted but the problem stays just the same. According to Statista (2020), around 3.7 million Filipinos reported


[Home](#) [About](#) [Learn](#) [Contact](#)

causes and adverse effects of such crimes and the ways on how people should act as a responsible netizen and how to take care of their online profile/identities. The project also focuses on the development of essential skills using Angular that future web developers like us should possess to advance in our chosen careers.


continuing emergence of cybercrimes here in the country, and it is crucial for the citizens to be aware of such crimes to prevent further damages. Hence, the project addresses the cybercrimes covered by the Cybercrime Prevention Act of 2012, as well as cyberbullying, which are pertinent issues in the Philippine online setting.

MEET THE TEAM




Almond Rosos
Project Manager

[f](#) [t](#)




Myra Cuyagbo
Developer, Researcher

[f](#) [t](#)




Jarell Galura
Lead Programmer

[f](#) [t](#)



Hans Jardiel
Researcher

[f](#) [t](#)

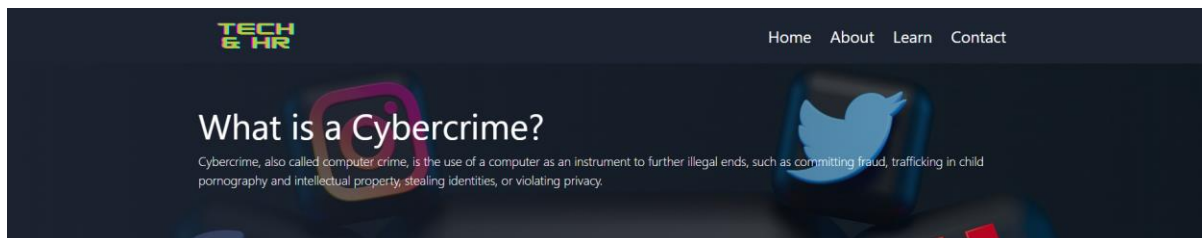


Drey Mandani
Researcher

[f](#) [t](#)

HOLY ANGEL UNIVERSITY

- Learn subpage 1 (What are cybercrimes page)



DIFFERENT TYPES OF CYBERCRIME



Phishing

Cybercriminals use phishing as a social engineering approach to mislead unsuspecting victims into installing harmful software or visiting malicious websites. Phishing attacks are most conducted by email, however other methods such as Vishing (Voice Phishing) and Smishing can also be performed (SMS Phishing).

Phishing's main purpose is to collect sensitive information in some way or another, by whatever means possible. Phishing is the most common sort of internet crime, according to 2019 FBI research, with over 114,000 victims in the United States, costing them a total of \$57.8 million. One of the main reasons why phishing is so popular is because it does not require any special tools or skills to launch a basic campaign.

How does phishing attack happen?



Identity Theft

Identity theft happens when criminals use the personal information of a victim to perform crimes. A thief assumes the victim's identity and engages in a variety of fraudulent acts in their name using the stolen information. Identity theft is committed by cyber criminals utilizing sophisticated cyber assault strategies such as social engineering, phishing, and malware. Criminals can take mail, crawl through dumpsters, and listen in on phone conversations in public locations, all of which can result in identity theft.

Many cyber-attacks aim to steal enough information about a victim to assume their identity and commit fraud on their behalf. Unfortunately, most people don't realize they've been a victim of identity theft until they try to establish a bank account, apply for a job, get a collection call, or seek a new credit card.

How does identity theft happen?

Identity thieves have gotten more sophisticated in their methods. The following includes some of the ways identity theft may happen:

- Steal wallets or purses in order to obtain identification, credit and bank cards
- Dig through mail and trash in search of bank and credit card statements, preapproved credit card offers, tax information and other documents that may contain personal details
- Fill out change-of-address forms to forward mail, which generally contains personal and financial information
- Buy personal information from an inside, third party source, such as a company employee who has access to applications for credit
- Obtain personnel records from a victim's place of employment
- "Skim" information from an ATM — this is done through an electronic device, which is attached to the ATM, that can steal the information stored on a credit or debit card's magnetic strip
- Swipe personal information that has been shared on unsecured websites or public Wi-Fi
- Steal electronic records through a data breach

HOLY ANGEL UNIVERSITY


- Learn subpage 2 (Philippine cybercrime laws page)


Home About Learn Contact




PHILIPPINE CYBERCRIME PREVENTION LAWS

The Philippine Congress enacted Republic Act No. 10175 or "Cybercrime Prevention Act of 2012", the pinnacle of cybercrime prevention laws in the Philippines, which addresses crimes committed against and through computer systems. It includes penal substantive rules, procedural rules, and rules on international cooperation. The


Home About Learn Contact


Other than R.A. 10175, there are also other laws that address cybercrimes in the Philippines, and these are the Anti-Bullying Act of 2013 (which addresses cyberbullying in its provisions) and the Anti-Child Pornography Act of 2009. To know more about these laws, click on the links below which provide the excerpts of each law: punishable acts and sanctions for the crimes violated by the cybercriminal.



**Cybercrime Prevention Act
(R.A. 10175)**

*An excerpt of the Cybercrime Prevention Act from
[Official Gazette PH](#)*


[Read Article](#)



**Anti-Bullying Act
(R.A. 10627)**

*An excerpt of the Anti-Bullying Act in relation to
cyberbullying from [Official Gazette PH](#)*

[Read Article](#)



**Anti-Child Pornography Act
(R.A. 9775)**

*An excerpt of the Anti-Child Pornography Act from
[LawPhil.net](#)*

[Read Article](#)

HOLY ANGEL UNIVERSITY

○ Cybercrime Prevention Act page



Click on each section to learn more.

Section 1. Title.	^
This Act shall be known as the "Cybercrime Prevention Act of 2012".	
Section 2. Declaration of Policy.	▼
Section 3. Definition of Terms.	▼
The Key Provisions of the Cybercrime Prevention Act of 2012	▼
Penalties	▼

OTHER LAWS

○ Anti-Bullying Act page



Click on each section to learn more.

Section 1. Short Title.	^
This Act shall be known as the "Anti-Bullying Act of 2013".	
Section 2. Acts of Bullying.	▼
Section 3. Adoption of Anti-Bullying Policies.	▼

OTHER LAWS

HOLY ANGEL UNIVERSITY

○ Anti-Child Pornography page



Click on each section to learn more.

Section 1. Short Title.	^
This Act shall be known as the "Anti-Child Pornography Act of 2009."	
Section 2. Declaration of Policy.	▼
Section 3. Definition of Terms.	▼
Section 15. Penalties and Sanctions.	▼

OTHER LAWS


• Learn subpage 3 (Be secure page)



TIPS ON HOW TO PREVENT BEING A VICTIM OF CYBERCRIMES

Keep your software updated	^
This is especially critical when it comes to operating systems and internet security software. To obtain access to your machine, cybercriminals usually employ known vulnerabilities, or software faults. Patching such vulnerabilities and holes might reduce your chances of being a target for cybercrime.	
Use a full-service internet security suite	▼
Know that identity theft can happen anywhere	▼
Take measures to help protect yourself against identity theft	▼
Opt-Out of Credit Card and Insurance Offers	▼
Secure your Internet connection	▼

HOLY ANGEL UNIVERSITY


[Home](#) [About](#) [Learn](#) [Contact](#)

THINGS TO DO WHEN YOU BECOME A VICTIM OF CYBERCRIME

1. If you suspect you've been a victim of cybercrime, you should contact your local police department, as well as the NBI in some circumstances. Even if the offense appears small, this is critical. Your report might help authorities with their investigations or prevent crooks from exploiting other individuals in the future. If you believe your identity has been stolen by cybercriminals. These are some of the measures you should think about.
2. Make contact with the firms and banks where you suspect fraud.
3. Place fraud alerts and get your credit reports.
4. Report identity theft local or national authorities.
5. Disconnect and Detach
6. Take Legal Action

References:

- <https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html>
- <https://cybersecurity.att.com/blogs/security-essentials/how-to-avoid-becoming-a-victim-of-cybercrime-5-tips>
- <https://www.legalteamusa.net/5-ways-to-prevent-being-a-victim-of-cyber-crime/>
- <https://www.dbs.com/act/4-important-steps-that-all-cyber-crime-victims-must-take.html>

TECHNOLOGY & HUMAN RIGHTS

This is a website created by a group of web development students that aims to address the issues on the persistent issues related


USEFUL LINKS

What are Cybercrimes?
Philippine Laws on Cybercrimes

CONTACT

📍 Angeles City, Pampanga, PH
✉️ techandhr.ph@gmail.com

• Contact page


[Home](#) [About](#) [Learn](#) [Contact](#)

Connect with the team.

If you wish to know more about who we are and what we do, feel free to contact us by filling up the form.

Get in Touch

HOLY ANGEL UNIVERSITY

REFERENCES

Carter, J. (n.d.). *9 most common computer and internet cyber crimes*. The Law Office of Elliott Kanter APC. Retrieved April 15, 2022, from <https://www.enkanter.com/article/9-most-common-computer-and-internet-cyber-crimes>

Latto, N. (2022, February 2). *What is cybercrime and how can you prevent it?* Avast.

Retrieved April 15, 2022, from <https://www.avast.com/c-cybercrime#topic-1>

Online scams, libel cases top PNP's cybercrime list from March to September. (2020, October 27). CNN. Retrieved April 14, 2022, from

<https://www.cnnphilippines.com/news/2020/10/27/Online-scams-libel-cases-top-PNP-s-cybercrime-list-.html>

Sonnie. (2022, March 30). *Cyberbullying in the Philippines: Applicable laws and practical help*. HR Mentor. Retrieved April 17, 2022, from <https://asksonnie.info/cyber-bullying-philippines/>

Statista. (2021, December 1). *Cyber crime in region 3 Philippines 2019, by type*. Retrieved

April 15, 2022, from <https://www.statista.com/statistics/1135347/philippines-cyber-crime-victims-region-3-by-type/#:%7E:text=In%202019%2C%20the%20number%20of,hacking%2C%20phishing%2C%20and%20cyberbullying.>

GITHUB Repository Link: [WD-302-Technology-and-Human-Rights/TechnologyAndHumanRights \(github.com\)](#)

Link to the web application: [Technology and Human Rights \(techandhr.xyz\)](#)

