OCHA
centre for humdata
IFRC
ICRC

TIP SHEET ON THE RESPONSIBLE USE OF ONLINE CONFERENCING TOOLS

INTRODUCTION

Recent changes to working conditions have increased the use of online conferencing tools throughout the humanitarian sector. These conferencing technologies are invaluable when face-to-face meetings are impossible, but they also pose a significant information security and data protection risk when not used responsibly. The International Committee of the Red Cross (ICRC) Data Protection Office, the International Federation of Red Cross and Red Crescent Societies, and the Centre for Humanitarian Data have developed this tip sheet to support the responsible use of online conferencing tools by humanitarians around the world.

This tip sheet offers:

- an overview of the **risks** associated with online conferencing, including unauthorized access to meeting rooms/calls, breaches of confidentiality and data protection, third party retention of conferencing data, and malware or social engineering attacks
- **recommendations** to mitigate those risks to help you protect yourself and your organization, maintain security for online conference calls that you initiate, and maintain security for online conferences initiated by persons outside your organization
- a set of **resources** for further reading.

1. RISKS

Some common risks of online conferencing are unauthorized access, breaches of confidentiality and data protection, third party retention of conferencing data, and malware or social engineering attacks.

UNAUTHORIZED ACCESS TO MEETING ROOMS/CALLS

- Meeting rooms/online conferences may be accessed by anyone who has the link if password protection or authentication measures are not in place.
- In cases where links and/or passwords are sent to participants and not changed regularly, they can be reused later to allow participants access to the same meeting room without an invitation.
- It can be difficult to verify the identity of individuals who don’t usually work remotely and have created new profiles or who join using a mobile phone or landline connection.
- While many online conferencing tools now use encryption by default, allowing participants to dial in from landlines creates an unencrypted channel that is vulnerable to interception.

BREACH OF CONFIDENTIALITY AND DATA PROTECTION

- Once someone has gained access to a meeting room/online conference, they can drop in and out of that room and listen in to calls at any time.
- This can (and often does) happen accidentally, e.g. where someone joins a meeting by mistake or joins a meeting early, interrupting the end of another call.
- In some cases, this might be a minor inconvenience, in others confidential matters or personal information could be disclosed; in worst-case scenarios, hackers might be able to join calls and eavesdrop.
- Audio recording is getting easier and some new online conferencing tools include "record" and "transcribe" functions, allowing anyone with access to the meeting, invited or otherwise, to record the conversation.
- Unauthorized recording and transcription of staff and organizational positions and policies significantly increase the risk of unauthorized disclosure of confidential information.
- Even screensharing can compromise information, e.g. by sharing the wrong screen.
- Files that are shared in videoconferencing groups may be downloaded by unauthorized participants.
- Participants may join online conferences from public places or using (insecure) public Wi-Fi networks, amplifying the risk of unauthorized access to information (e.g. eavesdropping, monitoring by external entities or CCTV, interception of data across insecure networks).
- Working from home can amplify these risks because so many "smart homes" and connected devices have voice assistants and audio capture capabilities (e.g. TVs, lighting systems, fridges) which may leak conversation without their owner's knowledge.
- Some online conferencing tools enable "attention tracking", which may be used to profile participants without their consent.

THIRD PARTY RETENTION OF CONFERENCING DATA

- Online conferencing tools generate metadata about the event and participants, including date, duration, device IDs, IP addresses, settings and other variables that can reveal private information.
- Metadata can be combined with other data to profile users and make inferences about their activities and behaviour.
- Online conferencing tools may also retain content data, such as audio recordings, shared messages and attachments.
- Metadata and content data retained by third parties can be used in ways that conference participants are not aware of and/or would not consent to.
- Service providers can be compelled to disclose metadata and content data by law enforcement and security agencies and judicial authorities.
- Data used for non-humanitarian purposes could undermine the neutrality, impartiality and independence of humanitarian organizations.

MALWARE OR SOCIAL ENGINEERING ATTACK

- Sharing files via online conferencing tools may bypass security systems and introduce malware into an organization's system.
- Many tools allow online conference participants to self-identify: people may not be who they say they are.

These risks are serious. Anyone using online conferencing tools should consider the following measures to mitigate these risks.

2. RECOMMENDATIONS

PROTECTING YOURSELF AND YOUR ORGANIZATION

- Familiarize yourself with your organization’s approved online conferencing tools, their features and settings.
- Only use tools approved by your organization when initiating a conference call, and whenever possible when calls are requested by people outside of your organization.
- Only use your organization’s conferencing tools for approved/work purposes.
- Be aware of your surroundings and ensure that only authorized entities can see and hear the information shared during an online conference.
- Take a risk-based approach to online conferencing and adopt increased security measures for higher-risk calls:
  - Consider what is going to be discussed (sensitive issues, personal data, operational matters, unofficial policies or positions, information about vulnerable individuals or groups, etc.).
  - If in doubt, consult your organization’s information classification framework for guidance as to what constitutes internal, restricted and confidential information.
  - **For higher-risk calls**, particularly those initiated by third parties using non-approved conferencing tools, seek further advice, find a suitable alternative (such as a secure messaging app) or be prepared to withdraw if you are concerned about information security, data protection or confidentiality.

MAINTAINING SECURITY FOR CONFERENCE CALLS YOU INITIATE

- Use only online conferencing tools that are approved, configured and verified as secure by your organization.
- Restrict access to online conferences by limiting participation to people you have invited, or use an access code in addition to a link.
- Ensure attendees keep links and codes confidential:
  - If you cannot limit access to specific invitees, request that they do not share these credentials with any other parties.
- Use new invites/links/meeting rooms for every meeting.
- Where a sensitive topic is being discussed, use a unique access code so that only those with the code for that meeting can access the room.
- For recurrent meetings, change the access code regularly (i.e. weekly).
- Do not allow phone dial-in unless a participant cannot take part otherwise.
- Monitor attendance throughout the online conference:
  - Use a dashboard to keep track of who is in the room.
  - Stop the call and notify all attendees if an unidentified party joins the call.
- Disable any function that is not needed in a meeting:
  - e.g. chat, file-sharing, recording or any other unnecessary feature.
- Before anyone shares their screen, remind participants to only share the document/file/page that is relevant, rather than their whole screen.
- Do not record meetings unless:
  - this is necessary for a predefined purpose
  - all participants are informed and agree
  - recordings will be stored securely, encrypted using password protection, and deleted when no longer needed.
- Where available, use the “waiting room”/“green room” function to ensure that:
  - a meeting cannot begin until the host has joined
  - attendees cannot enter until the host approves them.
- Identify all attendees before opening the lines and allowing them to join the call:
  - use one-time pins, identifier codes or other means to identify attendees.
- Lock the call once you have identified all attendees and lines in use.
- Once a call ends, do not stay on the call to have a follow-up or side conversation as the meeting can easily be rejoined by those who left.

MAINTAINING SECURITY FOR CONFERENCE CALLS INITIATED BY PERSONS OUTSIDE YOUR ORGANIZATION

- Take a risk-based approach by considering:
  - whether the subject matter to be discussed is classified or sensitive
  - the situation and security risks facing the organization that has invited you
  - any risks posed by other invitees.
- If you are concerned about the security of the call or the tool being used:
  - discuss this in advance with the host
  - request a pin or access code if none have been issued
  - consider inviting them to use your organization's approved tool.
- If the concerns you raise are not addressed or mitigated, do not take part and do not disclose any information that is not in the public realm.
- At the beginning of the meeting, check whether the call will be recorded.
- Throughout the call, monitor the dashboard of participants to ensure no uninvited parties are attending.

3. RESOURCES

- *Tips for Cybersecurity When Working from Home,* EU Agency for Cybersecurity: https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home
- *Safe Teleworking Tips and Advice,* Europol: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/safe-teleworking-tips-and-advice
- *Home working: Preparing Your Organisation and Staff,* UK National Cyber Security Centre: https://www.ncsc.gov.uk/guidance/home-working
- *Preventing Eavesdropping and Protecting Privacy of Virtual Meetings*, National Institute of Standards and Technology: https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings
- *Protecting Personal Data When Working Remotely and Staying Safe Online during a Pandemic,* Irish Data Protection Commission: https://dataprotection.ie/en/protecting-personal-data-when-working-remotely-0
- *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*, Privacy International and ICRC: https://www.icrc.org/en/download/file/101039/final_web_the_humanitarian_metadata_problem_-_doing_no_harm_in_the_digital_era.pdf
- *Handbook on Data Protection in Humanitarian Action*, ICRC and Brussels Privacy Hub (see Chapter 11 on messaging apps): https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action
- *Guidance Note on Data Incident Management,* The Centre for Humanitarian Data and Jackson Institute for Global Affairs at Yale University: https://centre.humdata.org/guidance-note-data-incident-management/

facebook.com/icrc
twitter.com/icrc
instagram.com/icrc

Centre for Humanitarian Data
UN Office for the Coordination
of Humanitarian Affairs
Fluwelen Burgwal 58
2511 CJ, The Hague, The Netherlands
centre.humdata.org

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org

International Federation of Red Cross and Red Crescent Societies
Chemin des Crêts 17
Petit-Saconnex 1209 Geneva
Switzerland
Ifrc.org

4459/002 04.2020