# Safe, wise and private use of digital tech for community radio journalists

*Source: Tim Unwin*

**Professor Tim Unwin**

**24 July 2024**

**A workshop convened for community radio journalists in Nepal**

ICT4D Collective

https://ict4d.org.uk

# Latest headline news: 20 July 2024

ICT4D Collective

BBC For you Home News Sport Weather iPlayer Sounds

NEWS

Home | InDepth | Israel-Gaza war | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politics

Technology

## CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft says


Joe Tidy
Cyber correspondent, BBC News

20 July 2024

Support the Guardian
Fund independent journalism with £12 per month
Support us

The Guardian
News provider of the year

News | Opinion | Sport | Culture | Lifestyle | More

UK World Climate crisis Ukraine Football Newsletters Business Environment UK politics Education Society Science Tech Global development Obituaries

Microsoft IT outage

Explainer

### What is CrowdStrike, and how did it cause a global Windows outage?

Software made by US cybersecurity company was intended to protect against crashes and disruptions in vital systems - it ended up taking them down

Global IT outage: live updates

Nick Robins-Early


Advertisement

Recruiting? Post your job with us and find the right person today.

Post a job

The Guardian Jobs
Find good company

bci Leading the way to resilience

Membership | Thought Leadership | Events | News

Homepage → News → Microsoft's Global IT Outage: Strategies to manage IT downtime

## Microsoft's Global IT Outage: Strategies to manage IT downtime

# Purpose and outline

- To share with you some of the ideas that have emerged from our work with migrants in Nepal
  - That have been developed further through work in South Africa, Brazil and Mozambique
- Providing you with advice that will hopefully be of value to you personally and in your professional lives
  - Many of the slides are taken from a training deck
- To give you resources that you can use to advise listeners
- An opportunity for discussion and dialogue
  - Please don't hesitate to interrupt!

*Source: Tim Unwin*

# Overall aim of the training deck upon which this workshop builds

*Source: ACORAB*

To provide community radio journalists and volunteers who have little experience of digital tech with a basic introduction to its safe, wise and secure (or private) use, so that they can better

- Avoid the harms and benefit appropriately from the use of digital tech, and
- Share this information with others through their contribution to community radio networks

# Origins of the training resource upon which some of this workshop is based

Builds on a training resource in 7 languages used in Nepal originally created collaboratively with organisations in Nepal as part of Work Package 9 of the MIDEQ Hub, then developed in South Africa and Brazil, and most recently reworked with CAICC in Mozambique. We are grateful to all who have helped to shape it.

ICT4D Collective

# Key message: digital tech can be used to do both good and bad

*Source: Tim Unwin*

## So, be careful how you use it

ICT4D Collective

# What digital technologies do you regularly use?


**Please do share some examples, especially of where such use has been challenging or problematic**

ICT4D Collective

# Digital tech has many positive uses


*Source: Tim Unwin*

Social, economic, cultural and political

---

Improving lives, emergency support, providing access to services…

ICT4D Collective

https://ict4d.org.uk

**But to take advantage of all this, it is essential to use digital tech SAFELY, WISELY, and SECURELY/PRIVATELY – all inter-linked**

*Source: ACORAB*

Journalists have a very special role with respect to the responsible use of digital technologies

ICT4D Collective

# Implications for community radio

- We must make sure our systems are safe and secure
  - For our employees and volunteers
  - For our networks and services
- We have an important role in sharing information about the safe, wise and secure/private use of digital tech
- We all need to improve our own individual cyber security practices
  - There are always new threats

*Source: Tim Unwin*

# 1. Need to begin with basic use of digital tech


*Source: Tim Unwin*

Encouraging people to use the full functionality of their devices and apps

ICT4D Collective

https://ict4d.org.uk

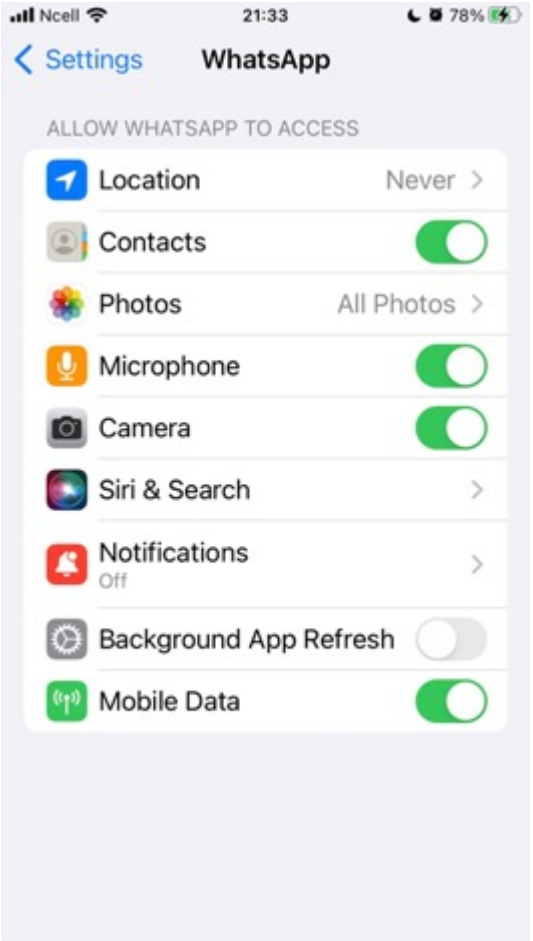
# Key themes about which many people require basic  training

- How to use devices
  - Usually a basic mobile phone or smart phone
  - The importance of access to electricity
- Being connected to a network
  - SIM cards (Subscriber Identity Module)
  - Payment options
- Internet connectivity
  - Access to WiFi and mobile networks
  - Costs and payment options
- Knowing how to use apps

# Useful to distinguish between digital literacy and information literacy

ICT4D Collective

- Digital literacy: gaining trusted advice
  - Knowing how to use devices effectively
    - The full potential of a phone
    - Screens
    - Keyboards
    - Other uses – such as a torch or compass
  - Using software appropriately
    - Learning how to use different apps
      - Understanding and changing the settings
    - Learn how to use social media (Facebook, X/Twitter) and messaging apps (WhatsApp, Signal) safely and securely
- Information literacy:
  - Learn how to know if information is true or not
  - Is the information genuine and authentic?



# Journalists can play a very important role in providing trusted advice

Source: https://www.electronicsforu.com

But how best to do this?

# Discussion

Please use this opportunity to ask questions around the **basics** of using digital tech in Nepal

ICT4D Collective

# 2. The safe use of digital technologies

Source: Tim Unwin

*"Using digital tech so you are not at risk of harm - or of harming others"*

ICT4D Collective

# Key elements to remaining safe: knowing the potential harms

- Knowing the potential harms
  - Being tracked
  - Online abuse and harassment (especially sexual)
  - Bullying
  - Scams and losing money or documents
  - What we give to companies by using digital tech
  - If it seems too good to be true, it probably is…
- But don’t be too afraid of them
  - Act wisely, safely and securely
    - So that you can avoid the harms and benefit from digital tech


https://www.oceanpointins.com/ri-business-insurance/cyber-liability-insurance/8-common-hacking-techniques/

# Key elements to remaining safe online: behaving safely

ICT4D Collective

## What to do 

- Learn about the tech and apps you want to use
- Keep your digital identity safe
- Protect the most vulnerable (e.g. children and elderly)
  - Use parental controls on apps
- Use multiple different passwords
- Treat the digital world as you would the real world

## What not to do:  Don't…

- Share anything that could harm you or others
- Write or say something online that you would not say to someone's face
- Join an app/platform if you don't want to, or are unsure about
- Click on a website link you aren't sure about
- Use geo-location on social media
- Beware of "deep fakes": they are not what they appear to be

# Key elements to remaining safe: technical

- Always report (to app owners and police/authorities) as soon as you can:
  - Phishing: tricking you to do something wrong
    - Never click a link you are unsure of
  - Hacking: compromising a digital system
  - Scams: many varieties of fraud – often to access your money, documents or identity
    - Watch out for scams using QR (Quick Response) codes
- Do a factory reset on any second-hand device
- Authentication
  - Passwords (keep them complex and unique for each app)
    - Longer than 12 characters and using numbers, symbols, and upper- and lower-case letters; or three random words
  - Biometric authentication (fingerprints, face)
  - Multi-factor (several pieces of evidence)
  - Device recognition (securing your devices from malicious actors)
  - Be sure you know who you are really interacting with online or on social media

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|---|---|---|---|---|---|
| 4 | Instantly | Instantly | 3 secs | 6 secs | 9 secs |
| 5 | Instantly | 4 secs | 2 mins | 6 mins | 10 mins |
| 6 | Instantly | 2 mins | 2 hours | 6 hours | 12 hours |
| 7 | 4 secs | 50 mins | 4 days | 2 weeks | 1 month |
| 8 | 37 secs | 22 hours | 8 months | 3 years | 7 years |
| 9 | 6 mins | 3 weeks | 33 years | 161 years | 479 years |
| 10 | 1 hour | 2 years | 1k years | 9k years | 33k years |
| 11 | 10 hours | 44 years | 89k years | 618k years | 2m years |
| 12 | 4 days | 1k years | 4m years | 38m years | 164m years |
| 13 | 1 month | 29k years | 241m years | 2bn years | 11bn years |
| 14 | 1 year | 766k years | 12bn years | 147bn years | 805bn years |
| 15 | 12 years | 19m years | 652bn years | 9tn years | 56tn years |
| 16 | 119 years | 517m years | 33tn years | 566tn years | 3qd years |
| 17 | 1k years | 13bn years | 1qd years | 35qd years | 276qd years |
| 18 | 11k years | 350bn years | 91qd years | 2qn years | 19qn years |

HIVE SYSTEMS

› Hardware: 12 x RTX 4090 | Password hash: bcrypt

# Remember the cultural contexts where you use digital tech

- Know the local cultural and legal contexts where you are living
  - In many  countries it is wise not to take photos of government and military activities
- Remember to respect other people's privacy and don't take photos of them without permission
  - Especially women and families
- Keep your selfies to yourself
- Don't share pictures of your children publicly

*Source: Tim Unwin*

# Specific recommendations in dangerous or violent contexts

- Never share personal information
  - Even with people you trust (you or they may be compromised)
- Consider very carefully whether to use location tracking on your devices
  - Just like your friends, people with bad intentions will also know where you are
- Only use messaging apps with high levels of encryption
- Always carry a backup phone (from which the battery can be removed) for emergency use
  - Consider having relevant medical information on this phone
- Always use a VPN
- Regularly back up your data to a secure, encrypted external hard drive
- Do not use digital technology in any way that could put others at risk
- Remember that group chats are highly susceptible to being compromised

# Discussion

Please this opportunity to ask questions about the **safe** use of digital tech

ICT4D Collective

# 3. Using digital tech wisely

*Source: Tim Unwin*

*"Using digital tech with good judgement and knowledge"*

# Key elements to wise use of digital tech: what to do

- Do use it productively for what you want to use it for
  - and not for what companies or governments want you to use it for
- Do be very careful about what you post online
- Do learn properly how to use the tech and apps you have
  - Read the terms and conditions
  - Adjust the settings (remember parental controls)
- Do remember that everything “posted” remains online somewhere for ever
- Do be thoughtful and polite on social media
- Do take time away from digital tech
- Do think about creating multiple identities/e-mails (with a separate one for purchases)
  - And keep a “clean” basic phone for emergencies

# Key elements to wise use of digital tech: what not to do

- Don’t post anything you would not want everyone to see
  - Who can see what you post?
  - Check privacy settings
  - Never post when you are upset or distressed
- Don’t ever respond to messages/links you do not trust
  - Especially those pretending to be from a finance company
- Don’t waste too much time on
  - Social media
  - Gaming online
  - Online gambling
  - Digital violence
- Don’t waste money
  - As with TikTok gifting
- Don’t take risks through using digital tech
  - As with crypto currency investments
- Don’t respond to provocation if you suffer a “troll” attack
  - It will only make it worse

*Source: Tim Unwin*

# Think twice about sharing images of yourself and your family

- Journalists' families can be especially vulnerable
- What kind of image do you wish to portray of yourself?
  - What will others think of you?
  - Who is watching you?
- Remember that anything you post online is likely to be there for ever
  - Consider using private and secure social networks
  - Or have settings so only your family can see
- Do you know everyone who is following you online?
- Be very careful if you post images of children
  - Paedophilia and child sexual abuse are very real threats
- Always think about your own safety and security
- Do use parental controls

Source: https://www.end-violence.org

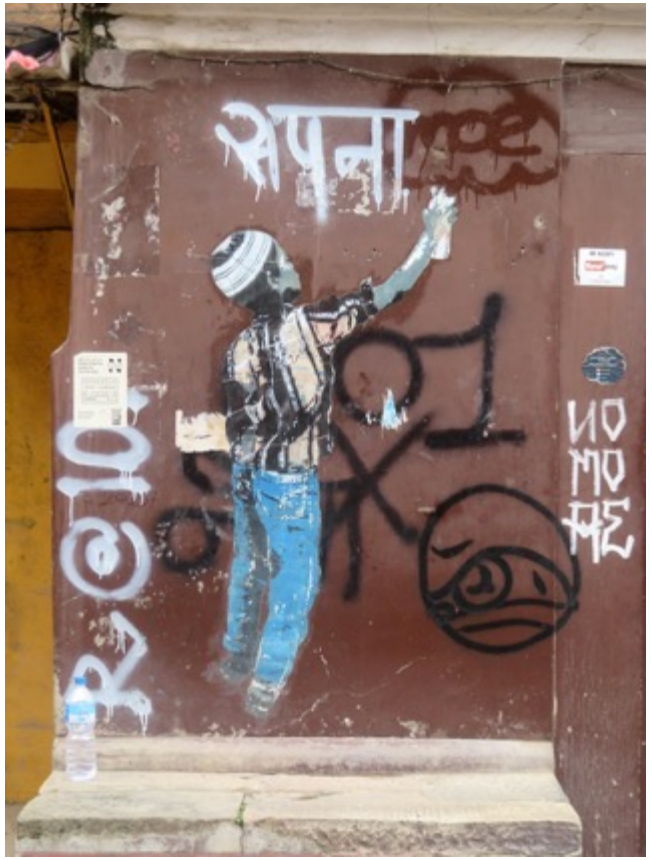
# Dangers of deepfakes: images and videos

- Always check something that surprises you online with other trusted sources
- Be very careful if you play a public role
  - Journalists and civic activists can have their reputations attacked.
  - Public figures face non-consensual online violence
  - Social movements face attacks on their leaders and their narratives.
- Beware of news that seems unusual
  - Rise in fakes contributes to distrust in institutions and a “zero trust” society in which truth is replaced by opinion.
  - Rise of conspiracy campaign
- Attacks on legal processes
  - Challenges to the credibility of videos used for news and evidence harms the legal process
- Personalized AI-generated content uses the psychological profile of someone to target falsified content and reinforces existing biases

Derived in part from https://lab.witness.org/brazil-deepfakes-prepare-now

# Never share fake news

- Never assume that news shared, especially on social media, is true
- Check multiple sources for any news that surprises you
- Use more than one fake/fake news checking app to help validate its truth
- Remember that public service broadcasting is not always reliable
- Use different sources/apps than you usually do to see if they are telling the same story
- Identify generally reliable sources and authors and use them carefully
- Maintain a critical mindset
- Use trusted fact-checking sites (such as NepalFactCheck.org)




*Source: Tim Unwin*

# How to combat disinformation?

- **Check Information**:
  - Always verify information before believing or sharing it on social media. Look for reliable sources and information from a variety of trusted media to ensure accuracy.
- **Question the sources**:
  - Examine sources of information. Be sceptical of information from unknown or unverified sources, and prioritize information from established, trusted institutions.
- **Critical thinking:**
  - Develop critical thinking skills by asking questions like: Does this information make sense? Are there logical inconsistencies or biases in the content? How does this information compare to what I already know? Ask an expert, ask an official person for migration.
- **Media Literacy:**
  - Learn critically to analyse the content present in the media. Understand how media organizations work, their possible biases and how they verify information. Be aware of sensationalism and clickbait.
- **Digital Citizenship**:
  - Share material online responsibly. Be mindful of the content you share and consider its potential impact. Report misinformation to the appropriate platforms or authorities to help combat its spread.


Authored by Unesco Nepal

# Discussion

Community Information Network

**Plase use this opportunity to ask questions and ensure you know about the wise use of digital tech**

ICT4D Collective

# 4. The secure/private use of digital technologies

https://www.smartcitiesworld.net/ai-and-machine-learning/ai-and-machine-learning/ai-expands-capabilities-of-surveillance-and-public-safety-tech

*"Using digital tech securely and with privacy"*

ICT4D Collective

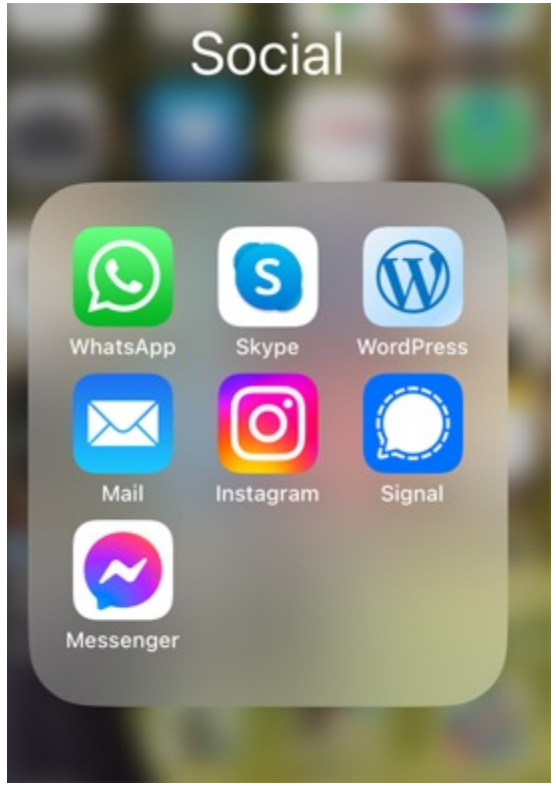
https://www.telegraph.co.uk/news/2018/11/06/chinese-surveillance-grows-stronger-technology-can-recognise/

https://ict4d.org.uk

See also video at https://www.facebook.com/scmp/videos/246038106344865/?t=34

# Key elements to secure use of digital tech – social behaviours

- Being private online
  - Remember that what you post on the Internet is there forever
  - Only post if you are sure that you and related others are happy with this
  - Never share your passwords with anyone
    - Don’t ever share a One-Time Password (OTP) with anyone
  - Whenever possible reject all cookies when visiting websites.
- Secure and private from whom?
  - Governments
    - Remember mobile devices can be used for surveillance
  - Companies
    - Remember that most social media companies make their money from the data you give them for free!
  - Other people
    - Some are eager to exploit you through digital tech

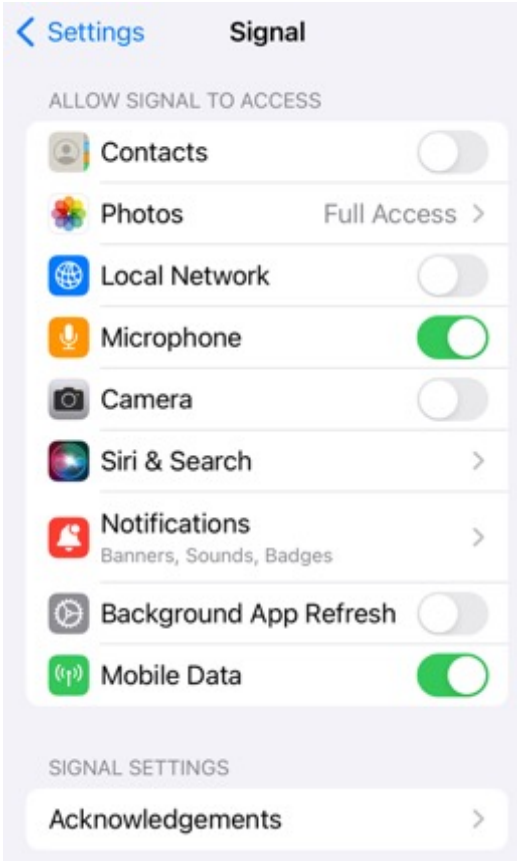



*Source: Tim Unwin*

# Key elements to secure use of digital tech: practical matters

ICT4D Collective

- Keep your software as up-to-date as possible
  - The latest versions of apps usually improve security
- Know how to use your device's settings
  - To make your phone work as you want it to
- Turn off as many cookies (permissions) as possible
  - Only accept necessary cookies (or reject all)
    - So that you don't share all you do online with organisations that you don't want to
- Thing about using free Virtual Private Networks (VPNs) to access the Internet
  - These help to hide a user's digital location and identity and makes them anonymous



# Discussion

Please use this opportunity to ask questions and ensure you know about the **secure and private** use of digital tech

ICT4D Collective

# Conclusions: always think about

*Source: Tim Unwin*

Is it safe?
Is it wise?
Is it secure/private?

ICT4D Collective

https://ict4d.org.uk

# Final reminders: being safe, wise and secure

ICT4D Collective

## What to do

- Learn about how to use your digital tech
- Create robust passwords
- Use multi-factor authentication
- Regularly update your apps and operating systems
- Be thoughtful and polite on social media
- Take time away from digital tech

## What not to do

- Don’t share your passwords
- Don’t become addicted to digital tech
- Don’t respond to messages you do not trust
- Don’t waste money you can’t afford on digital tech and social media
- Don’t send money or documents online to someone you don’t know
- Don’t share anything online you would not want everyone to see

# I have recently changed my mindset to thinking of everything digital as a possible threat

… a cybersecurity attack is likely, not a rare occurrence only affecting those who are stupid

ICT4D Collective

# Our latest guidance for small civil society organisations

ICT4D Collective

**Using digital technologies safely, wisely and securely:**
**a short guide for small civil society organisations**

Tim Unwin

On behalf of the ICT4D Collective
https://ict4d.org.uk

Version 1
July 2024

CC BY SA

ICT4D Collective

***It is not a matter of "if", but "when" your organisation will suffer from a cyber-attack of some kind.***

This could either be direct through your own digital environments, or you could be impacted by an attack on an organisation you work with. It is therefore essential to take all the precautions that you can to keep your staff and those you work with safe. Digital technologies can be used to bring many benefits to organisations, but it is essential to mitigate the harms so that the benefits can be realised.

Is it safe? Is it wise? Is it secure?

This short guide is designed to provide small civil society organisations (especially those with few resources) with basic advice on how to use digital tech safely, wisely and securely/privately. It is not intended to be all-inclusive or highly technical, but instead focuses on things that should be done by all civil society organisations, regardless of their technical or financial capacity. Basic cyber-security is essential, and with evolving technologies the threats are only going to get worse. Adopting these key practices will not necessarily prevent you from being attacked, but they should reduce the chances and impact of such attacks, and will help you to get back online as soon as possible.

How would you react to, or prevent, the following scenarios?

You are the founder of a civil society organisation providing refuge to women who have been subject to violent domestic abuse. Your website showed pictures of some of the women at one of your shelters, and pictures from it were shared on social media. One day, a gang of youths including a man who had previously assaulted one of the women, attacked those at the shelter, and killed two of the women.

You run a large organisation supporting children at risk of living and working on the streets, and keep a record on your computers of the contact details of all your staff, those you work with, and their families. You open the organisation's main computer on arriving at work one day and discover that you cannot access the data and there is a large image and text on your screen saying that your data will be shared openly on the web unless you pay a large ransom that would bankrupt your organisation and ruin your reputation.

The following guidance notes are kept as simple and clear as possible, with minimal use of technical language. Recommendations in red are deemed to be essential; those in blue are highly recommended.

https://ict4d.org.uk/wp-content/uploads/2024/07/udtsws-v2.pdf

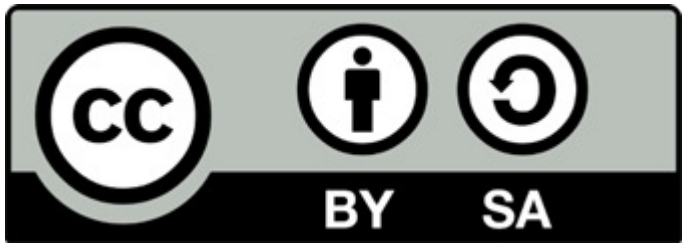
*This slide deck has been developed* in partnership with organisations including ACORAB (Nepal) and CAICC in Mozambique. *It builds in part on research-practice in Nepal by the UNESCO Chair in ICT4D at Royal Holloway University of London (2019-2023) as part of the MIDEQ Hub funded by UKRI GCRF, supplemented by the activities of the ICT4D Collective with individuals and organisations in South Africa in 2024. It builds more specifically on a slide set created by Professor Unwin and Professor Harindranath in 2024 under a project which was funded by the Economic and Social Research Council, which had considerably involvement from colleagues in Brazil. The copyright in the slide set belongs to Royal Holloway and Bedford New College and Professor Tim Unwin. However, the slide set can be used by anyone for free under the creative commons CC-BY-SA licence.*



Social Science Impact Accelerator

ROYAL HOLLOWAY UNIVERSITY OF LONDON

UKRI Economic and Social Research Council



# Additional slides that can be used

*Source: Tim Unwin*

# Disinformation in more detail from TheConversation.com

ICT4D Collective

- False connection between headlines and content
- Manipulated content
- Misleading content
- Fabricated content
- Sponsored content
- False content
- Satire or parody
- Imposter content
- Propaganda
- Error


Source: https://theconversation.com/misinformation-disinformation-and-hoaxes-whats-the-difference-158491

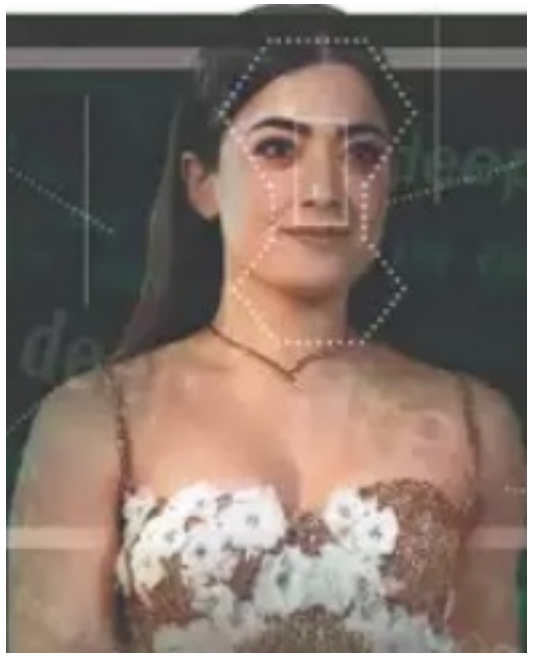
# Avoiding email scams intended to trick you into sharing information

- Do not click on any link in an email unless you are 100% sure it is safe to do so.
  - If there is even the slightest doubt, delete it immediately.
- Do not open or respond to emails that appear suspicious or unusual and ask for personal or financial details.
- Never provide personal data via email or fill in forms that appear when you open an email, as these are often attempts to deceive you.
- If you receive an email from an institution informing you that you need to update your details or change your password, do not follow the instructions and go directly to the institution's website to check if your account is secure.
- Report to your IT department immediately if you work for an organization and think you may have opened an email with a malicious attachment or clicked on a malicious link.
- If you receive an email calendar invite from someone you don't know or it seems suspicious, don't accept it.

# Tips for identifying deepfakes from MIT Media Lab

ICT4D Collective

1. **Pay attention to the face**. High-end DeepFake manipulations are almost always facial transformations.
2. **Pay attention to the cheeks and forehead**. Does the skin appear too smooth or too wrinkly? Is the agedness of the skin similar to the agedness of the hair and eyes? DeepFakes may be incongruent on some dimensions.
3. **Pay attention to the eyes and eyebrows**. Do shadows appear in places that you would expect? DeepFakes may fail to fully represent the natural physics of a scene.
4. **Pay attention to the glasses**. Is there any glare? Is there too much glare? Does the angle of the glare change when the person moves? Once again, DeepFakes may fail to fully represent the natural physics of lighting.
5. **Pay attention to the facial hair or lack thereof**. Does this facial hair look real? DeepFakes might add or remove a mustache, sideburns, or beard. But, DeepFakes may fail to make facial hair transformations fully natural.
6. **Pay attention to facial moles**. Does the mole look real?
7. **Pay attention to blinking**. Does the person blink enough or too much?
8. **Pay attention to the lip movements**. Some deepfakes are based on lip syncing. Do the lip movements look natural?



Source: https://www.media.mit.edu/projects/detect-fakes/overview/