Cyber Invasion

Cyber Invasion is a kind of an attempt to expose alter, disable, destroy, steal or gain an unauthorized use of assets and how to secure them

Camera often Lies :
Digital Image Manipulation Attack

Manoj Singh Gaur
Director, Indian Institute of Technology Jammu jagti, PO Nagrota, NH-44, India

Vijay Laxmi
Professor, Department of Computer Science and Engineering, Malaviya National Institute of Technology Jaipur, India

Mohit Singh
Ph.D. Scholar, Department of Computer Science and Engineering, Malaviya National Institute of Technology Jaipur, India

With the tendency to spend more anWd more time online the use of social media for spreading misleading multimedia content is very common. The materials are of utter importance as they can use an influencing identity to disseminate false information. With the advancement in AI techniques, one can create fakes with no technical knowledge and at a low cost. Third party filtering or manual checking can be very costly and time-consuming. The potential of these fakes generates the requirement of an algorithm or some automated tool for detection. This article attempts to give a brief introduction to multimedia manipulation and its detection with necessary technical details.

Keywords : CNN - DeepFake

Introduction

Data from Global Digital report 2018 [1] states that we just crossed the 4 billion mark of internet users globally. With 52% of Smartphones ready to provide a rich internet experience where ever we go, Peoples are spending more and more time online. The social platform continues to grow with an alarming rate of 11 new users every sec. Due to the broad span nature and ease of access to the internet and social media, there is an increase in the tendency to receive news, reviews, and other promotional information online. About 68 % of adult [2] are reported to get news online due to which social platforms is the favorable choice among Marketers.

But with this constant change, we must consider the fact that the spread of false and fake information is quite common on the social platform and is affecting the critical decision making and thinking skill of our society. The fake news can have long-lasting impacts on individual, society, and country. Fake news is intentionally trolled to mislead people to believe false. It depends on the people's intellect that how they will respond to factual information later on. And in all, it broke the trustworthiness of the entire news system.

Despite fake textual content, recent advancement in AI technologies and other Digital manipulation tools make it easy to create fakes in the audiovisual form in low cost and without any expertise in the field. The contents are of special importance as it can be a misleading story, a Hoax or a viral stunt containing some rational comments or can feature some public or an authority figure to disseminate false information.

Visual deception: Seeing is what believing

With considerable progress in detecting the textual fakes by employing community checks and third-party fact refining, little effort has been directed to protect consumers from fake multimedia contents. There are cases that, fake videos by Hollywood

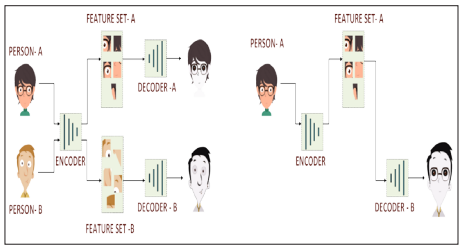


Figure 1.
Face Swap Process

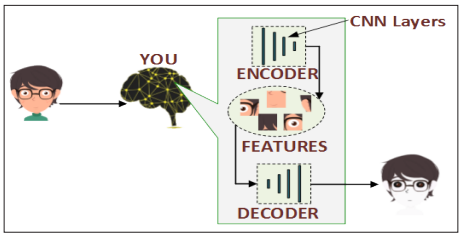


Figure 2.
Encoder and Decoder without Sketch Artist

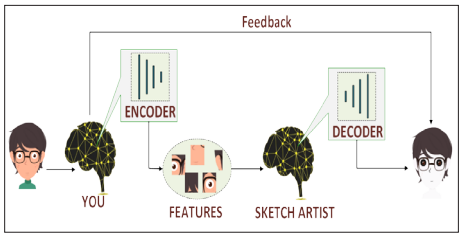


Figure 3.
Encoder and Decoder in presence of Sketch Artist.

CG artist out of hobby got a million views on the social media platform. Manual detection is very costly and requires an expert by Knowledge and experience. Digital manipulation using tools such as Photoshop, Adobe Premiere or techniques such as AAM (Active appearance model) is computationally expensive.

DeepFake:
A product of AI Deepfake multimedia contents are created using machine learning (A branch of AI that helps computer systems to learn from examples and perform complex task). As Visual impersonation requires similarity in appearance and behavior, it is complicated for a human to learn the gesture. The process of creating easier fakes by using the concept of learning from example is Deepfake.

Until now, Cinematographic and Gaming industries were few to have access to these technologies known as CGI (Computer Generated Imagery) to create realistic graphics, games, and Movies. The availability of high-performance GPU's and availability of open source tools make this technology accessible for users to combine, replace or superimpose images or videos in a malicious way.

Exploring Deepfakes
Several digital manipulation techniques come under the umbrella of deepfake, such as:

- Face Swap
- Audio Deepfake and Lip syncing
- Deepfake puppetry.

Deepfake works on the principle of learning hence we have to collect several samples to learn from for two different faces A and B. Auto-encoder [4] or Generative Adversarial networks [3] are mostly used for this purpose. Basic Autoencoder and Face Swap process are briefed in the next section.

Face Swap using Auto-encoder

As we know that CNN is a Neural network that is used to extract features from images. Consider the following cases:

Case:

Someone asked you to draw the sketch of person A as shown in Fig.2, or to describe person A to a sketch artist as in Fig.3.

Steps:

- You will recall some facial features of person A. such as eye color, hair color facial structure and other.
- Try to draw those facial features on paper or describe to sketch artist and now will draw those facial features on paper.

`When you are drawing the sketch, you are your teacher and can improve the sketch by drawing, again and again, recollecting the facial features recognized in the first step meanwhile improving those features while you draw. And when you have to describe the features to the artist, then he will continuously take feedback from you to refine the sketch. The CNN responsible for generating features from samples is our ENCODER and one accountable for regenerating face from the features is our DECODER. Hence ENCODER is the CNN layers for downsampling and DECODER is for upsampling features back to the image.

Consider two different Decoders trained two generate different person A and B. Face swap can simply be obtained by swapping A's Decoder with B's in the process of regeneration and input it with the feature set of person A. As Decoder B is trained to generate person B, it will assume input feature set as noisy features of person B and will regenerate person B having features from person A as shown in Fig. 1. Some basic steps that can help in improving the result are to increase the training data, data variability and increased training time.

Challenges with digital forensic

Digital forensic was primarily focused on duplicating, slicing, copy pasting and other low-level manipulations till now. But AI techniques and the leverage of these techniques in other tools such as Adobe VoCo and Scene Stitch worsen the situation.

In the situation of multimedia content, being presented as evidence the vulnerability of the digital content must be considered. Shortly the media forensic expert must also be knowledgeable in the field of Machine learning and AI. And considering the facts that most of the multimedia contents are distributed primarily through social media, high compression factor should also be considered. Compression can remove the evidence of tempering in
the digital media.

Conclusion

With extensive AI developments we are moving in the era where any multimedia data can be faked. Deepfakes being the new challenge for digital forensic, images and videos must be checked before accepting them as evidence or allow them on social media.

XceptionNet, a CNN, is proved to an efficient algorithm for detecting doctored photos both for the compressed and uncompressed case. Several algorithms are yet to come as AI is constantly in the verse of improvement. DARPA, a part of US military is also funding research realizing the potential of Deepfakes.

References:

- *https://wearesocial.com/uk/blog/2018/01/global-digitalreport- 2018*
- *Shu, Kai, Suhang Wang, and Huan Liu. "Understanding user profiles on social media for fake news detection." 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR). IEEE, 2018.*
- *Goodfellow, Ian, et al. "Generative adversarial nets." Advances in neural information processing systems. 2014.*
- *Doersch, Carl. "Tutorial on variational autoencoders." arXiv preprint arXiv:1606.05908 (2016).*

Phishing attacks and the countermeasures

Alwyn R. Pais
Assistant Professor in Department of Computer Science and Engineering, NITK Surathkal

Routhu Srinivasa Rao
Research Scholar in Department of Computer Science and Engineering, NITK Surathkal

Phishing is an attack in which attacker tries to trick users to reveal the sensitive and personal information such as credit card details, password etc. Attacker can perform phishing attack for financial benefits, to sell identities of the victims, to obtain ransom, to exploit vulnerabilities in the system. Attacker carry-out the attack by designing a phishing website which looks similar to that of target legitimate site such that online user can be deceived to reveal the sensitive information.

Phishing attacks are so popular because they are lucrative and is easy to perform due to the existence of phishing tool kits. According to RSA (2013) report [1], there has been a loss of $5.9 billion in 2013 itself. Phishing is a growing threat and is hard to defend against it. It has become highly prevalent problem because distributing millions of fake emails is a trivial task and even a less success rate is significantly profitable to the attackers.

Statistics of Phishing attacks

Phishing attacks are rising year by year due to increase in number of internet users. As per Anti-Phishing Working Group (APWG) Q3 (2017) report [2], the number of unique phishing attacks reported was 296,208, nearly 23,000 more than Q2. According to RSA Q1 (2018) fraud report [3], 24,581 phishing attacks were detected which is almost half of all cyber-attacks. According to the latest APWG (2016) report [4], 1,220,523 number of phishing attacks were recorded in 2016 and has been concerned to be the highest than in any year since it began monitoring in 2004. These figures reveal that phishing attacks increased year after year from 2010 to 2016 accounting to billions of dollars in loss.

Example of Phishing attack

This example gives some clarity to the concept of phishing. Figure 1 claims to be like a legitimate site ebay. The design and content is mimicked exactly like ebay website. The user cannot identify the website as fake unless he observes the URL of the website in this case. Figure 2 is a snapshot of legitimate eBay site. By observing both the website's snapshot one cannot identify which is phishing and legitimate unless the user is well trained. There are some circumstances even a well-trained individual may not identify phishing sites.

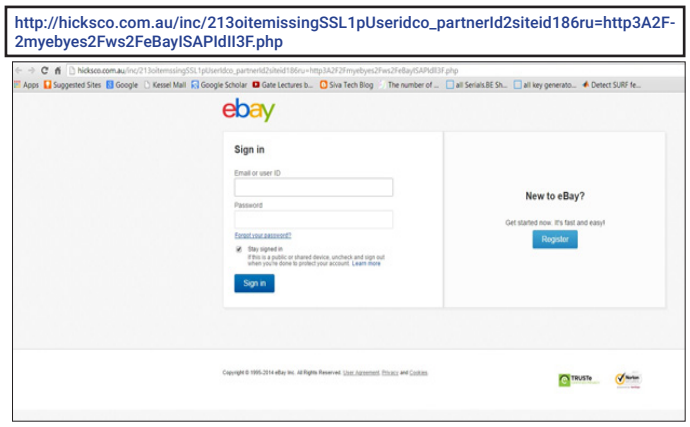


Fig. 1 Phishing Website targeting legitimate EBAY

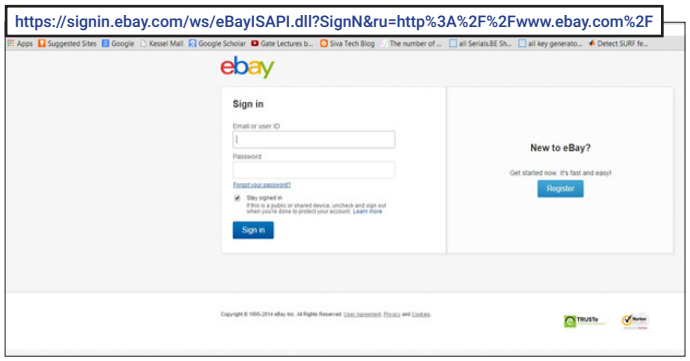


Fig. 2 Legitimate EBAY Website

Types of Phishing attacks:

Phishing attacks vary widely in terms of their complexity, quality of the forgery and the attacker's objective.

Email Phishing:
Attackers design fake emails which claims to be arriving from trusted company. They send fake emails to millions of online users assuming that at least thousands of legitimate users would fall for it.

Website phishing:
Attacker builds a website which looks like a replica of legitimate site and draws the online user to the website either through advertisements in other websites or social networks such as Facebook, Twitter and some blogs etc.

Why People Fall for Phishing ?

- Lack of awareness about phishing attacks
- Lack of knowledge about importance of security in the computer systems
- Use of more sophisticated phishing techniques (for e.g. use of images in place of text)
- Paying no attention to address bars, URL and websites containing visually deceptive text (for e.g. Using paypl instead of paypal)
- Ignoring warnings about fake certificate

Malware phishing:
Attacker inserts a malicious software such as Trojan horse into a compromised legitimate site without the knowledge of a victim. The malware can be attached to a link, music file or an application in a website and on clicking the links, malicious software is installed into the user computer, keeps track of sensitive information and sends to the attacker.

Smishing:
It tricks the online users into revealing their sensitive information via a text or SMS message.

Vishing (Voice Phishing):
Users are contacted randomly with an automated dialing program called as war dialer where the users hear a prerecorded message claiming their account is compromised or need to be verified. Further, they are prompted to enter sensitive information into the telephone.

Spear Phishing:
These attacks target a specific group of people or community belonging to an organization or a company. They send emails which pretend to be sent by a colleague, manager

or a higher official of the company requesting sensitive data related to the company. The main intention of general phishing is financial fraud, whereas spear phishing is a collection of sensitive information.

Whaling:
It is a type of spear phishing where attackers target bigger fish like executive officers or high profile targets of private business, government agencies or other organizations.

Types of anti-phishing techniques

List-based approach:
It can use either whitelist or blacklist. Blacklist consists of a list of suspicious URLs and IP addresses to validate the status of URL. If the visited URL is listed in Blacklist then it is considered as malicious site. Similarly, the whitelist consists of list of legitimate URLs which are accessed by the browsers. This technique allows, website to be downloaded only if it is present in the whitelist.

Heuristic feature-based approach:
In this approach, features are extracted from URLs, source code of web pages and third party-based features. The limitation of this approach is that the heuristic features are not guaranteed to exist in all phishing sites.

Visual similarity-based approach:
This compare suspicious website image with legitimate image database to get similarity ratio which is used for classification of website. The website is classified as phishing when the similarity score is greater than a certain threshold else it is treated as legitimate.

Machine learning-based approach:
These techniques are combination of heuristic methods and machine learning algorithms i.e. dataset used by the machine learning algorithms is extracted through heuristic methods. Various machine learning algorithms are applied to evaluate the built model. Some of the algorithms are Random Forest (RF), Bayesian network (BN), Support vector Machine (SVM) etc

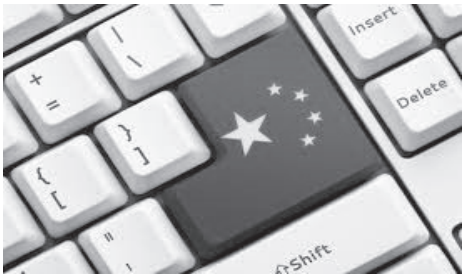
Conclusion

Phishing is an art of manipulating online users into performing actions or divulging sensitive information. Phishing attacks are on rise. Lack of awareness is one of the major reason for the rise of phishing attacks. It is impossible to defend against every attack. User education is the strongest defense and at the same time it is the weakest link to counter phishing attacks. However, if we leverage better user intervention mechanism and employ advanced heuristic technique which filters new kinds of phishing websites, we can reduce the risk.

Precautions:
- Change the browser settings to prevent fraudulent websites from opening
- Check the address of the link embedded in the email before clicking the link.
- Never respond to an email seeking sensitive data because banks or organizations will not ask for it
- Use antivirus and firewall and update them regularly.
- Be cautious before opening any attachment in the email regardless who sent them

Various Ways of Cyber Attacks

Dr. Deepak Shikarpur
IT entrepreneur, author and Digital Literacy activist



Cyber wars can be conducted in a number of ways. James Clapper, Director of National Intelligence, has classified cyber warfare into two categories – first is cyber spying and second is cyber attacks. America constantly fears attacks on its computer networking systems.

A lot of information can be exchanged as well as stored on the web, regarding national security and also the international position on certain issues. Such information is not only very sensitive and confidential but can also be copyright protected. Any attempt to procure such information and use it in an unauthorized manner or sell it or get other services in exchange for it is generally termed as cyber spying. Such data can be obtained from personal, institutional or departmental emails .In addition it can be secured by cleverly getting hold of the person's business or political rivals or benefactors or opponents. In order to get the information hackers are employed to manipulate the internet, networks, software as well as computers and computer systems.

There can be military, political, economic and social motives behind this. Such stolen, secret information is not only used in an unauthorized manner but also retained on the site after making a few changes, (to suit the interests of the hackers or those who hire them), which is more dangerous and misleading. Consequently, those handling as well as reading the main source of the data cannot make out (at least initially), that the information is distorted. There is every possibility that wrong decisions or actions are taken based on such incorrect information. These mistakes are likely to be advantageous for rival nations. There is likelihood that the country in question may be caught unawares when an attack is made on it. Such attacks can be made on various levels. It is not necessary that every assault on intellectual property or loss of information is liable to cause national security threats or lead to betrayal of the nation. America which is a leader in all these aspects is used to such attempts of sabotage. America has always been vigilant of the 'internet traffic' in other countries and many a times fallen a victim to its own trap. The recently instituted American secret service agency called 'Cyber Command 'has named these cyber attacks with names such as Titan Rain, Moonlight Maze. But Americas

In the opinion of the Governor of 'The Reserve Bank of India', Raguhram ,
If we wish to bring about positive changes in the banking sector we must pay serious attention to the issue of cyber security.

Cyber wars can be conducted in a number of ways. James Clapper, Director of National Intelligence, has classified cyber warfare into two categories – first is cyber spying and second is cyber attacks. America constantly fears attacks on its computer networking systems.

A lot of information can be exchanged as well as stored on the web, regarding national security and also the international position on certain issues. Such information is not only very sensitive and confidential but can also be copyright protected. Any attempt to procure such information and use it in an unauthorized manner or sell it or get other services in exchange for it is generally termed as cyber spying. Such data can be obtained from personal, institutional or departmental emails .In addition it can be secured by cleverly getting hold of the person's business or political rivals or benefactors or opponents. In order to get the information hackers are employed to manipulate the internet, networks, software as well as computers and computer systems. There can be military, political, economic and social motives behind this. Such stolen, secret information is not only used in an unauthorized manner but also retained on the site after making a few changes, (to suit the interests of the hackers or those who hire them), which is more dangerous and misleading. Consequently, those handling as well as reading the main source of the data cannot make out (at least initially), that the information is distorted. There is every possibility that wrong decisions or actions are taken based on such incorrect information. These mistakes are likely to be advantageous for rival nations. There is likelihood that the country in question may be caught unawares when an attack is made on it.Such attacks can be made on various levels. It is not necessary that every assault on intellectual property or loss of information is liable to cause national security threats or lead to betrayal of the nation. America which is a leader in all these aspects is used to such attempts of sabotage. America has always been vigilant of the 'internet traffic' in other countries and many a times fallen a victim to its own trap. The recently instituted American secret service agency called 'Cyber Command 'has named these cyber attacks with names such as Titan Rain, Moonlight Maze. But Americas self acclaimed position as 'world police' and urge to always be in the driver's seat took a beating with Snowden's 'Wiki Leaks'.

Recently America has confessed that owing to security concerns, it has hacked the computer systems all over the world. Even countries such as India, Germany and France have not been spared.

If these miscreants become successful in making connections between the computers and satellites commissioned for information or any other function then certainly for them 'the sky is the limit.' These two elements are the most sensitive and crucial in any modern electronic system. This can cause unprecedented danger to military systems. For e.g., in the American system, constituents such as C41STAR play an important role related to the control tower while launching missiles or sending laser beams .The hackers can close down this system or manipulate it to suit their purpose and create havoc. Since all systems depend upon the net and computers it is possible to influence them and even without actually waging a war generate an equal amount of damage. All sectors such as power production, dams and water supply, telecommunication, railway and air transport, industrial production have been digitized on a large scale. If this is manipulated by unauthorized sources it will certainly affect the respective countries.

In July 2010, security experts unraveled a non-military instance of sabotage in the form of a software programme called Stuxnet,(a worm or malware) which was thrust into the computer network systems of a number of industries all over the world. Fortunately as it was possible to curb the germ before it could cause any damage, it was feasible to avert large scale industrial and financial losses. According to the New York Times this was the world's first damaging cyber sabotage.
A few instances of financial scams in the Indian share market leading to a loss of thousands and crores of rupees of investors as well as the country took place during the beginning of the twenty first century. Ketan Parekh, Harshad Mehta and Satyam Computers, a number of co-operative banks, financial scams and irregularities cost a loss of hundreds of crores of rupees to the investors. Our share market as well as share markets of other countries can be attacked and this will lead to financial losses. But more important is that the extremists will be successful in creating an atmosphere of disbelief, uncertainty and fear among the people.

Denial of Service:

One way in which to cause discomfort is by obstructing the electronically provided services to the consumer or user .Not allowing the services to reach the consumer at all is

another method of sabotage. This is called Denial of Service, DoS. If the scope widens it is called Distributed Denial of Service, DDoS. Usually these attacks are launched on customer services such as banks, credit cards, payment gateways, online booking, route servers and signaling systems. There are instances of how as a consequence, a particular service failed completely over a vast area at a specific point of time and disrupted all transactions leading to weakening the computer security systems and tactics of that country. This assault can be actually or physically made instead of conducting it electronically and cause equal damage. For e.g., Many Asian countries faced a total net blank out because a communication cable which is located in the Atlantic Ocean was busted. Even though this incident was an accident it could have been purposely sabotaged.

The Department of Homeland Security has agreed that 'many power grids in America are likely to fall a victim to sabotage and cyber war'. According to an internal report in 2009 Russian as well as Chinese spies had hacked software of the control system and manipulated certain programmes which would enable them to stop the power supply whenever they wished to do so. This idea has been explored in a Hollywood movie, 'Die Hard 4'.

If power supply gets disrupted in a large area of the country (or if telephones are out of order), it leads to considerable financial losses as well as a mistrust of the services. It creates a negative approach in the public mind towards these facilities and services and they feel that 'they are not secure'. The extremists become successful in spreading a feeling of insecurity in the minds of people. Some experts feel that since, computer networks are involved in the distribution and control and general administration rather than power production, so the power plants are not endangered by cyber attacks. So far there is not a single instance of power grids being attacked and brought under control by the terrorists. We must remain alert because the danger of cyber attacks is widespread. Prevention is always better than cure!

How to prevent your Home/Personal Network from DDoS attack ?

Jeetendra Kumar Singh
Deputy Director
NIELIT Agartala

A DDoS (Distributed Denial of Service) attack occurs when multiple computers flood an IP address with data. The intent is to take the network offline, or slow it down. The best way to prevent a DDoS attack is to take steps to prevent it before it starts. Once a DDoS attack starts, you will need to change your IP address.

Attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites and social media. Once infected, these machines can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target. Some botnets are millions of machines strong.

Botnets can generate huge floods of traffic to overwhelm a target. These floods can be generated in multiple ways, such as sending more connection requests than a server can handle, or having computers send the victim huge amounts of random data to use up the target's bandwidth. Some attacks are so big they can max out a country's international cable capacity.
Specialized online marketplaces exist to buy and sell botnets or individual DDoS attacks. Using these underground markets, anyone can pay a nominal fee to silence websites they disagree with or disrupt an organization's online operations. A week-long DDoS attack, capable of taking a small organization offline can cost as little as $150-$200.

Symptoms:

The United States Computer Emergency Readiness Team (US-CERT) has identified symptoms of a denial-of-service attack to include:

- Unusually slow network performance (opening files or accessing web sites)
- Unavailability of a particular web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received

Additional symptoms may include:

- Disconnection of a wireless or wired internet connection
- Long-term denial of access to the web or any internet services.

If the attack is conducted on a sufficiently large scale, entire geographical regions of Internet connectivity can be compromised without the attacker's knowledge or intent by incorrectly configured or flimsy network infrastructure equipment.

Prevention Steps:

Use a firewall.
A firewall is a good first line of defence against a DDoS attack. It can prevent attackers from trying to detect your IP address which can be used to launch an attack on your router.

Use antivirus software.
Antivirus software alone won't prevent an attack, but it can prevent your computer from becoming part of a larger DDoS attack without your knowledge. Be sure to keep all security software on all your devices up to date.

Use a Virtual Private Network (VPN).
A virtual private network is able to hide your IP address by routing all your internet traffic through the provider's network. An attacker trying to detect your IP address would only detect the VPN's address. Traffic from a DDoS attack would reach your VPN's servers first, where they would hopefully be screened out before they hit your home network.

Keep your operating system up to date.
Whether you are using Windows, MacOS, Android, or iOS, make sure it has the latest security updates installed.

Keep your hardware and software up to date.
Make sure any apps that access the internet are kept up to date with the latest patches and security updates. When possible, configure these programs to automatically receive updates. Additionally, if your modem and router is more than a few years old, you should probably upgrade to the latest hardware. Some routers and external firewalls have built-in safeguards against DDoS attacks. They can block heavy bursts of traffic and block traffic from known attackers.

Only take voice chats from people you know.
Voice chat programs, like Skype, are known for having weak IP security. Keep these programs up to date with the latest updates and patches. Make sure your profile information is kept hidden, and only receive voice chats from people you know and trust.

Reset your IP address.
If all the preventative measures have failed, and you still find yourself victim of a determined attacker, you'll need to reset your IP address. There are a few ways you can do this.

Unplug your modem and router.
Depending on your internet service provider, you will be assigned a new IP address if you unplug your modem and router from 5 minutes, up to 24 hours.

Using the router's Admin console.
Type the router's IP address in a web browser (usually http://192.168.1.1) and log in as an admin. You should be able to find the appropriate settings to change your IP address under "Network Settings" or something similar. Consult your router's user manual for information on how to access the admin console and change your IP address for your specific router model.

Using the Command Prompt (Windows).
Click on the Start menu in the lower-left corner of the task bar. Type cmd. This will bring up the Command Prompt app in the start menu. Click on the app with the image that resembles a black screen with a cursor in the upper-left corner. Type ipconfig /release at the prompt and press ↵ Enter. Then type ipconfig /renew and press ↵ Enter. This will change the IP

References:

- *Data Sheet of Atlas Intelligence Feed*
- *https://en.wikipedia.org/*
- *https://www.digitalattackmap.com*

INFORMATION SECURITY AWARENESS FOR POLICE

Police Personnel should have a good understanding of the technology, the working of the devises, how internet works, how the citizens are targeted for online frauds and the use of tools and techniques to investigate and bring the culprits to Justice making use of different IT laws.

Awareness for the police is very much important to understand the various issues related to cyber world and safety guidelines which help them to save themselves and promote/share them with general public to participate securely while using Internet.

Let's have a look at the different initiatives taken under the purview of ISEA programme to create a cyber aware Police in India.

1. **Cyber Awareness weeks** across the country were organized along with the respective state police department in coordination with ISEA Team. As part this awareness **Master Trainers Groups** are created consisting of the Police personal, Teachers, NGOs/ CSR agencies, CSCs, and local youth at all levels, which are @ Village level, Mandal/ Block level, District level and State level.

2. In coordination with police Department **full day training** is given to selected MasterTrainers @ State level/ Regional/ District level by the identified experts from ISEA Team, C-DAC Hyderabad.

3. By Associating with **Cyber Dost of MHA**, ISEA implemented cyber Awareness program for general public.

4. Cyber Aware Rallies, Cyber Aware walk/ Run, Roadshows are organized as part of the **awareness week** in the identified areas to **create mass awareness.**

5. All the resource material in the form of soft copy (Presentations. Videos, Posters, Broachers and Hand books) are shared with the police department at State level by ISEA Team, C-DAC, Hyderabad which is further **translated to regional language** and distributed through Police to the general Public during rallies road shows and workshops.

6. All the Hand books created as part of the awareness program have a chapter with **Information on Cyber Laws: IT Act 2000 and IT Act 2008.**