DIGITAL SECURITY POLICY AND GUIDELINES FOR FILIPINO JOURNALISTS

Digital Security Policy and Guidelines for Filipino Journalists

Writers: Rein Tarinay, Janess Ann J. Ellao and Ronalyn V. Olea

Editor: Ronalyn V. Olea

Layout: Anne Marxze D. Umil

Cover: Aaron Macaraeg

Published by ALIPATO MEDIA CENTER with the support of Internews.

October 2020

Address: 60 Kamuning, Quezon City
Email: pr2@bulatlat.com
Website: bulatlat.com

Digital Security Policy and Guidelines for Filipino Journalists

Table of contents

Preface

Digital security as safety training and media literacy

By Danilo A. Arao
Associate Editor, Bulatlat

The ubiquity of technology demands heightened security.

In the same way that journalists and media workers take necessary steps to ensure truth-telling in their reportage, there is a need to take the necessary precautions to ensure safety amid these trying times. They have to survive today to continue reporting the next day.

To say that protecting devices is a life-and-death situation is hardly an exaggeration. Heightened state surveillance and cyber-attacks against the media are as real as red-baiting and extra-judicial killings.

While journalists and media workers have their own ways of protecting themselves and securing their tools of the trade, there is a need for more information on how they can improve their digital security. On the other hand, they should also be open to the possibility that old habits could be wrong, hence the need to rectify.

This handbook provides vital information on digital security and recommends a standard policy not just for individual journalists and media workers but also for various media organizations. That this is being produced amid a repressive regime makes it even more relevant as the media continue to be under attack from those who should protect and uphold press freedom and other basic freedoms.

Digital security is as technical as it is political. It is part of safety training, in the same way that it is part of media literacy. May we all continue to learn the intricacies of emerging technologies while pursuing the best practices of shaping public opinion.

Protecting digital rights, defending press freedom

One fateful day in December 2018, Bulatlat's website – all of its in-depth reports, breaking news, features, and commentaries – became inaccessible to its readers. This was where the journey began.

For the past 19 years, Bulatlat has been fearlessly publishing online the stories of the marginalized and issues that are widely underreported in line with the media's role in informing the public of crucial information they need and in serving as a watchdog against the excesses and abuses of the powers-that-be. It is not surprising indeed that it would one day find itself as subject of one of the biggest Distributed Denial of Service (DDoS) attacks ever recorded in the Philippines.

This experience paved the way for Bulatlat's advocacy of defending our digital rights as part of the overall struggle for freedom of expression and of the press. After all, digital rights are but an extension of our inalienable rights that are recognized by both local and international instruments and of which the state is bound to guarantee.

In a resolution, the United Nations Human Rights Council in June 2016 affirmed that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice" in accordance to other UN mechanisms and instruments.

With the increasing reliance of Filipinos to the Internet amid the pandemic, access to fast, reliable, and affordable Internet as well as private and secure online communications are no longer considered a luxury but a fulfillment of our rights.

It has, too, altered how we do journalism – from news gathering to how our intended audiences consume them, to name a few. Media institutions have scrambled to set up home-working systems and embraced multiple online communication platforms in an effort to "create a parallel and secure virtual office world."

This spelled out the need to revisit our digital rights as journalists and ensure that our role as truth-tellers are not muffled, if not completely silenced, with threats on free press arising in this digital age. Hacking, online threats, and mobile surveillance are among the frequently-recorded attacks online. Attacks on digital rights often stem from the various governments' efforts to clamp down on people's access to information and to spy on individuals and organizations deemed as enemies of the state.

As such, Bulatlat has partnered with Internews to produce this publication titled *Digital Security Policy and Guidelines for Filipino Journalists* as part of an effort to promote safe digital space for journalists, advocates of free expression, and human rights defenders. The talking points and discussions here were part of a series of digital security capacity-building training, and consultations with community journalists. Accompanying this book is a series of podcasts on digital security and a mechanism for threat sharing among journalists.

Pandemic, terror law, and new threats against truth tellers

In March 2020, the Philippine government began what would turn out to be one of the world's longest and strictest lockdown as it dealt with the dreaded COVID-19.

The Philippine media, both those belonging to the dominant and alternative media tradition, has since made its COVID-19 coverage a priority. The uncertainties and deluge of unverified information has posed challenges for journalists both here and abroad on the truthfulness of their reports. Still, journalists have continued to provide the public with information they need to make sense of what is happening, and in striking down the widespread disinformation later referred to as "massive infodemic."

This has changed many aspects of a Filipino journalist's work, from the protective gear to wear and minimum health standards to observe, and even the process of news gathering. Conducting interviews and covering of press briefings have primarily moved to the digital space, with Zoom, Jitsi, and Google Meet as among the commonly used teleconferencing applications. Social media platforms have become even more a tool for news gathering.

But in the middle of a pandemic, the Philippine government had other priorities in mind. President Rodrigo Duterte, four months into the lockdown, signed into law the controversial Anti Terrorism Act of 2020, which is currently one of the most challenged laws before the Supreme Court.

The law and its many contentious provisions have been widely criticized for curtailing press freedom and the freedom of expression. It granted authorities to detain activists and journalists, and to allege them at the very least of committing terrorism as the law so vaguely defined.

On top of the threats posed by the pandemic and the terror law, the state of the Philippine media is currently at its worst since the Marcos dictatorship. Journalists have found themselves at the receiving end of hate speech, particularly on various social media platforms, as they are tagged as paid, "presstitutes", and worse, vilified as terrorists.

Women journalists are subjected to worse attacks, as they endure misogynist statements, including rape threats online.

The shutdown of ABS-CBN, the cyber-libel charges against Rappler's Maria Ressa and Rey Santos Jr. and the tax evasion cases, and the verbal attacks against the Philippine Daily Inquirer, among others, have virtually sent chilling effect to journalists whose role as truth tellers has never been more important than it is now.

The alternative media experience

While the Duterte administration has been infamously known for his attacks against the press, it is the community journalists, particularly those covering the human rights situation on the ground, who are at the receiving end of more vicious forms of intimidation and harassment.

Vilification and red-tagging campaigns usually precede graver forms of abuses against journalists, advocates, and human rights defenders. Such tactic attempts to discredit the work of the media, with the end goal of controlling public opinion.

Much like the shutdown of the television giant of ABSCBN, websites of alternative news outfits have been made inaccessible to its readers and stakeholders as they were subjected to Distributed Denial of Service Attacks (DDoS).

DDoS refers to the use of infected computers to overwhelm a website, causing its shutdown. Among those who were subjected to this attack from 2018 to 2019 are news websites such as Bulatlat, Kodao Productions, Pinoy Weekly, and AlterMidya – People's Media Network.

Of late, the Baguio-based Northern Dispatch was also subjected to DDoS attacks, amid its reporting on the government response on the pandemic, while at the same time showcasing the relief operations and other services of people's organizations for the poor and vulnerable sectors.

Prior to the DDoS, Northern Dispatch and its writers and editors have long been subjected to red-tagging.

Online red-tagging, harassment

Much of the red-tagging these days happens in the virtual world, including known government-backed Facebook Pages that spread Internet memes on the supposed link of alternative news websites to revolutionary organizations.

Internet trolls are also known to swamp the comments' sections of stories on human rights violations, press freedom, and the controversial terror law, to name a few. News outfits usually ban, hide, or delete these comments to keep their respective social media accounts from being used by paid trolls to peddle disinformation and false narratives.

But in 2018, trolls took their attack to a completely new level when they mass reported the Panay Today Facebook Page, over a video coverage of a protest action against President Duterte. This resulted in the many incidents of temporary shutdown of their Facebook Page.

Journalists have also received death threats through internet-based messaging applications, coupled with a photo of them during a coverage and a message that read: "Keep safe."

The suspicion that these types of online harassment are coming from state security forces has been bolstered when Facebook took down more than a hundred pages of police and military-backed Pages for supposed inauthentic behavior. Philippine government officials were quick to retort that this is a form of censorship -- which isn't. President Duterte himself issued public tirades against Facebook for taking down government's "advocacy" posts.

How online attacks translate to physical harm

Online vilification against journalists and alternative news outfits sends a chilling effect. It also hampers their duty of searching for truth as they have been turned down by interviewees, afraid of reprisals from state forces, or kept from official government briefings.

At times, such as in the case of a Panay-based journalist, he was confronted by a suspected intelligence agent and was asked if they can "talk for a second."

Copies of alternative newspaper Pinoy Weekly have also been repeatedly tagged as "subversive" in at least two separate incidents in Bulacan during the pandemic. During a police raid in an urban poor relocation site in Bulacan, authorities burned thousands of copies of the news magazine.

Still, alternative media journalists have been forcibly pulled out from the communities and issues they cover as red-tagging and threats to physical safety intensifies. Journalists have also been subjected to trumped-up cases, including charges of rebellion, illegal possession of firearms and explosives, and cyber libel.

Journalists who were arrested in Cebu while covering a protest against the Anti-Terror Law found out that there are fake Facebook accounts using their names.

Safety measures

In the course of such threats, safety mechanisms have been put in place for alternative media practitioners. Most of these were lessons drawn from a series of training on

journalist safety that media advocacy groups such as the National Union of Journalists of the Philippines and the International Association of Women in Radio and Television-Philippines have provided.

A welcome addition to these training is the digital safety training conducted by Bulatlat, in partnership with Internews. Here, journalists saw the need to properly document attacks online and realized that the assertion of digital rights is no way any different from their struggle for a free press.

The consultations gave birth to the need for a digital security policy that they can adopt in their respective news agencies.

In the near future, a dedicated office that will look into digital attacks against journalists to protect the people's hard-fought right to information would be very welcome.

Digital Security Policy

Introduction

This document provides a set of procedures that journalists are encouraged to observe and implement in order to enhance their personal digital security as well as that of the organization.

All staff are encouraged to follow this policy and take every measure to implement its procedures to help protect it, its staff and constituents.

This document should be reviewed and updated at least once a year.

I. SOP before, during & after coverage

Planning before every coverage is the first step to safety. Your preparation will depend on the nature of coverage you have.

Put utmost importance to your own safety, the safety of your team and the safety of your data.

Before coverage:
Make a checklist of all the things you need to bring and put them inside your bag/s at least a day before your coverage.

Have a large ziplock or wet bag, in case it rains, for camera, SD cards, cellphones and other equipment. Store your SD cards in hard cases.

Be sure to have fully charged power banks or plan ahead where to recharge your electronic gadgets.

For sensitive assignments, coordinate with the media liaison regarding their protocols. In armed conflict areas, cellphones and cameras might not be allowed.

Inform your desk/family members when you will be accessible.

Be sure to bring protective gear such as face mask and shield, alcohol, soap and tissue.

During coverage:
If going live, ask permission from the organizer/s first. The same goes for live interviews. Do not randomly pick out anyone from the crowd.

Do not connect to free WIFI. Always use your own mobile internet.

Never post anything sensitive on Instagram and/or Twitter. Location settings may be turned on for FB Live or live tweets but be sure to turn these off after every event.

Be mindful of your safety and security while recording. Better to have a buddy in case you might need to leave early.

If tension builds up, find a safe spot where you can still observe what is going on.

In case of arrest, assert your rights as a journalist. Be quick to hide your SD cards and other storage devices, or find a way to pass these on to your colleagues.

For sensitive coverage, always follow the protocols set by the media team. Never reveal your exact location via SMS, email or social media apps to anyone while you are still in the area. Doing so might jeopardize your safety and that of others.

Wear face mask and observe physical distancing. Wash your hands frequently, or if water is not accessible, use alcohol or sanitizer.

After coverage:
Store your data and have a backup which can be accessed by other team members. (See Data and Information Management)

If you need to share content with your colleagues, use secure email such as Protonmail or Tutranota.

For large files, use MegaNZ or other encrypted cloud storage. If you must use Google Drive (only for non-sensitive materials), use two-factor authentication for your account and ask the recipient/s to do the same.

Take a bath immediately after coverage, whether you go straight to your office or your home. Wash your clothes immediately or put in a bin with cover/plastic (when not at home).

Sanitize your cellphones and other equipment.

II. Data information & management

The information we produce and use every day is of great value to the continuity and security of our work. The data and information we gather as journalists are our biggest asset and so we need to protect these.

As media outfits and individuals we need to ensure that:

1. Data (files, images, videos etc.) are stored in a secure place and that those who are not authorized to view, use or modify these data do not have access to it whatsoever.
2. Our data are available and accessible to us or other authorized users whenever and wherever these are needed.
3. Data that we no longer need are destroyed and no longer retrievable by others.

4. We know the information and data that sit on our devices and are able to remove it when needed. It is therefore highly important that we have both the knowledge and tools that allow us to manage our data securely.

Since most alternative media outfits do not have the resources to devise solutions that are normally costly, we make recommendations for free and open source tools that can be utilized to achieve these goals.

Storing data

Encrypting important data locally

For sensitive files that need to be stored locally:

- Sensitive and important files must be stored in encrypted folders or on encrypted storage units.
- All staff are required to create an encrypted file container(s) on their computers to store sensitive and important files.
- All encryption keys must be shared with the Management (2 people) and stored securely to ensure continuity in the case of emergency or staff departure.
- Staff are required to install and use Veracrypt to encrypt important files.
- Have at least two physical backup for your files, stored in separate places. Make sure to encrypt the hard drives. Storing data in encrypted cloud storage should be your third backup.

For your guide on how to encrypt your data, see "How to Secure Sensitive Files on Your PC with VeraCrypt" (https://www.howtogeek.com/108501/the-how-to-geek-guide-to-getting-started-with-truecrypt/).

Storing data in encrypted cloud storage

For staff who work collaboratively on files and documents, MEGA cloud storage must be used to both store and backup data.

It is recommended that this is centralized by the management.

How to use MEGA Cloud storage

1. Go to www.mega.nz.
2. Create a Mega account (remember to use a strong password).
3. Once you have your MEGA account set up, enable two factor authentication and back up your recovery key (you need this for password recovery and account recovery).
4. Install the MEGA Sync Desktop App.

Backing up data

For the purpose of simplifying data backup, all staff are encouraged to use MEGA SYNC to back up important files.

To this, staff are encouraged to:

1. Install MEGA Sync on their laptops and mobile phones.
2. Create Mega accounts.
3. Set up synchronization folders.
4. Ensure that Sync is on.

Destroying data

To ensure that staff and their information are secure and cannot be accessed by unwanted parties, it is important that staff use appropriate data destruction software to securely delete sensitive files when needed and clean up their devices in a secure manner.

Staff are required to install and use:

1. File Shredder to securely delete files that are no longer needed and contain sensitive information.
2. CCleaner to wipe drives or drive partitions when needed and to delete and securely clean your system of traces left when browsing the internet or using certain programs.

Retrieving data deleted in error

Staff are encouraged to take measures to safeguard data. In the event files are deleted in error, staff members may use Recurve to retrieve lost files.

Recurve is a free software that scans hard drives to receive deleted files with a reasonable rate of success.

III. Online accounts & password management

Hackers manage to steal/take over online accounts which have weak passwords. The possibilities are endless -- they can spy on you, steal your personal information/identity for devious purposes, blackmail you, or harass you.

Strong passwords provide the first layer of protection. A two-factor authentication is an additional layer of security, preventing others to access your online accounts.

1. All staff are encouraged to separate their personal and professional online accounts. These include email, social media or any other online services.
2. All online accounts must use secure passwords (12+ digits, upper and lower case letters and characters)
3. Passwords must be changed every six months.
4. All staff are required to use a password manager such as

Bitwarden or KeePassXc to securely keep passwords.

5. All staff should enable two factor authentication on Bitwarden and back up their archives.
6. Passwords are not to be written or saved anywhere no matter what.
7. All staff are required to download their password archives and keep a copy in a secure, encrypted folder.
8. All online accounts must have two factor authentication enabled to provide an additional layer of security.
9. All staff are required to use an authentication app for two factor authentication and refrain from using SMS for that purpose.
10. Accounts that are co-managed by different staff members:

    a. Staff should agree on a master admin of the account.
    b. When passwords are changed, the new password should be communicated using encrypted channels such as Signal or Protonmail. Once the password is sent, both parties must delete the message.
    c. No reference should be made to which account the password is associated with in the same message where the password is communicated. This information should be communicated via another channel (if you use email to communicate password, then use Signal to communicate the information).

What is malware?

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware.

Downloading applications from unreliable sources and opening email from unknown sources are some of the ways one can get malware.

Malware protection

Malware remains one of the most persisting threats that ICT users face in this day and age.

Malware is used by state and non-state actors to compromise the devices and online accounts of activists, human rights defenders, journalists and civil society actors. It is therefore of paramount importance that organizations and individuals take all the possible measures to protect against these attacks. The following measures are recommended:

1. Antivirus malware: All staff are required to install and keep up to date a functional antivirus software on all their devices. For that purpose, we recommend Malwarebytes. It is free and open source. To learn more about the software, please visit its support page . Malwarebytes is available for Windows, Mac OS and Android.
2. All staff are required to keep their operating systems and software up to date. Up to date software prevents hackers and hostile actors from exploiting exposed security vulnerabilities and provides improved security protections. Most operating systems and software automatically update. Staff can use this application to scan their devices for required updates and do the necessary.

Communication

Communication security and privacy are essential to the media outfit's work, continuity and the safety of staff. At a time when digital surveillance is legalized, securing our communication has become more urgent.

General principles

- All staff are required to use secure and encrypted communication platforms.
- All staff are required to use Signal for texting, audio and video calls.

- All staff are required to use Protonmail or Tutanota for email communication.
- Gmail can be used only for non-sensitive communication
- All staff are required to use secure passwords on all accounts.
- All staff are required to enable two factor authentication on all their communication accounts/apps.
- All staff are required to delete sensitive conversations once completed and ask the other party(ies) to do the same.
- All staff are required to regularly clean up files and images sent and received via communication apps from their devices using Shred It on Android and File Shredder on Windows.

Email

Every media outfit places great importance on security. All staff are encouraged to use Protonmail or Tutanota for professional communication among staff. Staff are also encouraged to ask their contacts to use Protonmai or Tutanota for sensitive email communication.

Beware of phishing email. Do not open emails from sources unknown to you. Double check the email address before opening any file. Look closely at the URL and look it up at who it is.

What is phishing?

Phishing is a type of online attack often used to steal user data, including login credentials and credit card numbers. An attacker, masquerading as a trusted entity, lures a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, or the revealing of sensitive information, among others.

Text, audio and video

Communication via text, audio call or video call should be encrypted so as to prevent other parties from eavesdropping to our conversations.

- While WhatsApp is considered secure enough as it uses end to end encryption, the fact that it is not open source, makes it vulnerable.
- All staff are required to use Signal for their professional communication.
- All staff are required to enable screen lock or fingerprint lock for Signal to add an additional layer of security
- For more sensitive communication including group calls, staff are encouraged to use Jitsi Meet. If using Zoom, be sure to adjust the security settings. (See sidebar: How to Prevent Zoombing).
- Google Hangouts are not fully encrypted (the company can read, listen and watch and may keep records). They are not to be used for sensitive communication at all.

IV. Security

Mobile security

Mobile phones are not designed to honor user's privacy and they continue to pose various security threats to people working in sensitive fields such as journalism, human rights and social movements.

All staff are required to take every measure possible to protect their mobile devices and their content to minimize security threats. Consider having separate phones for office use and for personal use.

How to prevent 'zoombombing'

As working in a remote environment or from one's home becomes the "new normal," cyber-security experts have advised on the use of secured means of communication platform for online classes, public fora, office meetings, and information dissemination.

These past weeks, teleconferencing app such as Zoom has been under fire over security and privacy breaches, and vulnerabilities to hijacking of uninvited participants in a forum, also known as "zoombombing."

Here in the Philippines, uninvited participants believed to be trolls zoombombed a webinar held by a group of women advocates on April 17. Trolls who hijacked the webinar showed doodles of penis and played an audio recording of what appeared to be from a pornographic video.

How do we prevent 'zoombombing?

Do not share your meeting ID on public – One way to prevent zoombombing is to keep your Meeting ID private. When holding a public discussion, it is helpful to filter participants by creating an RSVP. Meeting ID may be shared through secured e-mail, such as Protonmail.

Customize Meeting Password – Zoom can automatically generate a password for meeting rooms. However, auto-generated passwords are vulnerable to attacks. One option is to customize it.

Limit screen sharing – When screen sharing is provided to "all," any participant who enters the virtual meeting room can play images or videos to the rest of the participants. This can be used to project any harmful and violent content.

In the advance setting, check the option that only the meeting host can share the screen.

Turn off annotation – Host and participants have the privilege to doodle and mark up content together using annotations. To prevent trolls from writing all over the screen, disable the annotation feature in your Zoom app.

Kick them out – When participants are still not following the community guidelines set, they may be kicked out. Go to the Participants pane, hover on her or his name, and choose Remove. Those kicked out from the Meeting Room cannot rejoin.

If all else fails, Jitsi, a more secured teleconferencing app, may also be used.

Device security

Computers, laptops and cellular phones must be secure and should only be accessed by authorized individuals. In cases of loss or theft, data stored in our devices should not be easily stolen.

1. All staff are required to enable screen lock on their phones using the password or figure print features. Do not use the pattern or the simple PIN as they are nor secure enough.
2. All staff are encouraged to back up the content of their phones regularly.
3. Mobile phones are not to be used to receive or store sensitive files. If sensitive files are to be received on mobile phones, they must sent through a secure channel such as Signal or Protonmail be deleted once the files are no longer needed, using a secure file deletion app such as Shred it.
4. All staff are encouraged to download CCleaner for Android on their phones and run the app regularly to clean up their devices (delete downloaded files and clean digital footprints).
    1. All staff are encouraged to encrypt all their devices.

Apps and permissions

Mobile apps can pose serious threats. App stores are full of apps that carry out malicious activities. The way mobile apps work requires them to access information on your devices such as your location, your contacts, your messages, your storage or access features such as your device mic or camera. Malicious apps take advantage of this to spy on your device, collect information about your activities (such as who you communicate with or what websites you visit), read your messages or even copy and send content from your phone to a remote server. Apps installed from other sources outside the official app stores are particularly dangerous.

All staff are required to observe the following:

1. Download apps only from official app stores only (Google Play and App Store).
2. Limit the number of apps you install to the bare minimum and install apps you need only.
3. When installing a new app, do the following:
    a. Make sure it is a legitimate app from a legitimate developer. Google the app and the developer and read some reviews. If you are not happy, look for an alternative.
    b. Examine the app permissions. If the app asks to access information on your device that you believe is not needed for the app to run, move on and find another app.
    c. Check the app history and when it was last updated. Apps get regular updates and if the app has not been updated for several months then it is most probably not a good one as it does not take security seriously.
    d. Read the users' reviews. They help form an opinion about how good the apps is.
4. Review your existing apps permissions and disable all permissions to your location, camera, contacts, messages and mic unless it is needed for the app to work. You may also choose to disable these permissions and only enable them when you use the app then disable them again.
5. Disable location services on your device.
6. Ensure that your OS and apps are all up to date to patch and possible security flaws that can be exploited by hackers to access your device.
7. If you use an Android prior to Android 6, make sure you encrypt your phone. All phones that use Android 6 or later are encrypted by default. (Settings -> Personal -> Security -> Encryption).

8. If you use android and your device is linked to your Google account. You should always disable your Google services tracking of your activities by reviewing your Google Dashboard.

To check app permissions on android, go to settings, apps then permissions. You can also use a third-party app such as App Permission Watcher to scan apps on your device and find out what app accesses what information.

Social media

Social media has become essential to the work of most if not all media organizations these days. Social media accounts can be a source of vulnerability as they are easily identified and can be easily targeted. Media outfits and journalists must follow the following guidelines when setting up and using social media accounts.

1. All staff are encouraged to have separate social media accounts for work. Personal social media accounts are not to be used for work at all.
2. All work-related social media accounts must be associated with secure emails. This means that these emails have strong passwords, two factor authentication and are not publicly available to others.
3. All social media accounts must have strong passwords and two factor authentications enabled.
4. All social media accounts are to be managed by two people to ensure accessibility in case of emergency.
5. Facebook pages must have two admins with full admin privileges only. All the other team members must have the status of editor, analyst or advertiser based on their role.

6. Facebook pages must be managed via a business account owned by your media outfit to protect its security.

Friendly tips for personal accounts

1. Always check the audience settings of each post.
2. Do not post your exact location at any given time.
3. Refrain from posting photos of your children, which school they go to, and other details.
4. Clean your friends' list. Delete those you never really know.
5. Never approve requests from strangers. Verify first with your friends if such accounts belong to them.
6. Never join the bandwagon. Facebook apps might seem cool but these might undermine your security. Unwittingly, you are giving permissions for these apps to use your data in any way they want. FaceApp, for example, will have access to your photos forever.

How to deal with trolls

1. Don't feed the troll. Stick to the issue at hand. Do not respond with hate or insult.
2. Respond with facts. Engage with trolls so that they can just voice their opinion, and so you get to show the facts. This is also one way to expose them.
3. Diffuse the situation with humor.
4. Block if they are obviously just bots.
5. Enable filter tools in your social media accounts.
6. Report. In case of threats and harmful posts report the user.

V. Using the internet safely

General behaviorial requirements

When browsing the internet, staff members must follow the following guidelines:

1. Use a VPN when browsing sensitive websites or there is fear of surveillance
2. Do not use public Wi-Fi to connect to the internet. If you must
   - Use a VPN.
   - If you use a public computer, browse the internet in private mode and make sure you sign out of any online accounts you signed into.
   - Clear browsing history and make sure the browser does not save your log on credentials.
3. Use search engines that do not collect user data such as https://duckduckgo.com to protect their privacy and security.
4. Use privacy oriented internet browsers such as Firefox and Brave for Windows and Firefox Focus for:
   - When using Firefox, staff are required to configure their browser privacy and security to maximum.
5. Brose the internet in private/incognito mode as much as possible.
6. Add browser extensions that help maximize the privacy settings of your internet browser (see how to section).
7. Use CC Cleaner regularly to clean up traces left by their internet activities on their devices (see how to section).
8. Learn about and use privacy enhancing tools such as:
   - Privacy Badger
   - Cookie Auto delete
   - Facebook Container
   - Firefox Multi-Account Containers
   - uBlock Origin

General device security protocols

1. All staff are required to keep their operating systems and their software up to date.
2. All staff are required to create a non-admin account on their devices and use it for day to day use. Accounts with admin privileges are only to be used for maintaining and installing new software. This helps defend the device against unwanted programmes such as malware.
3. All staff are required to lock their devices using a strong password and change it every three months.
4. All staff are required to encrypt their hard-disks if their operating systems allow for whole device encryption (Windows 10pro and up).
5. All devices must have an up to date anti-virus software.
6. All staff are required to take care of the health of their device by cleaning it using CC Cleaner regularly.

How to deal with red-tagging/fake memes aiming to discredit your media outfit or you as a journalist

1. If from government offices, document the incident. Screenshot the post and save the URL.
2. Report the violation to Facebook. Ask friends/colleagues to do the same.
3. Consider filing legal cases if the perpetrators are identified.
4. Block the perennial red-tagger from posting on your social media accounts.
5. For fake memes, screenshot the post and label it with "FAKE." Explain why is it fake.
6. Report Facebook accounts that publish false information.

What is DDoS?

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. A heavy DDoS attack could render a website inaccessible.

Website security

For many alternative media outfits, the website is the main platform for content distribution. Maintaining our website is key in growing our audience so we should keep it secure. Outdated themes, plugins and tools are often exploited by hackers to attack websites. Here are some tips:

1. Continuously update your theme, WordPress, Joomla, Drupal or any CMS, plugins and tools in general.
2. Limit admin access to only two. Change passwords regularly.
3. Before installing plugins, check for security. Plugins in WordPress are the main cause of the majority of attacks or malware infections. Outdated plugins make it easier for hackers to access your site and infect it.
4. Avoid installing software from unsafe sites or sites that do not offer confidence.
5. Always use an antivirus.
6. If using Wordpress, consider using DDoS protection tools such as Deflect. Contact Internews community manager or Access Now for guidelines.
7. Consider hosting services from international NGOs promoting privacy and security rather than the commercial ones.
8. If you suspect that your site is being attacked, contact Internews community manager or Access Now.

Threat information sharing

Threat information sharing is important for any community. It is a mechanism for alerting your colleagues and getting assistance/ advice.

Alerts and suspected digital threats/ attacks should be sent via Signal cybersecurity group which has been created early this year. When receiving a suspected phishing email, review "Sent From." Server details from the ORIGINAL MESSAGE of the email, download the suspected phishing email first and send it as an ATTACHMENT to digital security experts.

If it's a DDoS or Web Hacking incident, document the TIME and DATE that you have detected it.

For a possible infected computer, document the last ACTIVITIES that you did (e.g. download a file etc.).

For possible PHYSICAL security incident, capture the TIME and DATE and if possible, take PHOTO.

In such cases, consider doing the following:
1. Change passwords.
2. Apply security updates.
3. Implement changes in security policies.
4. Use DDoS service as a protection.
5. Remove any sensitive information on metadata (See "Destroying data").

References

https://en.unesco.org/news/journalism-pandemic-reinstating-paramount-importance-facts

https://news.berkeley.edu/2020/05/06/covid-19-and-the-media-the-role-of-journalism-in-a-global-pandemic/

https://www.ifj.org/media-centre/news/detail/category/press-releases/article/philippines-media-workers-file-petitions-to-reject-anti-terror-law.html

https://www.bulatlat.com/2018/10/02/filipino-women-journalists-attacked-but-unbowed/

https://www.bulatlat.com/2020/06/09/fake-facebook-accounts-meant-to-silence-dissent/

Acknowledgment

The past few months have been very tough. Protecting ourselves against an unseen enemy while protecting our human rights, digital rights at the same time has been challenging.

This project would not be possible without the help of our colleagues from the alternative media--Paghimutad, Pokus Gitnang Luzon, Altermidya, Kodao Productions,Northern Dispatch, The Breakaway Media, Panay Today, CEGP - Cebu, Manila Today, Tudla Productions, Quezon Reels, Radyo Natin Guimba, Pinoy Weekly, Bicol Today, and Baretang Bikolnon. We have braved the slow internet connection and the restrictions on mobility! Thank you for all the Tuesdays we've shared figuring out how to make ourselves less vulnerable while we are trapped in the world wide web.

Internews
Local voices. Global change.

ALIPATO
MEDIA CENTER

BULATLAT