Fake Things

Understanding misinformation & fakenews

भारतीय प्रेस परिषद
PRESS COUNCIL OF INDIA

"Fake news means news, story, information, data and reports which is or are wholly or partly false."

- What is Fake news?
- Types of Fake news
- How to spot Fake news ?
- Dont be a part of Spreading Hoax Messages
- Fake whats app messages
- Fake e-Mail messages
- Fake customer care
- Fake tech support scams
- Laws regulating contents on Social Media

Programme by

सत्यमेव जयते

Ministry of Electronics
and Information Technology
Government of India

For Virus Alerts,Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

Action Group Members

A K Pipal, HoD (HRD), MeitY
Shri.Sitaram Chamarthy
Prof. M S Gaur
Prof. Dr.Dhiren R Patel
Representative of Chairman (CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, Additional Director, MeitY

Honorary Professor. N Balakrishnan
Prof. Sukumar Nandi
Prof. V Kamakoti
Prof. M S Gaur

Dr. Hemant Darbari
Director General, CDAC

Shri G V Raghunathan,
(Retd) Sr Director, MeitY
Shri Magesh E,
Executive Director, CDAC
Shri S K Vyas, MeitY
Shri Ch A S Murty
Mrs K Indra Veni
Mrs Soumya M
Mrs G Jyostna
Mrs Indrakeerthi K
&
ISEA Team Members,
C-DAC Hyderabad

Implemented by

सी-डैक
CDAC

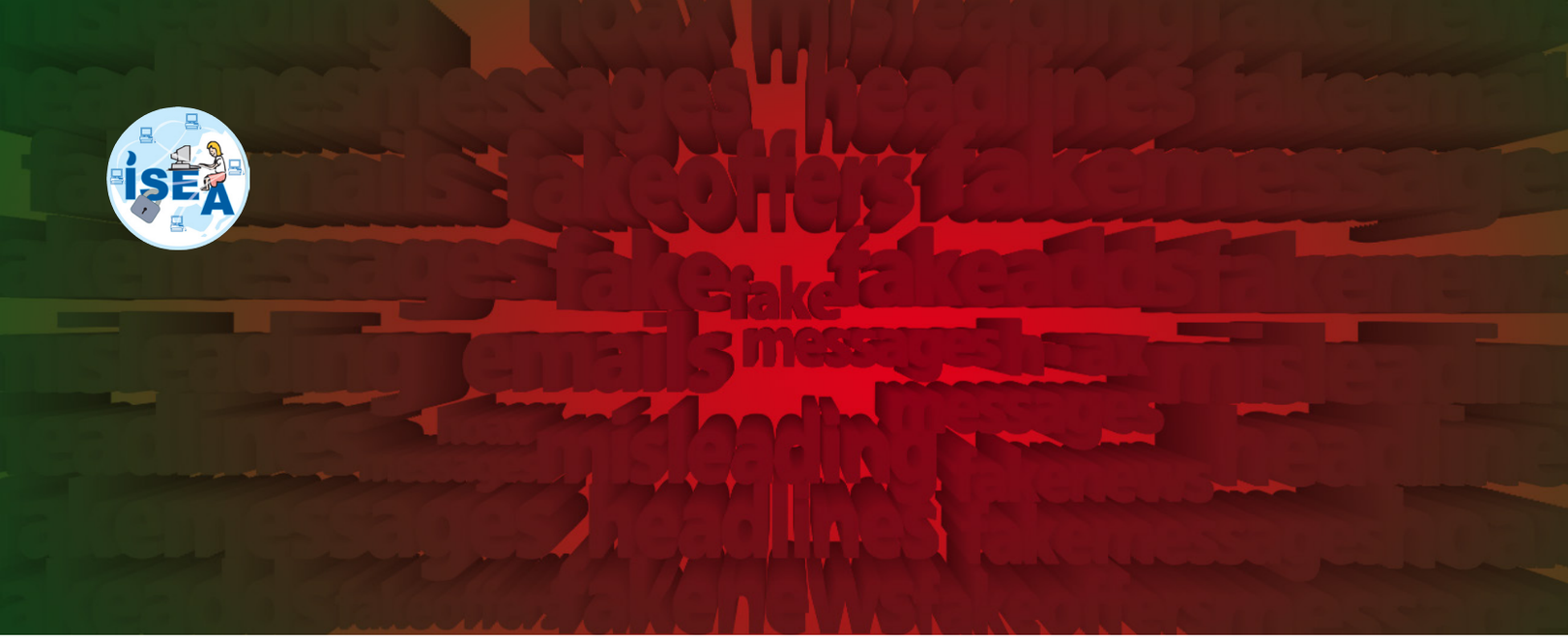
स्वच्छ भारत
एक कदम स्वच्छता की ओर

स्वच्छ भारत
स्वच्छ मोबाइल

Always clean

unwanted / unused apps
history / cookies from browser
saved payment details
virus/malware

from your mobile



What is fake news ?

Social media including the instant messaging Apps have become integral part of our lives. In the era of online communications, spreading of information (or mis information) happens at a very fast pace. Every day we come across various social media feeds, some of which may be true and some may appear to be true. At times it becomes quite difficult to differentiate true information from false information. A News item which contains misrepresented facts to deceive readers, can be treated as fake news. Fake news is nothing but earlier day's rumors which were spread word to word. Only difference is that these rumors were shared person to person so, took time to spread but in today's digital world these false information gets viral and reaches millions in a short span of time. The main agenda behind creation of these false stories may be some may be some lobby to influence people's views to push a political agenda or some monetary gain, or just gaining profit by causing confusion

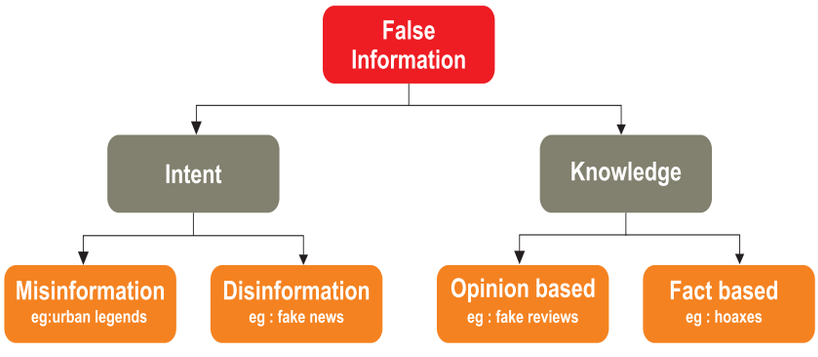
Fake news mainly works with half-truths, twisting them into believable news. People who propagate fake news might fudge the numbers fudge numbers, photoshop or morph images, take a photo from an old source or from another region and misappropriate it with wrong data. The issue of fake news has affected Internet giants like Facebook and Google, who have now started to collaborate with fact-checking organizations to authenticate the legitimacy and origin of the news they show on their feeds. Fake news is our biggest enemy now against which we have to be on guard.

Fake news mainly works with half-truths, twisting them into believable news

Types of fake news

There are differing opinions when it comes to identifying types of fake news. Understanding the reasons for why and how false information is created is important to proactively detect it and mitigate its impact and also the spread of false information can have far-reaching impact.

False information can be categorized based on its intent and knowledge content. According to intent, false information can be categorized as misinformation, which is created without the intent to mislead, and disinformation, which is created with the intent of misleading and deceiving the reader. Both have negative influences, but the latter is arguably more dangerous as its creator's primary aim is defenitely malicious. Based on knowledge, false information is categorized as opinion-based, where a unique ground truth does not exist as in cases of reviewing products on e-commerce websites, or as fact-based, which consists of lies about entities that have unique ground truth value.



However, when it comes to evaluating content online there are various types of fake or misleading news we need to be aware of. These include:

Clickbait
These are stories that are deliberately fabricated to gain more website visitors and increase their advertising revenue. Clickbait stories use sensational headlines to grab attention and drive click-through to the publisher website, normally at the expense of truth or accuracy.

Propaganda
Stories that are created to deliberately mislead audiences, change their opinion by promoting biased point of view or particular political cause or social agenda.Viral video clips which spread sucg misinformation, are part of carefully-designed attempts by some groups with vested intrests to spread false propaganda and gain political mileage in India.

It was an attempt to demean shaikh Mohammad Bin Zayed's goodwill gesture or the UAE's foundations of mutual respect and cultural co exixtence with India for the sake of domestic political gains.

Satire and Parody
Sometimes people use satire to make a point about some incident or specific individual within the society with various kinds of humour which can include elements of parody as well. But the facts shared may not be true. These fake items are published just for fun and entertainment.

Sloppy Journalism
Sometimes reporters or journalists may publish a story with unreliable information or without validating the facts, which can mislead audiences. For example, during the U.S. elections, fashion retailer Urban Outfitters published an Election Day Guide, the guide contained incorrect information telling voters that they needed a 'voter registration card'. This is not required by any state in the U.S. for voting.

Misleading Headings
Stories that are not completely false can be distorted using misleading or sensational headlines. These types of news can spread quickly on social media sites where only headlines and small snippets of the full article are displayed on audience newsfeeds.

Biased /Slanted News
Many people are drawn to news or stories that confirm their own beliefs or biases. Social media news feeds tend to display news and articles that they think we will like based on our personalized searches.

The internet and social media have made it very easy for anyone to publish content on a website, blog or social media profile and are capable of reaching large audiences. With so many people now getting news from social media sites, many content creators/publishers have used this to their advantage. Fake news can be a profitable business, generating large sums of advertising revenue for publishers who create and publish stories that go viral. The more clicks a story gets, the more money online publishers make through advertising revenue and for many publishers' social media is an ideal platform to share content and drive web traffic.

Spotting Fake News On

Social Media & Internet !

Consider the source.

Is it credible, trustworthy, well known? i.e. Consider the source from a reputed news paper, news channel or online news website.

Read beyond headline.

Does the article seem balanced, fair and objective? Study it critically, detecting the tone and viewpoint while checking your bias at the door.

Check the url.

Does it seem legitimate? Does the website have a track record of being reliable? Many sites use similar sites ending with .io .co .com

Disregard your bias.

It's easier to believe stories that confirm your internal views. But the next time you see on social media post that flames your political, racial or religious views.

Who's the author?

Did you search for the author's name online to see if they are credible and well respected? Many fake sites won't use the author's name.

Get a second opinion

If a story makes you very angry, dig deeper, consult known contact or use debunking sites before forwarding.

Supported by:

Information Security Education & Awareness

www.infosecawareness.in

IT, Electronics & Communications Department

Government of Telangana

Fake news has real consequences.
unk misinformation when ever you can.

tand up and speak up for a change.

END NOW FOUNDATION

ADVOCACY ON DIGITAL SAFETY

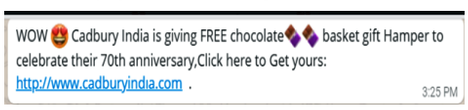
www.endnowfoundation.org

Let us know why fake messages are created and shared in social media

- First of all a website is created
- Google Adsense is linked to that site.

Now they should get traffic because someone should click on their ads so that each time a visitor click on ads each time the website owner earns money.

- So now they copy link and create some fake content and paste that link in that content. You can take the above picture as an example.
- So if you will click on that link you will be automatically redirected to one page where without knowing anything you will be automatically clicked on one add. (Surely we will click because we are attracted towards so called free stuff)
- After redirecting to that page you will see "share to 25 groups to avail this offer" so automatically without thinking for single second you start sharing and in same way they go on earning.



1 × 25 = 25
25 × 25 = 625
625 × 25 = 15625
15625 × 25 = 3,90,625
3,90,625 × 25 = ... it go on increasing to lakhs, millions.....

Just think "why do they give free products for us? Most of us are attracted towards free stuff, just remember we do not get anything for free until unless we work hard, harder.

Google and Facebook have announced new measures to tackle fake news through reporting and flagging tools.

The vast amount of information available online and rise in fake news highlights the need for critical thinking. Children need to develop critical thinking from an early age.

How to spot FAKE NEWS ?

There are a number of things to watch out for when evaluating content online.

1 Take a closer look
Check the source of the story, do you recognize the website? Is it a credible/ reliable source? If you are unfamiliar with the site, look in the about section or find out more information about the author.

2 Look beyond the headline
Check the entire article, many fake news stories use sensational or shocking headlines to grab attention. Often the headlines of fake new stories are in all caps and use exclamation points.

3 Check other sources:
Are other reputable news/media outlets reporting on the story? Are there any sources in the story? If so, check they are reliable or if they even exist!

4 Check the facts
check for published date and time. Fake news stories often contain incorrect dates or altered timelines. It is also a good idea to check when the article was published, is it current or an old news story? Have a check on who is the author.

5 Check your biases:
Are your own views or beliefs affecting your judgment because of news feature or report?

6 Is it a joke?
Mocking sites are popular online and sometimes it is not always clear whether a story is just a joke or parody... Check the website, is it known for creating funny stories?

7 Think before you share

Don't be a part of spreading HOAX MESSAGES

So, before you react to anything you read or see on a social network, think, be very, very suspicious. Here are some case studies.

1 Look for messages that look different

Be cautions to "look out for messages that look different" and to watch out for signs like spelling mistakes in order to determine accuracy of information circulated. Check for unusual characters and spelling mistakes to establish authenticity. Fake news "often" goes viral and just because "a message is shared many times, does not make it true".

Example:
A fake WhatsApp message created by an individual during the Kerala floods where he mentioned his account number instead of CMRDF original account. He was caught by the police so after the message was found fake.

The Kerala Police have initiated legal action against a native of Tiruchirappalli for allegedly attempting to dupe the public by propagating messages on social media in which he advertised his bank account number as that of the Chief Minister's Distress Relief Fund.

2 Click before you share

If any social media story has an eye-catching headline that tempts you to share or forward it even before you read it? Remember to click on the story, read and check whether it's genuine or not.

It is important to open the link before you re-tweet, share or like it. Fake stories are designed to mislead you to maximize profit or spread of disinformation. Many a time, rumors makers use shortened URLs and catchy headlines to make it look like the source is a reputed one. Never nod off your forwarding impulse with a "forwarded as received" disclaimer before sharing.

3 Question everything you read

According to research studies it was found that the cognitive psychological profile of people who fall prey to fake news, found that those who apply analytical thinking to what they are reading are less inclined to believe what they are reading. With everything you read or view online, the first step should be to apply your brain and be willing to disbelieve. Even if you read something or watch a video, from dependable sources online, always use your analytical powers to question the intent and honesty of the stories.

4 Is the URL real?

Even if the article seems to be genuine and is published on a website you trust, with the same fonts and layout, it can still be fake. The internet is loaded with tools like Clone Zone that offer easy templates for people to create fake BBC or New York Times articles. Some websites use similar domain names to confuse readers, with one letter of the alphabet different in the address. A fake NYTopinion piece on WikiLeaks recently had the URL "opinion-nytimes.com while the real one is "nytimes.com/pages/opinion". Red flags include ".com.co", ".go.com", ".news", ".limo" versions of known media sites.

Always read it first. Be thoughtful about what you share

Be thoughtful about the unbelievable offers that you receive by WhatsApp or in Social media

Always have a check on the urls received and the legitimacy of the news or any petition before signing.

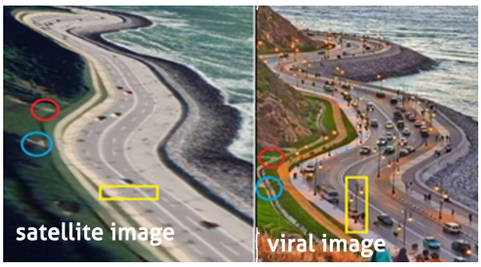
5 Install a browser plug-in

None of the available tools are perfect yet and can also be unsafe, but they are helpful to an extent in pointing out problematic content. Many are available here are a few examples for plug-ins that flag unreliable websites.

- BS Detector (BSdetector.tech, free), which works on Chrome and Mozilla-based browsers, checks all the links on a given webpage with unreliable sources and domains. Free Chrome plug-ins includes Fake News Alert, Fake News Detector and Fake News Blocker. All these cross-check the site you are on with a curated list of bad sites.
- There are few tools to check the trustworthiness of tweets by computing variables like content, user reputation, and URLs and pictures shared in the tweet.

6 Is the story a hoax?

If the first link you see to a story is from a website you have not heard of, and it asks you to forward it immediately, be suspicious and verify it by looking at other reliable sources. Cross-check on websites, news channels that can verify the news you have just read, or websites that have a good reputation." A quick Google search on the subject will tell you if the story has been carried by just one site or other reputed media sites too.



7 Cross-check with a fact-checking organization

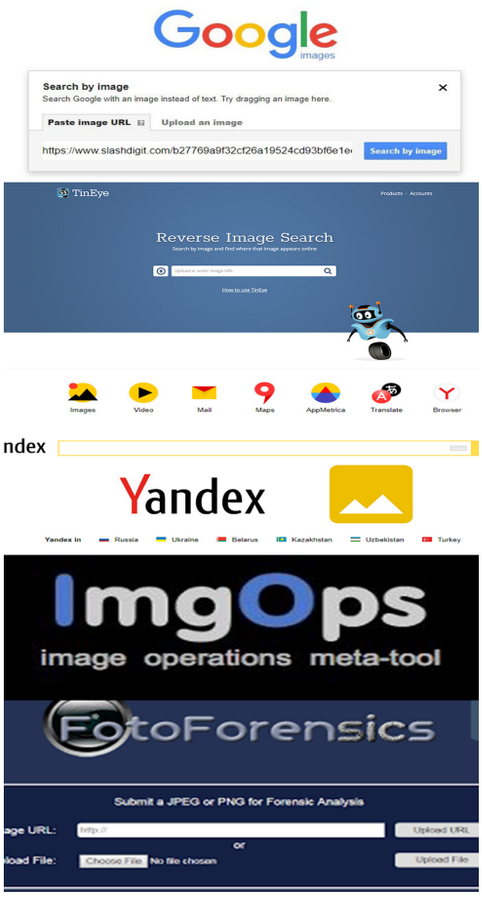
As an industry, fact-checking is fast spreading in India.India has a few fact-checking websites that assess trending, viral stories on Facebook, WhatsApp and Twitter and bust hoaxes. Many fact checking organisations are there to verify the news a few to mention are sites like Altnews.in, Boomlive.in, Factchecker.in, Smxhoaxslayer.com and Check4spam.com.

8 Is this image doctored?

A bridge that looks like an engineering marvel; a road from Morocco passed off as the road to Char Dham. Some people could easily make out that roads in India are not left-hand drive and that there is no sea en route to Char Dham in the Himalayas.

Reverse image search is a great first step to find out if the image you are seeing is genuine.

1. Open the image in Images.google.com, Yandex.com or Tineye.com and find out where else it has been published.
2. Another useful plug-in for both Chrome and Firefox is RevEye, which searches for the same image across different search engines. The original one generally has the largest image size, and would have been posted first.
3. ImgOps.com reveals information like GPS coordinates, the date of publication, the date that the picture was captured.
4. To check how much an image has been Photoshopped, go to Izitru.com or FotoForensics.com—both can detect patterns that indicate heavy editing.



9 If it's fake, flag it

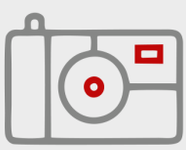
If you find that a forward or an image you have been sent is a fake, flag it. Do not share or promote something unless you are certain that it's true but definitely talk it if it's fake. Tell your friends, flag it on every social network, and inform fact-checking websites to stop the story from going viral.

Spotting Fake News

Photo Verification

Identify and verify the original source and the content (including location, date and approximate time)

Use tools like FotoForensics/Find exif for information on camera model/timestamp



Try to find multiple sources. Challenge the original source to prove veracity - ask follow up questions

Using Wolfram Alpha, check if weather captured in photo (e.g. sunny, rainy, overcast) was actually the weather in that area

Use tools like TinEye/Reverse Image Search on Google

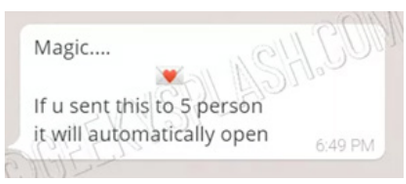
Source: www.factly.in, www.groundviews.org & www.google.com

Some examples of
FAKE WHATSAPP MESSAGES

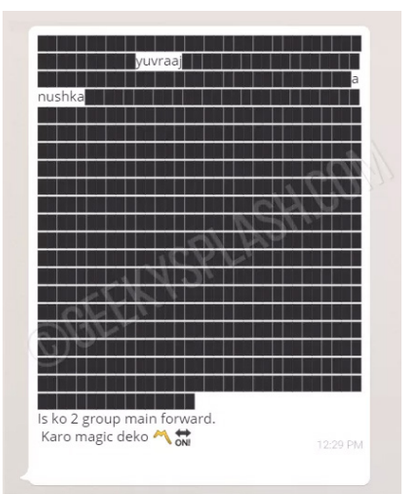
CASE 1 :

Fake chain messages in WhatsApp: Very often we receive such messages and without thinking we forward to our friends. We are unaware of the source of such kinds of messages as well as the reason behind creating such messages.

Example 1: Be cautious about forwarding unrelated messages in groups.



Example 2: Let's see another example where text written below says that if you forward this message to min of two groups, you will see the magic. And the image has names of famous celebrities to make you curious and forward in groups to see something unexpected.



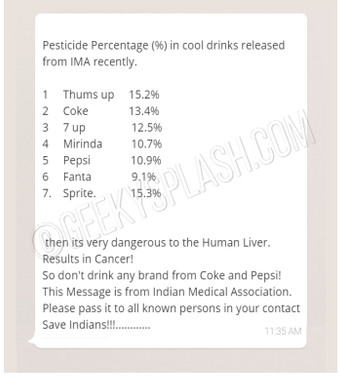
Example 3: WhatsApp charges Mobile Send this message to two groups and WhatsApp will automatically charge you're mobile.

Ask yourself,
Can it happen ?

CASE 2 :

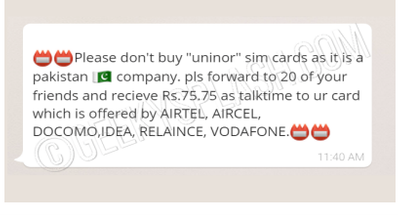
Defame a product by spreading fake news through WhatsApp message: Many of us may have come across messages that are used to defame a product. When you get any messages defaming product its better to check the fact associated with it before forwarding it or being a part of false news spread against a product.

Example 1: Indian Medical Association – IMA announced that these cool drinks contain pesticides. According to this logic almost 80% of Indians are already victims of Cancer!



Example 2 : You might have encountered the same text with a different cool drink like Coca Cola, Maaza, Pepsi, etc. which says that the product was contaminated by a worker of the company.

Example 3: This one is a similar case as mentioned above.



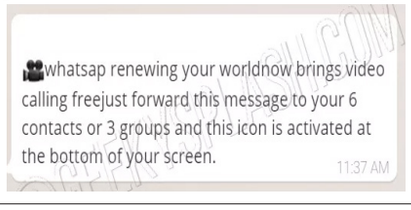
Example 4 : This one is a similar case as mentioned above.

CASE 3 :

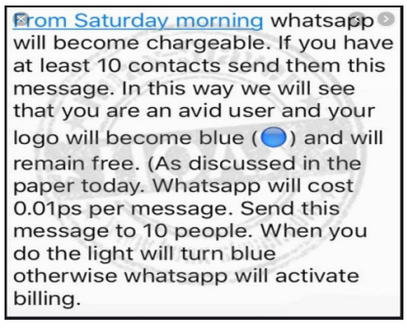
WhatsApp users get fake messages asking them to forward the message to continue using the App

Example 1: This message was widely circulted by people fearing the whats app will get charged.

Example 2 : Check for spelling & grammer mistakes in the meessage

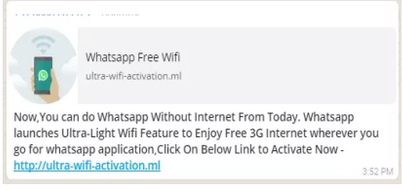


Example 3: This will allegedly show WhatsApp the recipient is an avid user and once sent to the contacts your WhatsApp logo, which is usually green, will turn blue and your messages will remain free.

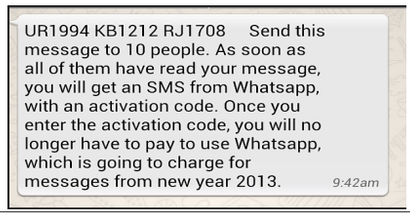


www.
InfoSec
awareness.in

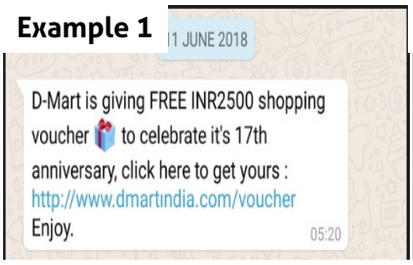
Example 4 :
Fake links , think before you click . is it possible to use without internet by anymeans?



Example 5 : This message urged the users to forward the message to minimum of 10 people to receive a activation code which will make your service free of cost.



Example 1



Example 2

Example 3

CASE 4 :

WhatsApp messages with fake links offering exciting offers:

When you receive such messages, first try to check authenticity of the link given in the message. This type of promotion is always for self-promotion of the particular website. The message with offers will generally have a link. It promises you a discount at online shopping site. In return, you have to fill in a short survey that asks you to answer various personal questions. This survey has absolutely nothing to do with the online shopping site, and everything to do with stealing your data. Actually the link takes you to a counterfeit website, and when you plug your details in it goes straight to the scammers.

Example 1: These messages are click bait messages to increase the traffic of a particular website

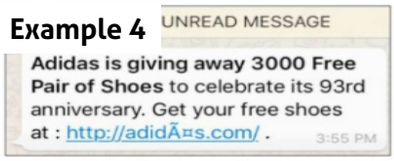
Example 2 : Double check the offers by visiting the website rather than clicking on the link which came along with the message.

Example 3: Don't Hurry, Think before you click , don't get carried away by the exciting offers

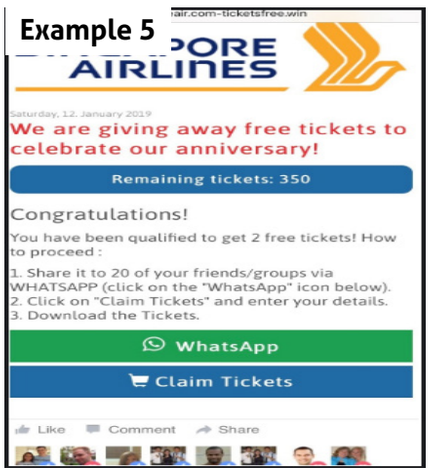
Example 4 :
Check official websites for authentic offers on branded products.

Example 5 : Make use of available search engine to verify the facts presented. Check for the logos and also cross check the details given in the message regarding anniversary of Singapore airlines. If they are providing offers it would definitely reflect in their website.

Example 4



Example 5



References :
http://www.tutorialspan.com/how-to-check-fake-whatsapp-messages/
https://www.geekysplash.com/25-hilarious-whatsapp-hoax-texts-and-forwarded-messages/

Fake WhatsApp messages

How can hoax messages be identified?

1. Grammatical errors is likely to be found
2. Usually promises rewards if you share the message
3. The message claims that it is from a legitimate source
4. There are many fake URL used in these type of messages which leads to malware-infected websites or may ask you for your personal details

Spotting Fake News

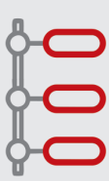
Video Verification

Identify and verify the original source and the content (including location, date and approximate time)

What information does social media/affiliated accounts give that indicate location, activity, reliability, bias or agenda of uploader?

Try to find multiple sources. Challenge the original source to prove veracity - ask follow up questions

How long have these accounts been active? How active are they?



Use Amnesty International's DataViewer (https://citizenevidence. amnestyusa.org)

Is the person listed in online databases/ networking platforms e.g. Linkedln?

Scrutinise uploader's name and date of upload

Are other accounts, including social media, a blog or website -affiliated with the uploader?

Source: www.factly.in, www.groundviews.org & www.google.com

Supported by:

Information Security Education & Awareness
www.infosecawareness.in

IT, Electronics & Communications Department
Government of Telangana

Fake news has real consequences.
unk misinformation when ever you can.

tand up and speak up for a change.

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY
www.endnowfoundation.org

FAKE EMAIL MESSAGES

CASE 1 :

Fraudulent Income Tax Refund E-mail from Fake Income Tax Web Sites

These days income tax assessee's face various Fraudulent Income Tax Refund E-mail from Fake Income Tax Web Sites. These emails are appear to have been sent from Income Tax Department, but were actually online traps to dupe unsuspecting victims.

What to do when someone receives Fraudulent Income Tax Refund E-mail :

If someone receive an e-mail from someone claiming to be the authorized by Income Tax Department or directing you to an Income Tax website:

- Do not reply.
- Do not open any attachments. Attachments may contain malicious code that will infect your computer.
- Do not click on any links. If you clicked on links in a suspicious e-mail or phishing website then do not enter confidential information like bank account, credit card details.
- Do not cut and paste the link from the message into your browsers, phishers can make link look like real, but it actually send you to different websites.
- Use anti-virus software, anti-spyware, and a firewall and keep them updated. Some phishing e-mails contain software that can harm your computer or track your activities on the internet without your knowledge. Anti-virus & Anti-spyware software and firewall can protect you from inadvertently accepting such unwanted files.

If someone receives an e-mail or find a website is pretending to be of Income Tax Department, forward the e-mail or website URL to phishing@incometax.gov.in. A copy may also be forwarded to incident@cert-in.org.in

CASE 2 :

Fake lottery email

Every month, thousands of these email messages are sent out by scammers to trick their potential victims into stealing their personal information and/or sending money.

CASE 3 :

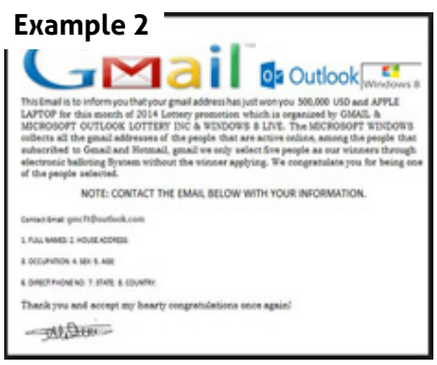
Fake email requesting banking details

Example 1: An email with logo of naukri.com but the actual message not sent from naukri instead from job4u.

Example 1

Example 2: At first glance, the email in looked official enough. The Bank of America logo had a professional appearance. With respect to the email upgrading servers would not have resulted in my losing access to my account. When you receive such emails first try login to your bank account through original bank website rather than clicking on the link to authenticate the message.

Example 2



Never send your personal information to anyone in an email message or send money to someone who contacted you via email message.

Check the sender's details closely for any discrepancies

Check with bank websites rather than clicking on any link

E-MAIL SECURITY

Use strong and easy to remember password or pick a passphrase

Never send sensitive details like password or credit/ debit card numbers through e-mails

Never click on web-links in your e-mail. Always type or copy paste the links in address bar

Delete chain e-mails and junk e-mail. Do not forward or reply to any of them

Avoid the e-mail when the sender is unknown or the attachment has a doubtful name

Never open attachments with double file extensions such as info.BMP.EXE or info.TXT.VBS

Avoid filling forms through e-mail links which ask for personal information

Don't open/ forward/ reply and also never click on links / attachments in unsolicited e-mails

Spotting Fake News

10 Types of Mis-and Dis-information

FALSE CONNECTION

When headlines, visuals or captions don't support the content

IMPOSTER CONTENT

When genuine sources are impersonated

FALSE CONTEXT

When genuine content is shared with false contextual information

FABRICATED CONTENT

Content that is 100% false, designed to deceive and do harm

MANIPULATED CONTENT

When genuine information or imagery is manipulated to deceive

PROPAGANDA

When content is used to manage attitudes, values and knowledge

SATIRE OR PARODY

No intention to cause harm but has potential to fool

SPONSORED CONTENT

Advertising or PR disguised as editorial content

MISLEADING CONTENT

Misleading use of information to frame an issue or individual

Source: www.factly.in, www.groundviews.org & www.google.com

Supported by:

Information Security Education & Awareness
www.infosecawareness.in

IT, Electronics & Communications Department
Government of Telangana

Fake news has real consequences.
unk misinformation when ever you can.

tand up and speak up for a change.

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY
www.endnowfoundation.org

FAKE POST in facebook

CASE 1 :

Two Lynched In Assam after Mob Suspects Them to Be 'Child-Lifters' Following Fake FB Post

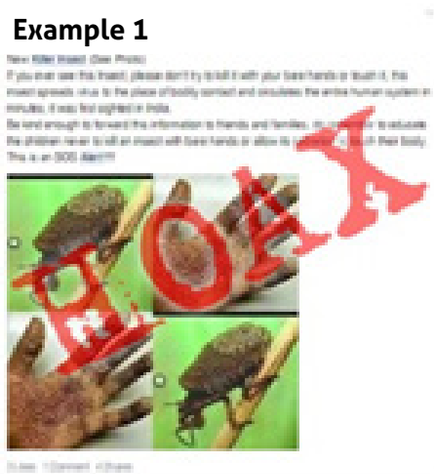
Fake news on social media claims lives of two artistes who looked 'suspicious.' Two youths were lynched in Assam's Karbi Anglong district after a fake post about 'child abductors' on social media went viral. This comes less than a fortnight after communal tensions in Shillong, which were triggered by rumors circulating on the Facebook-owned WhatsApp messaging service.

Example 1: A series of warnings have been circulating the Internet warning of a "new killer insect" from India that – when touched – results in horrific injuries, even death.

Example 2: Pictures of fake Indian currencies are doing rounds on social media. Beware.

- Fake Rs 1000 notes pictures have been circulated via social media.
- RBI has not released any Rs 1000 notes or Rs 1000 coins.

Example 1



Example 2

FAKE

Customer care/Toll free numbers

Save yourself from fake customer care numbers....!

When we face an issue with any product or service, most of us will try to search for customer care/ toll free numbers for assistance. New type of scam has come to the limelight where fraudsters post fake customer support numbers online, and they also find ways to make their numbers appear at the top of your Google search. Customers who call are divulged by offers and prizes. And these offers keep changing as well. They also convince the customers who call on fake toll free/ customer care number as official representative and collect sensitive information under the guise of helping them. The main motto behind the fake customer care /toll free numbers is to collect personal information. This fake phone number s is just one digit different from those of legitimate companies. Several cases are reported and this type of scam is on the rise where fake customer care executives elicit information like bank account details, debit/credit card or even OTP from the customer on the pretext of helping them.

Customer loses money by using fake customer care numbers that pop up

CASE 1 :

With many UPI based apps facilitating payment of utility bills, most of us moved to UPI based apps for paying utility bills considering the ease of payment and attractive cashback offers. With the increasing number of users fraudsters started targeting these apps through fake customer care numbers.

A case was filed by a victim, who was cheated of ₹96,000 by a fraudster who posted his number as Google Pay customer care online. The victim tried to pay his electricity bill using Google Pay mobile application, but he faced some error in the transaction. The complainant then searched for the online payment system's customer care number on the internet and contacted it. When the complainant called on the number, the cyber fraudster, posed as an official from Google Pay and told the victim that it was a common issue being faced by many users and would be resolved in minutes. The fraudster then sent a collect request to the complainant and asked him to click on it. The complainant clicked on the link, Rs 96,000 got transferred from his account. Later when the transaction was done, the complainant realized that he was been cheated. In case of UPI scams, the fraudster uses the 'Request Money' option to dupe people

https://www.freepressjournal.in/mumbai/mumbai-31-year-old-duped-of-rs-96000-by-online-fraudster-who-posted-his-number-as-google-pay-customer-care

CASE 2 :

A customer places an order through the well-known food delivery company. She was unhappy with the quality of food delivered and ought to raise a complaint seeking refund. She does a google search and gets hold of the customer care number and places her complaint on the food she received. The customer care executive assures the refund within 24 Hrs and collects the banking details for the refund process. After some time she received messages from her bank account showing zero balance. Similar complaints were received from customers and the food delivery company filed a complaint to the police seeking an investigation. They also notified the police that they do not have a customer care number and they address the complaints through a chat service available on their application. Complaints can also be registered through official website.

The customer had called on the number 9*******and was told the refund amount could be transferred immediately via Google Pay and she would have to download a mobile application called Remote desktop application. On following the steps dictated by the voice on phone, all the money in the bank account - Rs 17,286 - got debited.

CASE 3 :

A similar case where customer was asked to share his unified payment interface (UPI) pin, password and bank details to initiate a refund for his order when he called in the customer care number that he received from google search. He suspected something fishy and shared wrong pin. Soon after the call he received SMS from his bank that two transaction worth 5000 and 10,000 has failed due to incorrect pin.

A case was registered under section 420 (cheating) of IPC and section 66C (identity theft), 66D (impersonation to cheat by using electronic and computer device) of the IT Act.

For more details refer :

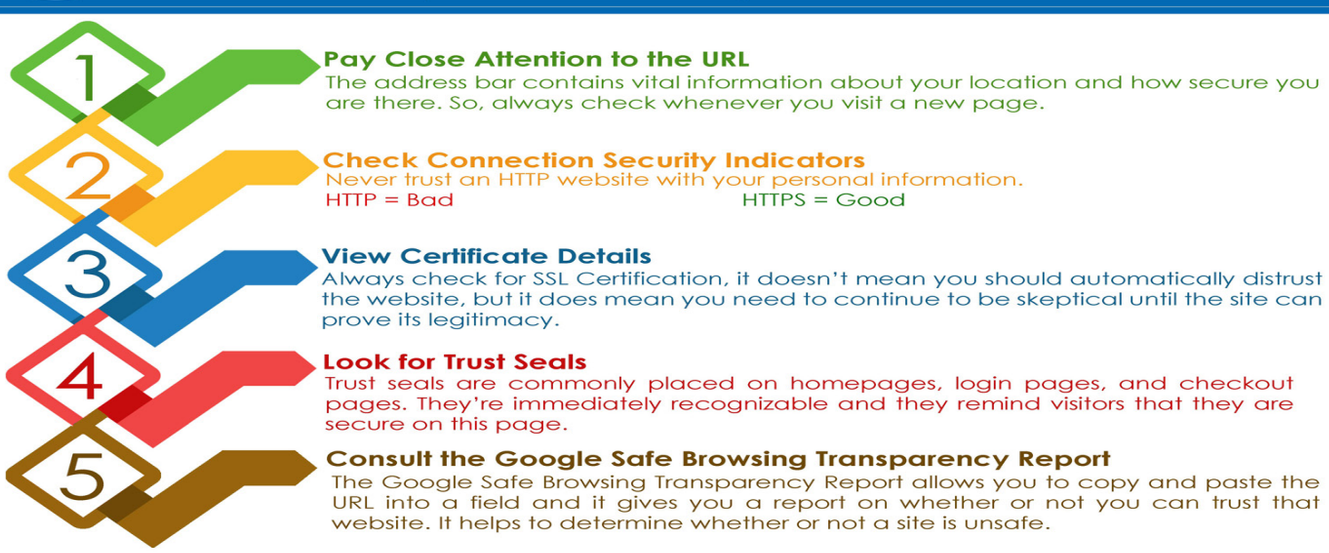
https://economictimes.indiatimes.com/news/politics-and-nation/beware-one-wrong-google-search-can-wipe-out-your-entire-bank-account/articleshow/70671479.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

https://www.indiatoday.in/india/story/customers-duped-zomato-call-centre-fake-customer-care-numbers-google-search-1580678-2019-08-14

The fraudster might either tell to download an app or will send a link on the victim's phone.

In most cases, the app could either be any other remote desktop sharing app. With remote desktop sharing apps, the user gives away the screen sharing code to the fraudster that enables him to see whatever the victim is doing on his/her phone secretly.

5 Ways to Determine if a Website is Fake, Fraudulent, or a Scam



CASE 4 :

Google search fraud - misuse of service that google made to help internet users: Nowadays most of us use e-wallet for our daily transactions. Recently a case was reported where a woman lost Rs 1 lakh through google search fraud. She was facing issues with her e-wallet account and to resolve the issue she searched for customer care number by using google search engine. The search results led her to a customer care number which she believed was an official number. But, in reality the google search resulted in a fake customer care number where a fraudster posed as a customer care executive. She was tricked by the fraudster and got hold of all her banking details for processing the refund. After sometime she got messages from her bank showing money deduction of 1 lakh.

Fraudsters are making use of the feature of google where it allows users to edit contact details and the phone number s of banks & shops and other establishments in google maps & google search. Similar kind of frauds where reported from customers who searched for bank contact details. In google, Even the ranking of websites can be faked. So it is always advisable to check the official website of a particular establishment to get contact information.

CASE 5 :

A similar incident happened with EPFO Provident Fund as well. A fraudster changed the contact details of an EPFO office on Google. When people contacted on that number, the fraudster asked for personal details from the callers and duped several of them.

http://timesofindia.indiatimes.com/articleshow/67148388.cms?utm_source=-contentofinterest&utm_medium=text&utm_campaign=cppst

CASE 6 :

Twitter, a social media platform where users post and interact through tweets. But twitter also is not free from fake accounts and many frauds are reported because many people think tweeting in twitter about issues with respect to a product or service is the best way to get an immediate response for resolving the issues.

Let's have a look how 'Twitter' frauds work: Consider the case of commonly used e wallet 'PhonePe' a UPI based e wallet has the twitter account https://twitter.com/PhonePe.Customers use this account to tweet about issues related to redeeming offers, availing cashback, money transfers, initiating refunds, linking their bank account on PhonePe and more. Fraudsters keep track of what is being posted and react immediately. While responding to customers they tweet in reply fake customer care numbers and ask the customer to call in that number to resolve the issue. Customers call on the fake helpline numbers that the fraudsters have tweeted and report that they haven't received a cashback or request a refund for a failed transaction. To resolve the issue, fraudsters ask customers to share sensitive information such as card details and the OTP details received on their phone. To win a customer's trust, fraudsters may also raise a collect call from their number to the customer's number and promise them a cashback as well. As soon as customers share their card details, OTP or accept the collect call, the money gets transferred from the customer's account to the fraudster's account.

What you should do to protect yourself from frauds ?

Before dialing, double-check the entire phone number including the area code. Hang up if you are:

- Asked to provide personal sensitive information
- Greeted by a recorded or live operator who doesn't mention by name the company or agency you think you have called, but instead offers congratulations for being selected for a survey or qualified to win a prize.
- Offered a prize or "free" product but are first required to provide a debit or credit card for "shipping costs."

References

- *https://www.aarp.org/money/scams-fraud/info-2015/avoid-scam-800-numbers.html*
- *https://www.gadgetsnow.com/slideshows/this-is-the-most-common-google-scam-that-people-are-losing-money-to/The-fraudster-in-disguise-of-a-customer-care-executive-asks-for-personal-details-to-verify-the-call/photolist/71105260.cms//economictimes.indiatimes.com/articleshow/70671479.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst*
- *https://blog.phonepe.com/save-yourself-from-frauds-on-twitter-beware-of-fake-helpline-numbers-8a9e278be65*
- *https://support.microsoft.com/en-in/help/17464*

FAKE

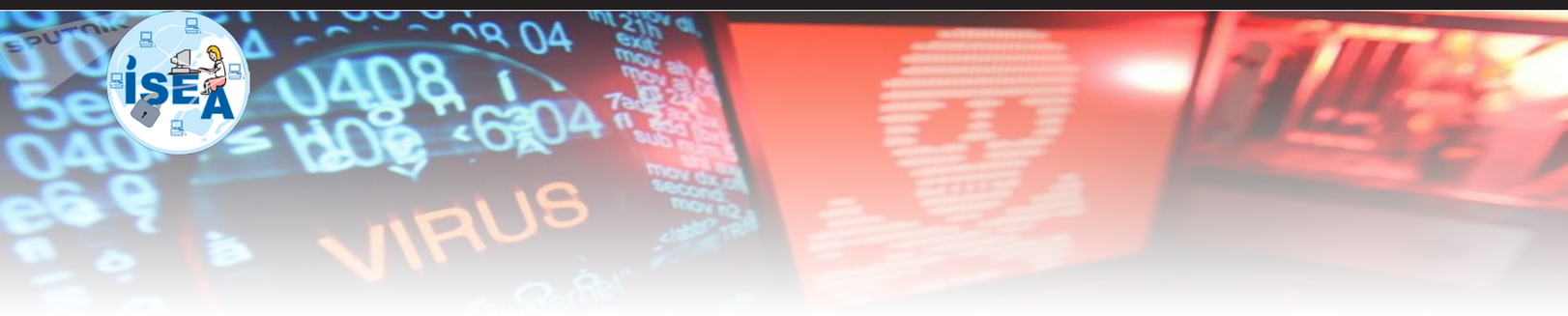
Technical Support calls

As part of creating Awareness we advise users to keep software updated to avoid virus attacks. Fraudsters come out with clever techniques to trick users into calling for fake tech support. There is a new type of fraud which most of the internet users may be less aware. It is called tech support fraud. Tech support fraud is on the rise, and it is getting more sophisticated. This happens when criminals pose as customer or technical support representatives. Fake call centers send alerts to customers saying their PCs have problems and need immediate technical support. They may also offer help with an email or bank account, or software license renewal. But in reality tech support fraudsters are selling expensive tech services under guise of helping them. And they are trying to convince people to grant remote access to their devices so they can get unauthorized access to their data.

A tech support scam targeted a reputed computer manufacturing company and its users. In this case fraudsters knew specific information about users and their PCs. And they used that knowledge to convince victims that the call is legitimate. Reputed Companies don't call and ask for access to your computer or your passwords. Only fraudsters do. Tech support fraudsters try to convince they are legitimate. They will pretend to know about a problem on your computer. They will ask you to open normal files that look alarming to make you think you need help. Once they convinced that the target victim is scared, the fraudsters will pressurize the victim to pay lum sum cash for repairs, new software, and other products and services. They may ask for a credit card number so they can charge the transaction, or request payment by gift card or online money transfer. They might even try to utilize the access to your computer to transmit actual malware that returns personal and financial information from the device, which they can use for identity theft.

If you do need help related to an issue with your computer or any other device, it is always better to directly visit the website or retailer from whom you purchased the product. Also general online searches for toll free number s are also now risky because they lead you to another fraudster.

Let's check out the modus operandi of fraudsters



Fraudsters create fake virus alerts:
Fake pop-ups can attack your computer if you happen to visit a fake website by following a link from a spam email. You might have received the spam mail through an "adware" or "scareware," where malicious codes you can accidentally acquire if you download free software. This may lead to fake warning from a rogue cybersecurity company with an unfamiliar name like Spy Wiper or System Defender or scam pop-ups which often mimic well-known tech brands. To increase the fear of the user, the alert might also accompany a blaring audio, or a long list of supposedly threatening files on your computer, and it won't go away when you try to close your web browser. You will be urged to call a toll-free phone number to speak to a technician or click a link to buy or download (bogus) antivirus software.

Figure 1

Figure 2

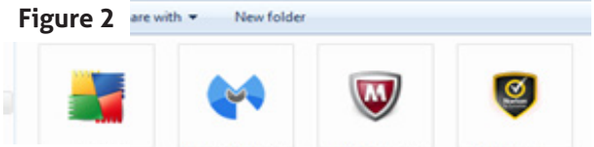
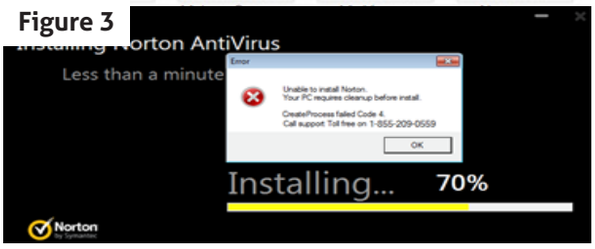


Figure 3



Fraudsters create Lookalike pages:
Fraudsters have set up fake download pages that look unbelievably like the authentic ones. You need to be watchful.

When you click on download the page links to a download, which of course is not the actual software but certainly looks like it as shown in the screen shot: figure (2)

The fraudsters take extra care that they actually hijacked on the real programs and inserted their own piece of code half way through the installation procedure where the user will start receiving warning message and indicating a toll free number for tech support as shown in screen shot. When you call on this toll free number the fraudster will answer the call pretending as official tech support from the original product organization. He will get hold of sensitive information or ask for transferring money to an account to complete the installation process.

Warning Signs

- You get an unsolicited phone call or email from someone claiming to work for a brand-name tech company such as Microsoft or Apple. Those companies say they do not contact customers unless the customer initiates communication.
- A pop-up or blue screen appears on your computer, phone or tablet with a warning that a virus or other malicious program has infected your device.
- The message urges you to immediately call a toll-free number or click a link to get technical help or security software.
- The message contains bad grammar or misspelled words
- You are asked to pay for tech support or other services with a gift card, cash-reload card or wire transfer.

To avoid becoming a victim, follow some basic safety measures.

- Don't give remote access to your computer or payment information to unknown persons
- Don't rely on caller ID as fraudsters use "spoofing" techniques to make it look like they are calling from a legitimate number.
- Don't call the number in pop-up virus alert. Real warnings from your operating system or antivirus program will not ask you to call anyone for support.
- Don't click any links in the pop-up, even to close the window. This could redirect you to a scam site or launch a "dialogue loop," continually serving pop-up messages.
- Don't buy security software from a company you don't know. If the name is unfamiliar, do an internet search to see if it has been linked to adware or scams.
- Don't open previously closed sites if prompted to do so when you restart the browser after getting a scam pop-up.
- Don't share personal information and financial information to someone who calls a few days, weeks or months after you've made a tech support purchase and asks if you were satisfied - it's probably a "refund scam." If you say "No," the caller will ask for bank or credit card information, ostensibly to deposit a refund in your account but actually to steal from you.
- Reach out to the tech company yourself.

If you believe that you are the victim of a tech support scam, please take the following actions:

- Report immediately to the service provider.
- Approach your nearest cyber-cell and file a police complaint
- Call your credit card company and ask to have the charges reversed;
- Check your bank and credit card statements for inaccuracies. If you find any, ask that those charges be reversed, too;
- Uninstall the applications that fraudsters have asked you to install.
- Consider resetting your device.
- Run a full scan for your device with antivirus and anti-malware software's.
- Consider changing your passwords

- *References*
- *https://www.fraud.org/tech_support_scams*
- *https://www.aarp.org/money/scams-fraud/info-2019/tech-support.html*
- *https://www.tmcnet.com/channels/call-center-management/articles/440647-tech-support-fraud-a-growing-problem.htm*

For queries on Information Security
Call us to Toll Free No.

1800 425 6235

Toll Free No. 1800 425 6235

Laws regulating contents on Social Media

Section 66A of the IT Act:
Social media law India is regulated by the Information Technology Act which was enacted in the year 2000 to regulate, control and deal with the issues arising out of the IT. Section 66A of the IT Act has been enacted to regulate the social media law India and assumes importance as it controls and regulates all the legal issues related to social media law India. This section clearly restricts the transmission, posting of messages, mails, comments which can be offensive or unwarranted. The offending message can be in form of text, image, audio, video or any other electronic record which is capable of being transmitted.

Section 499 and 500 of IPC:
Posting offensive messages on social media would be invoking sec 499 and 500 of IPC. Under the IPC, the defamatory statement could be oral or written or in sign language or by visible representation and should be made/ published with intention to harm or with knowledge about its defamatory character (IPC, section 499). Thus, section 499, IPC is wide enough to encompass the publication and dissemination of defamatory content via electronic means. Defamation is punishable under section 500, IPC.

Sections 292-294 of the IPC:
Posting offensive messages on social media would be invoking sec 499 and 500 of IPC. Under the IPC, the defamatory statement could be oral or written or in sign language or by visible representation and should be made/ published with intention to harm or with knowledge about its defamatory character (IPC, section 499). Thus, section 499, IPC is wide enough to encompass the publication and dissemination of defamatory content via electronic means. Defamation is punishable under section 500, IPC.

Guidelines to be followed before forwarding the messages to other member(s) and Groups

DO'S

- ✓ Understand when a message is forwarded
- ✓ Try to check the authenticity of the message
- ✓ Follow some unstated rules of group chat
- ✓ Be responsible for what you post
- ✓ Avoid being part of rumor chain
- ✓ Think Before You Post
- ✓ Double Check for Spelling & Grammar Mistakes
- ✓ Be selective of who you follow & approve as a follower
- ✓ Stay alert

DONT'S

- × Don't forward provocative message, fraudulent messages, undesired content, unwanted messages, religious, communal messages, which are punishable under the IPC.
- × Don't forward the messages which are received from the unauthenticated sources / persons/ groups.
- × Avoid Involving Yourself in a Fight or Argument on Social Media
- × Avoid misuse of Hashtags or Trending Topics
- × Don't accept friend requests from unknown persons
- × Don't get personal or emotional

All the images have been taken from www.googleimages.com

References

- *https://www.financialexpress.com/industry/technology/whatsapp-awareness-top-tips-how-to-spot-fake-news-false-information-and-hoax-messages/1240868/*
- *https://www.thehindu.com/sci-tech/technology/gadgets/going-hoax-busting/article17907886.ece*
- *https://www.livemint.com/Technology/aut4lb3oGkqrc4ZGgDoerO/8-ways-to-spot-fake-news.html*
- *https://www.webwise.ie/teachers/what-is-fake-news/*
- *https://www.quora.com/Why-do-some-people-send-fake-messages-in-WhatsApp*
- *https://www.news18.com/news/tech/tips-tricks-10-whatsapp-dos-and-donts-1013275.html*
- *https://reputation911.com/the-dos-and-donts-of-social-media/*
- *https://www.onlinethreatalerts.com/article/2014/4/2/your-gmail-address-has-just-won-you-500000-usd-and-apple-laptop-lottery-scam/*
- *http://taxindiaupdates.in/fraudulent-income-tax-refund-e-mail/*
- *https://www.consumeraffairs.com/news/bank-of-america-email-scam-still-going-strong-032017.html*
- *http://www.zeebiz.com/india/news-beware-these-pictures-of-fake-rs-1000-notes-coins-are-doing-rounds-on-whatsapp-21144*
- *https://www.thatsnonsense.com/is-there-a-new-killer-insect-from-india-on-the-loose/*

Disclaimer

The content is under review. For any suggestions / feedback, write us to isea@cdac.in

Concept Compiled by
Ch A S Murty
K Indra Veni
Soumya M
E Naresh
K Indra Keerthi
PSS Bharadwaj

Concept Reviewed by
Shri G V Raghunathan,
Retd Senior Director, MeitY
Mrs G Jyostna,
CDAC, Hyderabad
Ms Nisha Dua,
Cyber Safety Evangelist,
Cyber Peace Foundation

Supported by
Shri Anil Rachmalla,
End Now Foundation

Toll Free No. 1800 425 6235

BE AWARE OF FAKE JOB OFFERS

Don't respond to spam mails without verification of the e-mail origin

Avoid job offers that ask you to deposite money

Check for spelling mistakes
Fake job offer mails generally have spelling mistakes and grammatical errors

Always prefer for personal interview
Scammers also conduct telephonisc interview, which can be fake/risky

Don't beleive in emails received from personal mail id. Authentic job offers are sent from company registered e-mails

Never believe in the job offer to which you have not applied or if they ask for your personal information / bank details

For more details / queries on Cyber Security visit or call us to our Toll free number

Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

www.InfoSecawareness.in

1800 425 6235

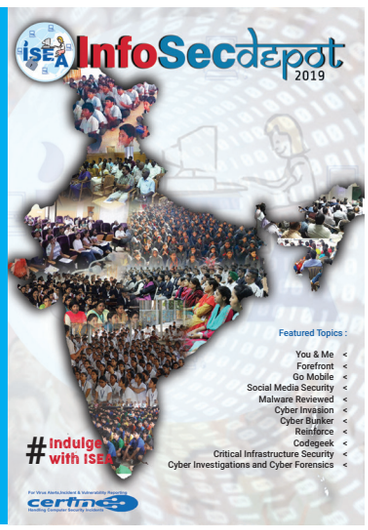
For Virus Alerts,Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

Contribute your

- Articles
- Columns
- Insights

for InfoSec Depot 2020
by 20th November
isea@cdac.in



Subscribe us on

https://www.youtube.com/c/InformationSecurityEducationandAwareness

Follow us on

https://tw/InfoSecAwa

Connect us with

https://www.facebook.com/infosecawareness

For queries on Information security

Call us on Toll Free No.

1800 425 6235

Supported by
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Programme by
Ministry of Electronics & Information Technology, Government of India

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510, Telangana(India)
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)