保護自己免於遭受「科技促成的性別暴力」（Technology- Facilitated Gender-Based Violence, 簡稱 TFGBV）的五個建議

近年來，女性記者和少數族裔記者在工作上遭受攻擊的情況呈現指數成長，包含騷擾和數位暴力的攻擊，迫使記者噤聲。每當一名記者被迫沉默，我們就失去一個寶貴的聲音，新聞觀點的多樣性也因此降低。

2020 年，1,210 接受調查的女性記者中，有將近四分之三人表示，她們經歷過網路霸凌、騷擾、威嚇和攻擊，其中有 20%的受訪者表示遭受現實生活中的霸凌與攻擊，他們相信這些線下的霸凌與攻擊是由「科技促成的性別暴力」（technology-facilitated gender-based violence, TFGBV）所引發[1]。

以下五個防範 TFGBV 的建議是根基於證據，有 Dart Centre Asia Pacific (DCAP) 的專家意見，以及完成由 DCAP 提供、Google 新聞倡議（Google News Initiative, GNI）資助 TFGBV 獎學金計畫的記者們，所提供的親身經歷。

完成 TFGBV 獎學金計畫的記者們，將此五個建議翻譯成多國語言，包括印度文、菲律賓文、斐濟文和中文。更多的語言可以到 Dart Centre Asia Pacific 的網站下載，連結如下:
https://dartcenter.org/asia-pacific

1. 精熟社群媒體（Be social-media savvy）

- 了解自己所使用的數位平台，包含在這些平台上常見的威脅手段。
- 參加如何在社群媒體自我防衛的相關課程，以學會辨識網路霸凌、以及對女性的影響。澳洲電子安全委員會提供一系列免費的網路課程，可以幫助記者們如何安全地設置社群媒體帳戶和個人檔案。這系列的網路課程還涵蓋了如何透過靜音（例如：關閉提醒）、封鎖（例如：列入黑名單）和舉報來處理網路霸凌 (https://www.esafety.gov.au/)。
- 瞭解您的國家針對 TFGBV、以及記者安全的相關法律，並理解這些法律是如何被執行的。
- 瞭解哪些平台最容易讓您受到攻擊與傷害（如：臉書、推特、Linkedln，Instagram 等）。

[1] Posetti, J., & Shabbir, N. (2022). The chilling: A global study of online violence against women journalists.

2. 強化您的網路使用安全機制（Bolster your cybersecurity）

- 使用長密碼（最好是一串單字和符號的混合）、永遠不要重複使用相同的密碼、除了密碼，最好額外設立安全問題，並且在您的重要個人帳戶和工作用帳戶（如電子郵件、社群媒體、銀行帳戶）上設置雙重身份驗證。
- 盡量將個人資料和工作檔案分開。
- 限制公開分享的個人資料（如，避免展示孩子的照片、可識別的地標、寵物等）。
- 不要使用工作用的電子郵件處理私人檔案，也不要在私人帳號，放自己的工作用電子郵件。
- 工作帳戶和私人帳戶不要放上相同的個人照片（例如：頭貼）。
- 不要使用相同的用戶名稱與暱稱，尤其在您希望保持社交距離的平台上。
- 和朋友討論標記問題（tagging）！（例如，您可能不希望他們在分享工作相關事務時，標記您的私人帳戶）
- 為保護隱私，建議使用 VPN。
- 為防止被肉搜（doxxing），請在 Google 上搜尋您自己的名字，查看有關您的哪些個資會顯示出來（可能是您的地址、電話號碼、可以聯繫到您的任何個人資料）。也可以單獨搜尋您的電話號碼或其他個人資料，查看是否有相關結果。如果發現您的個資是公開的，可以使用以下表單，要求 Google 從搜尋結果中刪除這些個資：https://reportcontent.google.com/forms/rtbf
- 清楚了解您網路檔案上個人資料的公開程度（包含圖片和影片）。

3. 紀錄並舉報科技促成的性別暴力（Document and report TFGBV）

- 記錄下任何 TFGBV 的實際案例。如果您舉報了網路霸凌內容，並成功刪除這些內容，您可能會失去寶貴的證據。因此，記得先保存證據，包括：電子郵件、語音郵件和任何文字訊息。也可以直接螢幕截圖社群媒體內容，並盡可能直接複製連結。
- 確保檔案是用安全的且多種方式留存。
- 評估和監測威脅的來源、特徵和發生頻率。仔細考慮威脅是否會由線上移轉至線下。您可以根據騷擾的類型進行評估。例如，如果您已知曉肇事者的身分，或者他們有跟蹤您的跡象，或揭發那些您並沒有公開發布於網路上的個資（如住家地址、車牌號碼、私人聚會的照片等），這個威脅就很有可能具殺傷力，建議您可以舉報。如果您認為這類威脅僅限於網路，您可以向您使用的平台檢舉該用戶，或使用封鎖功能。
- 如果您反覆遭受網路霸凌，建議您撰寫日誌紀錄過程，可以協助您識別霸凌的模式，也可作為舉報的證據。
- 在社群媒體上使用封鎖、黑名單和舉報等方式防止網路霸凌。

- 評估您個人的安全狀況。威脅是否具針對性、是否具體？威脅內容是否包含您的姓名、時間、地點或攻擊方法？霸凌者是否看起來不理智，例如，用他們的真名、電子郵件或電話號碼威脅您？霸凌者是否跨平台或將威脅移轉至線下（如語音郵件、或將威脅訊息放置在您家門口或工作地點）？如果您覺得安全受到威脅，請立刻向主管通報。

4. 知道在什麼情況下回應霸凌行為（Know when to engage）

- 人們通常都會建議「不要回應那些在網路上挑釁你的人」，這是有道理的。當您正面回應這些網路上的霸凌者，他們可能會升級他的攻擊行為，或試圖進一步挑釁攻擊目標，使受攻擊者自己先失控而陷入困境。然而，適時地抵抗霸凌行為，是可以自我賦權、反制這些攻擊。
- 因此，關鍵在於審視用什麼方式回應是有效和合適的。一種方法是，在不直接與霸凌者正面衝突的情況下，提出反駁言論。反駁言論可以是強烈譴責騷擾行為和仇恨言論、捍衛個人的聲譽，以及查核假訊息。
- 理解霸凌的情境脈絡也相當重要，如果您發現網路霸凌來自機器人而非真人，您還會費心回應嗎？

5. 建立一個創傷知情的支持社群（Build a trauma-informed community of support）

- 在這個社群中討論 TFGBV 可能引發的恐懼和羞恥情感。因為霸凌的目的是要讓您感到孤單。要記得：**您並不孤單**。
- 尋求朋友、家人、同事與專業人士的支持，並利用您廣泛的網路社群作為您的支持網絡。
- 支持您的同事。和同事對話、分享 TFGBV 的親身經歷時，讓同事知道尋求幫助是必須的、不丟臉的，破除尋求幫助的污名。除此之外，和同事討論自己的經歷，也可以從同事那裡獲得不同的觀點。
- 招募盟友協助。邀請信賴的朋友或同事協助，可以在您被霸凌者帳號封鎖時，協助監控霸凌者的動向。

保护自己免于遭受“科技促成的性别暴力”（Technology-Facilitated Gender-Based Violence，简称 TFGBV）的五个建议

近年来，女性记者和少数族裔记者在工作上遭受攻击的情况呈现指数成长，包含骚扰和数位暴力的攻击，迫使记者噤声。每当一名记者被迫沉默，我们就失去一个宝贵的声音，新闻观点的多样性也因此降低。2020 年，1210 名接受调查的女性记者中，有将近四分之三人表示，她们经历过网络霸凌、骚扰、威吓和攻击，其中有 20%的受访者表示曾遭受现实生活中的霸凌与攻击，他们相信这些线下的霸凌与攻击是由“科技促成的性别暴力”（Technology-Facilitated Gender-Based Violence，简称 TFGBV）所引发[1]。

以下五个防范 TFGBV 的建议是立基于证据，有 Dart Centre Asia Pacific（DCAP）的专家意见，以及完成由 DCAP 提供、Google 新闻倡议（Google News Initiative, GNI）资助 TFGBV 奖学金计划的记者们所提供的亲身经历。

完成 TFGBV 奖学金计划的记者们，将这五个建议翻译成多国语言，包括印度文、菲律宾文、斐济文和中文。更多的翻译版本可以到 Dart Centre Asia Pacific 的网站下载，链接如下：https://dartcenter.org/asia-pacific

1. 精熟社群媒体（Be social-media savvy）

- 了解自己所使用的数字平台，包含在这些平台上常见的威胁手段。
- 参加如何在社交媒体自我防卫的相关课程，以学会辨识网络霸凌以及对女性的影响。澳洲电子安全委员会提供一系列免费的网络课程，可以帮助记者们如何安全地设置社交媒体账号和个人档案。这系列的网络课程还涵盖了如何透过静音（例如：关闭提醒）、封锁（例如:列入黑名单）和举报来处理网络霸凌（https://www.esafety.gov.au/）。
- 了解您的国家针对 TFGBV 以及记者安全的相关法律，并理解这些法律是如何被执行的。
- 了解哪些平台最容易让您受到攻击与伤害（如:脸书、推特、Linkedln，Instagram 等）。

[1] Posetti, J., & Shabbir, N. (2022). The chilling: A global study of online violence against women journalists.

2. 强化您的网络使用安全机制（Bolster your cybersecurity）

- 使用长密码（最好是一串单字和符号的混合）、永远不要重复使用相同的密码、除了密码，最好额外设立安全问题，并且在您的重要个人帐号和工作使用帐号（如电子邮件、社群媒体、银行帐户）上设置双重身份验证。
- 尽量将个人资料和工作档案分开。
- 限制公开分享的个人资料（如避免展示孩子的照片、可识别的地标、宠物等）。
- 不要使用工作用的电子邮件处理私人档案，也不要在私人帐号放自己的工作用电子邮件。
- 工作帐号和私人帐号不要放上相同的个人照片（例如：头像）。
- 不要使用相同的用户名称与昵称，尤其在您希望保持社交距离的平台上。
- 和朋友讨论标记问题（tagging）!（例如，您可能不希望他们在分享工作相关事务时，标记您的私人账号）
- 为保护隐私，建议使用 VPN。
- 为防止被人肉搜索（doxxing），请在 Google 上搜寻您自己的名字，查看有关您的哪些个人资料会显示出来（可能是您的地址、电话号码、可以联系到您的任何个人资料)。也可以单独搜索您的电话号码或其他个人资料，查看是否有相关结果。如果发现您的个人资料是公开的，可以使用以下表单，要求 Google 从搜寻结果中删除这些个人资料：
  https://reportcontent.google.com/forms/rtbf
- 清楚了解您网络档案上个人资料的公开程度（包含图片和影片）。

3. 记录并举报“科技促成的性别暴力”（Document and report TFGBV）

- 记录下任何 TFGBV 的实际案例。如果您举报了网络霸凌内容，并成功删除这些内容，您可能会失去宝贵的证据。因此，记得先保存证据，包括：电子邮件、语音邮件和任何文字信息。也可以直接屏幕截图社交媒体内容，并尽可能直接复制链接。
- 确保档案是用安全且多种方式留存。
- 评估和监测威胁的来源、特征和发生频率。仔细考虑威胁是否会由线上移转至线下。您可以根据骚扰的类型进行评估。例如，如果您已知晓肇事者的身分，或者他们有跟踪您的迹象，或揭发那些您并没有公开发布于网络上的个人资料（如住家地址、车牌号码、私人聚会的照片等），这个威胁就很有可能具杀伤力，建议您可以举报。如果您认为这类威胁仅限于网络，您可以向您使用的平台检举该用户，或使用封锁功能。
- 如果您反复遭受网络霸凌，建议您撰写日志记录过程，可以协助您识别霸凌的模式，也可作为举报的证据。
- 在社交媒体上使用封锁、黑名单和举报等方式防止网络霸凌。

- 评估您个人的安全状况。威胁是否具针对性、是否具体？威胁内容是否包含您的姓名、时间、地点或攻击方法？霸凌者是否看起来不理智，例如，用他们的真名、电子邮件或电话号码威胁您？霸凌者是否跨平台或将威胁移转至线下（如语音邮件、或将威胁信息放置在您家门口或工作地点）？如果您觉得安全受到威胁，请立刻向主管通报。

4. 知道在什么情况下回应霸凌行为（Know when to engage）

- 人们通常都会建议"不要回应那些在网络上挑衅你的人"，这是有道理的。当您正面回应这些网络上的霸凌者，他们可能会升级他的攻击行为，或试图进一步挑衅攻击目标，使受攻击者自己先失控而陷入困境。然而，适时地抵抗霸凌行为，是可以自我赋权、反制这些攻击的。
- 因此，关键在于审视用什么方式回应是有效和合适的。一种方法是，在不直接与霸凌者正面冲突的情况下，提出反驳言论。反驳言论可以是强烈谴责骚扰行为和仇恨言论、捍卫个人的声誉，以及查核假资讯。
- 理解霸凌的情境脉络也相当重要，如果您发现网络霸凌来自机器人而非真人，您还会费心回应吗？

5. 建立一个创伤知情的支持社群(Build a trauma-informed community of support)

- 在这个社群中讨论 TFGBV 可能引发的恐惧和羞耻情感。因为霸凌的目的是要让您感到孤单。要记得：您并不孤单。
- 寻求朋友、家人、同事与专业人士的支持，并利用您广泛的网络社群作为您的支持网络。
- 支持您的同事。和同事对话、分享 TFGBV 的亲身经历时，让同事知道寻求帮助是必须的、不丢脸的，破除寻求帮助的污名。除此之外，和同事讨论自己的经历，也可以从同事那里获得不同的观点。
- 招募盟友协助。邀请信赖的朋友或同事协助，可以在您被霸凌者帐号封锁时，协助监控霸凌者的动向。