ANNAMACHARYA INSTITUTE OF TECHNOLOGY & SCIENCES
(AUTONOMOUS)
RAJAMPET

COMMUNTIY SERVICE INTERNSHIP

Designed & Developed by

ANDHRA PRADESH
STATE COUNCIL OF HIGHER EDUCATION
(A STATUTORYBODYOFGOVERNMENTOFANDHRAPRADESH)

A COMMUNITY SERVICE INTERNSHIP REPORT ON
ONLINE SCAM & FRAUD PREVENTION AWARENESS

Submitted in partial fullfillment of the requirement for the award of the Degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING (ARTIICCIAL INTELLIGENCE)

BY

O. AJAY	**23701A3101**
J. AKSHAI KUMAR	**24705A3101**
A. CHARAN KUMAR	**24705A3102**
C. HARIKRISHNA	**24705A3103**
S. MAHAMMAD RAFI	**24705A3107**

Under the esteemed guidance of

Mrs. C. V. Lakshmi Narayana, M. Tech (Phd) .

Assistant Professor in CSE AITS

Submitted to

Department Of Computer Science And Engineering (Artificial Intelligence)

Annamacharya Institute Of Technology And Sciences

(An Autonomous Institution)

(Approved By AICTE ,New-Delhi And Affiliated To J.N.T.U, Anantapur)

(Accredited By NBA & NAAC With A+ Grade)

New Boyanapalli, Rajampet, Annamayya (Dt), A.P-516 126

2025-26

Department of Computer Science and Engineering (Artificial Intelligence)

Annamacharya Institute of Technology and Sciences

(An Autonomous Institution)

(Approved By AICTE ,New-Delhi And Affiliated To J.N.T.U, Anantapur)

(Accredited By NBA & NAAC With A+ Grade)

New Boyanapalli, Rajampet, Annamayya(Dt), A.P-516 126

CERTIFICATE

This is to certify that the Community Service Internship entitled **"Online Scam & Preventions Awareness"** Is submitted by **C. HARIKRISHNA (24705A3103)** In partial fulfillment of the requirements for the Award of Degree of **Bachelor of technology** in **"Computer Science & Engineering (Artificial Intelligence)"** for the academic year 2025-26.

Signature of Project Supervisor:
Mr. C. V. LAKSHMI NARAYANA
Assistant Professor CSE(AI),

AITS, Rajampet. AITS,Rajampet.

Signature of HOD:
Dr. N. PENCHALAIAH, Ph.D,
Professor & Head,Dept. of CSE(AI),
Dean of Student Affairs,

PROGRAM REPORT
FOR
COMMUNITY SERVICE INTERNSHIP

NAME OF THE STUDENT :

NAME OF THE COLLEGE : ANNAMACHARYA INSTITUTE OF TECHNOLOGY & SCIENCES RAJAMPETA

REGISTRATION NO. :

PERIOD OF CSP: FROM: TO:

NAME & ADDRESS OF THE COMMUNITY / HABITATION:

Community Service Internship Report

Submitted in accordance with the requirement for the degree of ……

Name of the College:

Department:

Name of the Faculty Guide:

Duration of the CSP: From…… To- - -

Name of the Student:

Programme of Study:

Year of Study: Register

Number: Date of Submission:

Acknowledgements

We take this opportunity to express our heartfelt gratitude to the management of ***Annamacharya Institute of Technology and Sciences (AITS), Rajampet*** for granting us the invaluable opportunity to undertake the ***Community service internship*** as an integral part of our academic curriculum. This initiative not only enriched our learning experience but also instilled in us a deeper sense of social responsibility and empathy.

Our sincere appreciation goes to ***Dr. N.Penchalaiah, Ph.D, Professor & Head, Department of CSE, AITS***, for his inspiring leadership and constant motivation. His guidance helped us align our efforts with the core values of service, compassion, and learning.

We are profoundly thankful to our esteemed guide, ***Mrs.* C.V. Lakshmi Narayana , *MTech(Phd), Assistant Professor, Department of CSE, AITS***, for her unwavering support, insightful feedback, and continuous encouragement throughout the course of the project. Her mentorship played a pivotal role in shaping our approach and ensuring the successful execution of our activities.

We extend our deepest thanks to the ***management and staff of Brunda Spoorti Foundation, Kadapa***, for welcoming us with open arms and providing us with a platform to engage meaningfully with the senior citizens. Their cooperation and hospitality made our experience truly memorable and impactful.

Interacting with the senior citizens was a humbling and enlightening experience. We are immensely grateful to them for sharing their stories, wisdom, and life lessons with us.

Their resilience, warmth, and kindness left a lasting impression on our hearts and minds. Their blessings and smiles were the most rewarding part of our journey.

We also acknowledge the support of our fellow students and volunteers who contributed their time and energy to make this project a success. The spirit of teamwork and mutual respect that prevailed throughout the project was truly commendable.

Contents

Executive summary

The rapid advancement of technology and the widespread use of the internet have revolutionized communication, business, and education. However, this digital growth has also given rise to numerous online scams that target unsuspecting users. Online scams are deceptive activities carried out by cybercriminals to obtain money, personal data, or confidential information through fraudulent means. These scams can appear in the form of fake emails, job offers, investment schemes, lottery messages, or even impersonation on social media platforms.

This project explores how such scams operate by analyzing the methods and psychological tricks used by scammers. They often gain a victim's trust by posing as legitimate institutions or individuals, creating a sense of urgency or fear, and convincing users to share sensitive details or make payments. Once the victim is trapped, the scammer disappears, leaving behind financial loss or identity theft.

The report also emphasizes the growing role of artificial intelligence in modern scams, where fake voices, images, and videos are used to make frauds appear more realistic. To counter these threats, the project highlights essential safety measures such as using strong passwords, enabling two-factor authentication, avoiding suspicious links, verifying sources, and maintaining awareness about new cyber threats.

Ultimately, this project aims to create awareness among internet users about the nature of online scams and to encourage safe digital practices. By spreading knowledge and vigilance, individuals can protect themselves and others from becoming victims of online fraud, contributing to a safer digital society

Introduction: what is are online scams?

The rapid growth of the digital world has transformed the way individuals and businesses operate, offering unmatched convenience and opportunities. However, this advancement has also given rise to increasingly sophisticated online scams and fraudulent schemes. Cybercriminals are constantly developing new tactics to exploit human behavior, financial systems, and technological vulnerabilities. Online fraud can result in financial loss, identity theft, reputational damage, and even emotional stress. To counter these threats, it is essential to stay informed, vigilant, and proactive. Awareness is the first line of defense against such risks, empowering users to recognize, avoid, and report fraud attempts.

Common Types of Online Fraud

Fraudsters use different tactics depending on their target and objectives. Some of the most common types include:

1. **Phishing Scams** – Fraudulent emails or messages designed to trick individuals into revealing sensitive data such as passwords or credit card numbers.
2. **Identity Theft** – Stealing personal details to impersonate victims for financial gain.
3. **Investment & Ponzi Schemes** – Promises of quick returns or doubled investments that ultimately collapse, leaving victims at a loss.
4. **E-commerce Scams** – Fake online stores or deceptive ads tricking consumers into paying for products they never receive.
5. **Social Engineering Attacks** – Manipulating trust to extract confidential information.
6. **Healthcare and Insurance Fraud** – Exploiting patients or systems for financial reimbursement.
7. **Tax Evasion & Bankruptcy Fraud** – False claims to gain illegal benefits. These methods can be combined with digital tools such as fake websites, cloned apps, or deepfake technology to increase credibility.

Types of online scams

Text or SMS scams

Scam messages look like they are from the government, businesses you deal with or even your own family or friends to try to catch you out.

They sound urgent to get you to act quickly. They often have a link which will take you to a scam website. Scammers can steal any personal information entered on these scam websites and use it to take your money or commit fraud in your name.

Phone scams

1 in 3 reported scams happen by phone. Scammers call, claiming to be from well-known organisations. This includes government organisations, law enforcement, investment and law firms, banks, telecommunication providers.

Email scams

Scam emails look like the real thing, but watch out for links and attachments designed to steal your money or information.

Scammers send 'urgent' emails pretending to be from the government, law enforcement and businesses.

They use the same logo and a similar email address as the real organisation. Scammers can also copy or 'spoof' the email address of an organisation or business to make the scam email look more real.

Common signs of scams

Unusual communication: The way they talk to you seems strange or different from normal.

Communication from unverified sources: You don't really know who is sending the messages.

Deals that are too good to be true: They promise benefits or opportunities that sound amazing but seem unrealistic.

Visible errors or signs of spoofing: You can see mistakes or parts that look copied or fake.

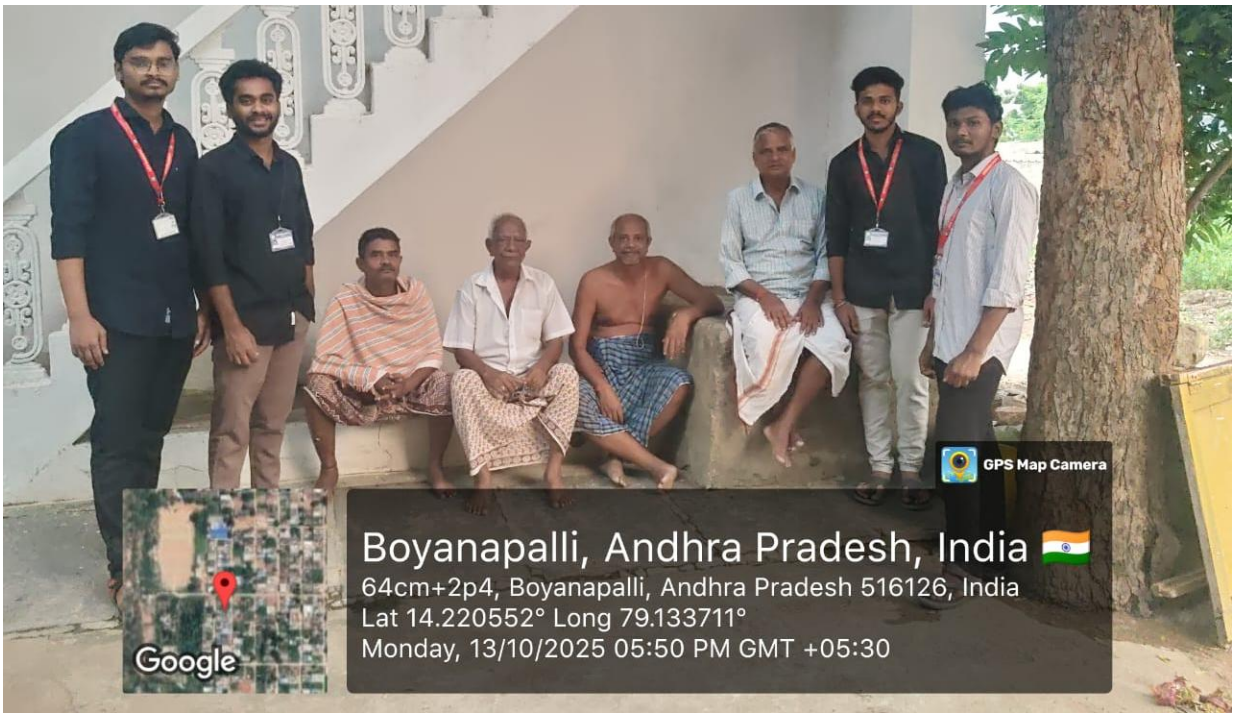
Requires clicking links or downloading things: They ask you to open links, or install files or apps on your phone or computer.

Requests for personal details: They ask for information about you that should be private.

Asking to send money to strangers: They want you to pay people or groups you do not know.

Asking to control your device (i.e. screen-sharing): They want more access to your phone or computer, like seeing your screen.

Saying you must act now: They try to make you feel like you need to act or respond urgently.



How Online Scams Work

Online scams aren't just about fake messages — they're carefully designed traps that play with your mind and emotions.

1. Targeting

Scammers start by finding easy targets:

They collect data from leaked databases, public profiles, or random WhatsApp numbers.

Sometimes, they message thousands of people — even if 10 respond, it's a win for them.

Example: You suddenly get a message saying you've won a lucky draw — that's their hook.

2. Building Trust

Next, they act like genuine people or companies:

They use fake logos, official-looking email IDs, and polite communication.

They may pretend to be from banks, delivery services, or even your friend's hacked account.

Example: "Hi, this is SBI customer care. Your card is blocked, please verify details."

3. Creating Urgency or Fear

They make you panic or rush before you can think:

“Your account will be locked in 30 minutes!”

“Limited-time offer — pay now!”

“Police complaint will be filed if you don’t respond.”

Why it works: When you’re anxious, you skip verification steps — exactly what they want.

4. The Trap Once you believe them, they make their move:

Ask for OTP, password, or PIN.

Send a fake payment link or QR code.

Request a small deposit to “unlock” a larger reward.

Install malicious apps that steal data in the background.

5. The Disappearing Act As soon as you send money or share data:

The scammer vanishes, blocks you, or deletes the account.

In phishing cases, they immediately transfer money or sell your details on dark web markets.

6. Automation & AI Tools Now, scammers even use AI-generated voices, videos, and messages:

Fake celebrity endorsements

Voice clones asking for help

AI chatbots that sound “human”

How to stay safe online

Essential Internet Safety Tips

To avoid all of these dangers, we recommend following our essential internet safety tips when you or your family are online:

1. Make sure you're using a secure internet connection

Although using public Wi-Fi is not recommended, it's sometimes unavoidable when you are out and about. However, when you go online in a public place and use a public Wi-Fi connection, you have no direct control over its security, which could leave you vulnerable to cyberattacks. So, if you are using public Wi-Fi, avoid carrying out personal transactions that use sensitive data, such as online banking or online shopping. If you need to do any one of these, use a Virtual Private Network or VPN. A VPN will protect any of the data you send over an unsecured network via real-time encryption.

If you don't use a VPN, we recommend saving any personal transactions until you can use a trusted internet connection. You can find out more about what a VPN is here.

2. Choose strong passwords

Passwords are one of the biggest weak spots when it comes to cybersecurity. People often choose passwords that are easy to remember and, therefore, easy for hackers to crack with hacking software. In addition to this, using the same password for multiple sites puts your data at further risk. If hackers obtain your credentials from one site, they can potentially access other websites which use the same login details.

Select strong passwords that are harder for cybercriminals to crack. A strong password is:

Long – made up of at least 12 characters (ideally more).

A mix of characters – upper-case and lower-case letters plus symbols and numbers.

Avoids the obvious – such as using sequential numbers ("1234") or personal information that someone who knows you might guess (or that might already be online), such as your date of birth or a pet's name.

Avoids memorable keyboard paths.

Using a password manager can help. Password managers help users create strong passwords, store them in a digital vault (which is protected by a single master password) and retrieve them when logging into accounts online.

3. Enable multi-factor authentication where you can

Multifactor authentication (MFA) is an authentication method that asks users to provide two or more verification methods to access an online account. For example, instead of simply asking for a username or password, multifactor authentication goes further by requesting additional information, such as:

An extra one-time password that the website's authentication servers send to the user's phone or email address.

Answers to personal security questions.

A fingerprint or other biometric information, such as voice or face recognition.

Multifactor authentication decreases the likelihood of a successful cyberattack. To make your online accounts more secure, it's a good idea to implement multifactor authentication where possible. You can also consider using a third-party authenticator app, such as Google Authenticator or Authy, to help with your internet security.

4. Keep software and operating systems updated

Developers are constantly working to make products safe, monitoring the latest threats and rolling out security patches in case of vulnerabilities in their software. By using the latest versions of your operating systems and apps, you will benefit from the latest security patches. This is especially important for apps that contain payment, health or other sensitive information about a user.

5. Check that websites look and feel reliable

For any website you visit, especially ones you transact with (such as e-commerce sites), it's crucial that they are reliable. A key element to look out for is an SSL/security certificate. This means, lookout for URLs that start with “HTTPS” rather than “HTTP” (the “S” stands for “secure”) and have a padlock icon in the address bar. Other trust

signals include:

Text which is free from spelling and grammar mistakes – reputable brands will make an effort to ensure their websites are well-written and proofread.

Images that are not pixelated and fit the screen's width correctly.

Ads that feel organic and are not too overpowering.

No sudden changes in color or theme. In some cases, where users have interacted with a particular website and returned to a familiar page from a link, subtle color or design changes might indicate forgery.

The accepted standards of online payments – legitimate ecommerce websites use credit or debit card portals or PayPal, only. If a website is using another form of digital money transfer to accept payments, it is probably fraudulent.

6. Review your privacy settings and understand privacy policies

Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. But you can take charge of how much information third-parties can access. Both web browsers and mobile operating systems have settings to protect your privacy online. Social media sites, such as Facebook, Twitter, Instagram, LinkedIn, amongst others, have privacy-enhancing settings that you can activate. It’s worth taking a while to review your privacy settings across the board and make sure they are set to a level you are comfortable with.

Many of us accept privacy policies without reading them, but with so much data used for marketing and advertising (and hacking) purposes, it's a good idea to review the privacy policies of websites and apps you use, in order to understand how your data is collected and analyzed. However, bear in mind that even if your settings are set to private, very little data online is totally private. Hackers, website administrators and law enforcement could still have access to the information you regard as private.

banner

7. Be careful of suspicious links and where you click

A careless click can expose your personal data online or infect your device with malware. That's why it's essential to browse consciously and avoid certain types of online content – such as links from untrusted sources and spam emails, online quizzes, clickbait, 'free' offers or unsolicited ads.

If you receive an email that you're not sure about, avoid clicking on any links in it or opening any attachments.

In fact, it's best to avoid opening untrusted emails at all. If you're not sure whether an email is legitimate or not, go directly to the source. For example, if you receive a suspicious email from your "bank", call your bank and ask them if the email is genuine. When you're on a website, make sure links click through to relevant or expected topics. For example, if you click on a link that you think is about safaris in Africa, but instead you're taken to a clickbait-style page about celebrity weight loss or a "where are they now?" style piece, then quickly close the page.

A woman researching online safety tips with her child and partner.

8. Make sure your devices are secure

With up to 60% of people using mobile devices for shopping and finding information online, instead of a desktop, it's important that they are secured correctly. With all your devices – phones, computers, tablets, smartwatches, smart TVs, etc. – it's good practice to use passwords or passcodes and other security options like fingerprint readers or face-scanning technology. These measures will reduce the likelihood of a cyberattack or your personal data being stolen by hackers.

9. Backup data regularly

It's important to backup important personal information on external hard drives and regularly create new backups. Ransomware – a type of malware – involves cybercriminals locking your computer so you can't access valuable files. Backing up your data – and your family's data – helps mitigate the impact of a ransomware attack. You can protect yourself further with appropriate security software.

Other forms of malware deny you access to your personal data by overwhelming your system or simply deleting files, so be careful.

10. Close unused accounts

Over the years, many of us accumulate old accounts that we no longer use. These can be a weak link in terms of safety when using the internet – not only are old accounts more likely to have weaker passwords, but some of those sites may have poor data protection policies.

In addition, cybercriminals could piece together the information you have left in them, for example, old social media profiles – such as your date of birth or location, etc. – to build up a picture of your identity in an attempt to hack you later. As a result, we recommend closing your old online accounts and requesting that your data be deleted from the relevant third-party servers.

11. Be careful what you download

A top goal of cybercriminals is to trick you into downloading malware, which can be used to open a "backdoor" to your machine. Malware might be disguised as an app – anything from a popular game to something that checks traffic or the weather. Or, it could be hidden on a malicious website that attempts to install malware on your device.

Malware causes damage – such as disrupting how your device operates, stealing your personal data or allowing unauthorized access to your machine. This usually requires some action on your part, but there are also drive-by downloads, where a website attempts to install software on your computer without asking for permission first. Think carefully before visiting a new website or downloading anything onto your device, and only download content from trusted or official sources. Regularly check your download folders and if unknown files appear on your system (potentially, from a drive-by), delete them immediately.

12. Be careful what you post and where

The internet does not have a delete key. Any comment or image you post online may stay online forever because removing the original won't remove any copies that other people may have made. There is no way for you to 'take back' a comment you wish you hadn't made or remove an embarrassing image you posted. So, don't put anything online that you would not want a parent or prospective employer to see.

Similarly, be careful about disclosing personal information about yourself online. For example, avoid disclosing your social security number, address or date of birth in social media bios. You wouldn't hand personal information out to strangers individually, so don't hand it out to millions of people online.

Be careful about where you display or submit your email address. It's good to have a secondary, throwaway email account that you use solely for email sign-ups and subscriptions, separate from the one you use for friends and family, and separate from the one you use for work.

13. Be careful who you meet online

People you meet online are not always who they claim to be. Indeed, they may not even be real. Fake social media profiles are a popular way for hackers to groom unwary internet users and pick their cyber pockets. Apply the same caution in your online social life as you would for your in-person social life. This is particularly true with the rise of online dating scams in recent years.

14. Double check online information

Sadly, fake news, misinformation and disinformation are all present on the internet. It's easy to feel lost with the flood of information we're exposed to every day. If you read something you are unsure of, do your own research to establish the facts. Reliable websites will have references to the original information and source materials. Suspicious pages won't offer any references at all. Read our guide to spotting fake news here.

15. Use a good antivirus and keep it updated

As well as following safety tips for online behavior, it's essential to use a good quality antivirus provider. Internet security software guards your devices and data and blocks common threats like viruses and malware (plus complex ones like spy apps,

“cryptolockers” and XSS attacks). As with all operating systems and apps, it's essential to keep your antivirus updated to stay ahead of the latest cyberthreats.

Awareness campaign ideas

1. Educational Workshops and Seminars

Conduct interactive sessions in schools, colleges, or community centers.

Use real-life examples and short videos to explain different types of scams like phishing, fake job offers, and UPI frauds.

Invite a cyber security expert or police officer to share practical tips

Distribute handouts or posters with “Do’s and Don’ts” for safe internet use.

2. Social Media Awareness Campaign

Launch a series of short posts or reels explaining one scam type per day/week.

Use hashtags like #ThinkBeforeYouClick, #OnlineSafety, or #CyberAware.

Share infographics showing “Red Flags” of scams — fake links, urgent messages, unrealistic offers, etc.

Conduct polls and quizzes: “Can you spot the scam?”

Encourage followers to share their experiences or scam alerts.

3. Short Films or Story-Based Videos

Create short videos or reels showing how a normal person gets trapped in an online scam — and how awareness can prevent it.

Keep them emotional or relatable for more reach.

Add a small message at the end like:

“Verify before you trust. Report scams at cybercrime.gov.in.”

4. Poster and Slogan Competition

Organize poster-making or slogan-writing contests in schools/colleges with themes like “Stay Smart, Stay Safe Online” or “Don’t Click the Trap”

Display the best entries on notice boards or online pages.

5. Collaboration with Influencers or Local Authorities

Partner with digital creators, tech educators, or police departments for awareness sessions.

They can post real scam examples and demonstrate how to report them.

Use regional language versions to reach rural or older audiences.

6. Interactive Website or App

Create a simple web page or app that tests users’ scam awareness through games or quizzes.

Include tips, news on latest scams, and official links for reporting cybercrimes.

7. Street Plays and Public Events

Perform short skits in crowded areas like markets or bus stands showing common scam scenes (e.g., fake bank calls, phishing messages).

End with a strong message on how to recognize and avoid them.

8. Awareness Week / Online Safety Day

Dedicate one week to digital safety activities in your school or organization.

Each day can focus on a theme:

Day 1: Password Safety

Day 2: Social Media Scams

Day 3: Online Shopping Fraud

Day 4: Financial Scam Prevention

Day 5: Reporting Cybercrime

9. Distribution of Digital Safety Guides

Design a small e-booklet or pamphlet with scam examples and safety tips.

Share it via email, WhatsApp groups, or social media posts.

10. Reporting & Support Drive

Encourage people to report scam attempts instead of ignoring them.

Share links to cybercrime.gov.in and helpline 1930.

Explain how timely reporting helps track and stop scammers.

Conclusion

Online scams have become one of the most serious challenges in today's digital world. As technology advances, scammers are finding new and smarter ways to deceive people. Through this project, we learned how scams operate, the psychological tricks used by fraudsters, and the importance of awareness and prevention. Staying alert, verifying sources, and practicing safe internet habits can protect individuals from online threats. Awareness campaigns, education, and responsible digital behavior are the keys to building a safer