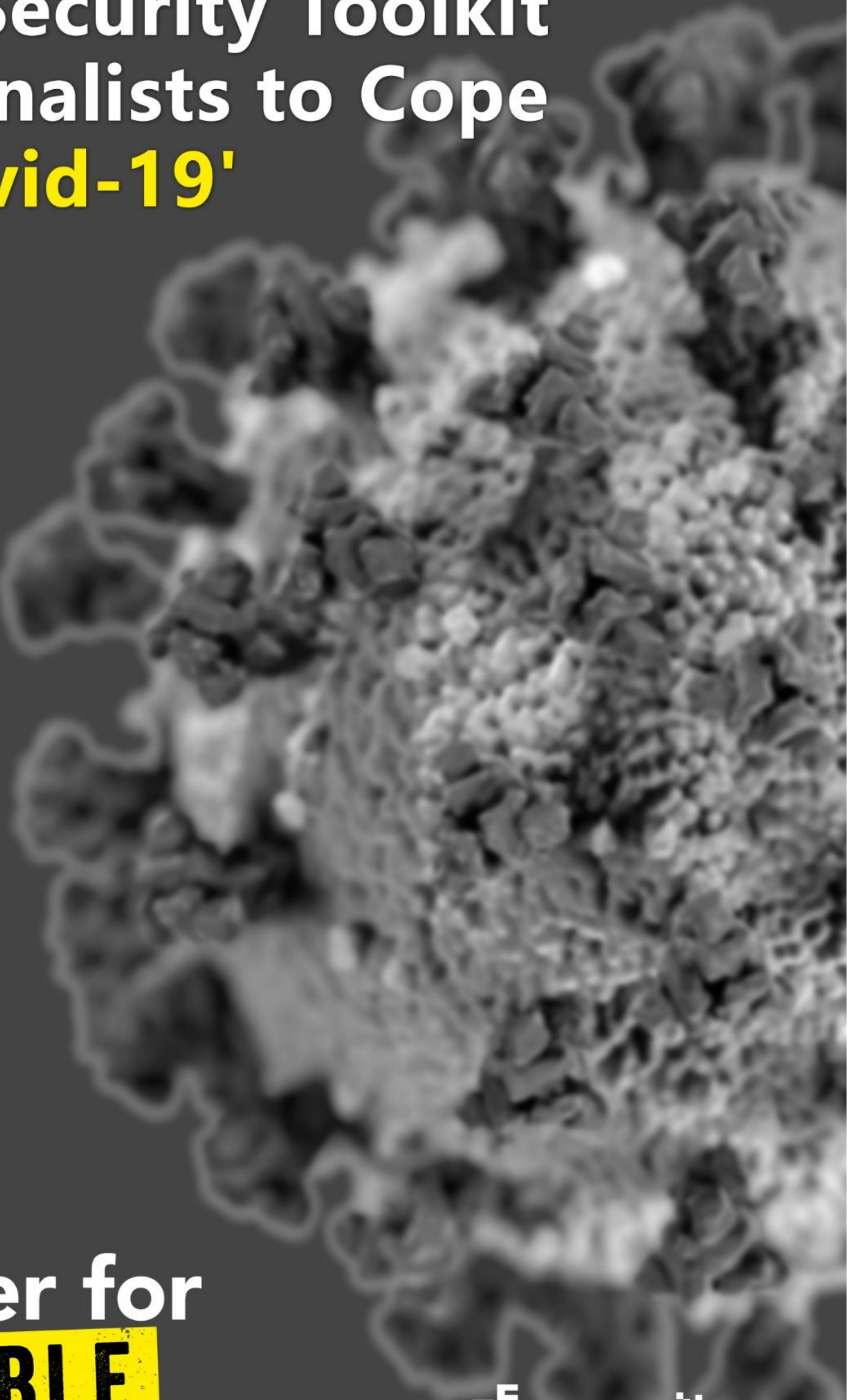
Digital Security Toolkit for Journalists to Cope with Covid-19'



Together for RELIABLE information

FREE PRESS UNLIMITED

DRF
DigitalRightsFoundation
"KNOW YOUR RIGHTS"

ABOUT

Founded in 2012, Digital Rights Foundation is a registered research-based advocacy NGO focusing on ICTs to support human rights, democratic process and digital governance.

DRF envisions a place where all people, and especially women, are able to exercise their right to expression without being threatened.

DRF

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

As **COVID-19** has ravaged the world and confined most of us to our homes, it has led to all of us depending on our digital devices for basic communication and daily tasks. This dramatic surge in online usage has attracted the attention of cybercriminals, thereby increasing the unseen digital threat we all.

Each profession is affected differently by cyber attacks, and each person has their own different level of threat. To make the best use of a digital security toolkit, such as this, you should go through these questions below and determine what your threat level is. The higher the level, the more precautions are necessary, the lower the level, the fewer the precautions.

THREAT ASSESSMENT:

01 Are you working from home during this pandemic? If not, are there social distancing practices that are in place at your work?

02 How many devices are you using for your job? (The higher the number, the more you need to be careful)

03 How many of your devices are provided by your employer? (If your employer gives you a device for work, you can ask them to help keep the device safe)

04 Do you have access to an IT department or person?

05 How much data do you store on a daily basis for your work, and how do you save it?

06 Have you, or any of your colleagues ever been the target of a cyber attack?

These questions are in no way the ultimate test of your digital security but will help you begin to understand your online behaviors as well as identify areas you might not have earlier thought about at all.

For example, if you're using a company device, ask your employer for security measures and tools that will help you keep the device secure. Additionally, this will help highlight to management that digital security plans and procedures are the need of the hour and this may be the necessary push needed towards that direction.

So generally, when thinking about your digital security, you need to think about these overarching areas:

- Privacy
- Device Security
- Data Protection and Backups

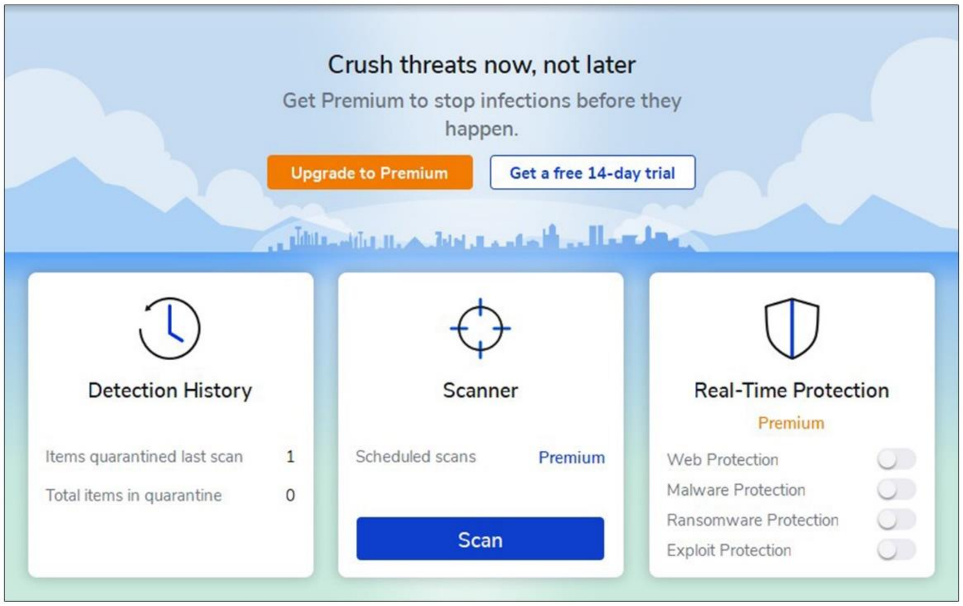
We'll go over these areas in this toolkit and also give you specific ways you can protect yourself during the COVID-10 Pandemic. These digital security concerns are always relevant, however, during a global pandemic, these issues are heightened given that everything is happening in the digital sphere.

Device Security:

Your device can either be a laptop, computer, or phone that you use on a daily basis for your work or for your personal use. Devices are integral, for their productivity but also as a store for information and data. During these times, they are our connection to the outside world and to those around us. They are also helping us to keep continuing doing our tasks.

This may seem basic, but it is a point that we must always reiterate. The simplest thing you can do to keep yourself is to install and use an 'Anti-Malware' software. As more and more people are using the internet, cybercriminals are thronging to the digital sphere in attempts to cheat people out of data or to leak their information. The first defense our devices must have is anti-malware software. It doesn't take too long to download and if you're concerned about which one to use, don't worry we have a suggestion.

During our training sessions, we recommend ‘Malware Bytes’ to our trainees. It is simple to use and has the ability to really scan through your device, giving you an extensive list of all the malicious files.



Crush threats now, not later

Get Premium to stop infections before they happen.

Items quarantined last scan 1

Total items in quarantine 0

Scheduled scans Premium

Web Protection

Malware Protection

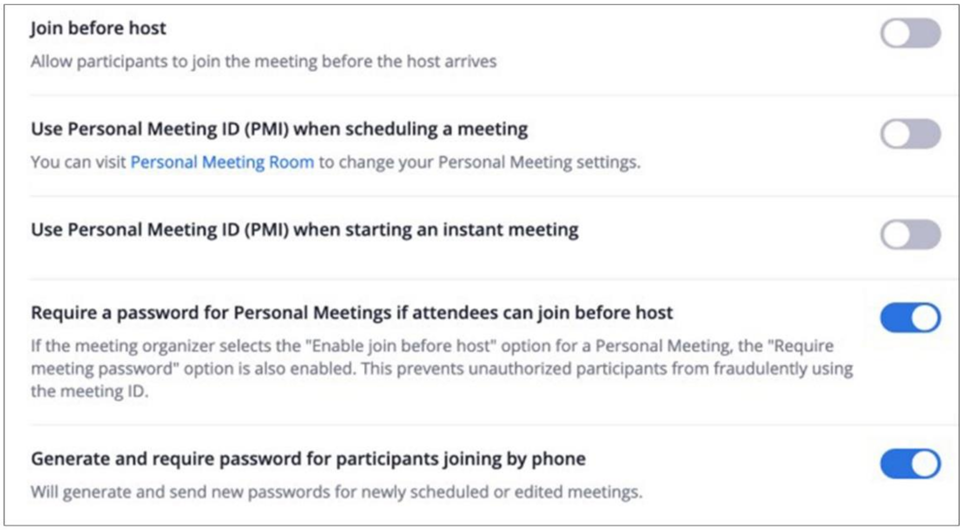
Ransomware Protection

Exploit Protection

COVID-19: Threats Working From Home

As the world entered a lockdown, one video conferencing application really took off. From online classrooms, board meetings to interviews, everything was being conducted over Zoom. This dramatic rise in traffic attracted a lot of attention from cybercriminals and people who wanted to create trouble. Initially, it seemed that all people needed to get into calls was a link, and this gave birth to a phenomenon where uninvited visitors would ‘troll’ calls and try to upset the ongoing conversation.

The lockdown really exposed major security concerns on Zoom and also began to highlight the need to reevaluate the security features on all the applications we use. Zoom responded with new security features and they are as follows:



Join before host ○

Allow participants to join the meeting before the host arrives

Use Personal Meeting ID (PMI) when scheduling a meeting ○

You can visit Personal Meeting Room to change your Personal Meeting settings.

Use Personal Meeting ID (PMI) when starting an instant meeting ○

Require a password for Personal Meetings if attendees can join before host ●

If the meeting organizer selects the "Enable join before host" option for a Personal Meeting, the "Require meeting password" option is also enabled. This prevents unauthorized participants from fraudulently using the meeting ID.

Generate and require password for participants joining by phone ●

Will generate and send new passwords for newly scheduled or edited meetings.

HOT TIP:

With the lockdown in place, a lot of new communication alternatives are coming out. Some of these become ‘hot’ new items with a lot of people using them. Before you fall into the bandwagon, do your research and find out what people are saying about the software and how to use it securely.

Another thing to look out for is ‘phishing attacks’ and ‘sextortion emails’. This has been an issue world over even before the lockdown began, however, with the lockdown in effect, these attacks have grown exponentially. Recent attacks have included emails where the cybercriminal has their victim’s passwords (often an old one), and tries to get a large payment in return for not releasing their passwords as well as ‘intimate’ photographs and videos.

Phishing attacks usually extend past emails and often include messages of social media, SMS and can also include calls. A phishing attacks is basically any time someone tries to get your personal data from you while pretending to be someone they are not.

In these times it is important to remember not to blindly open links and email attachments, even if they’re from people you know or people whom you communicate with regularly.

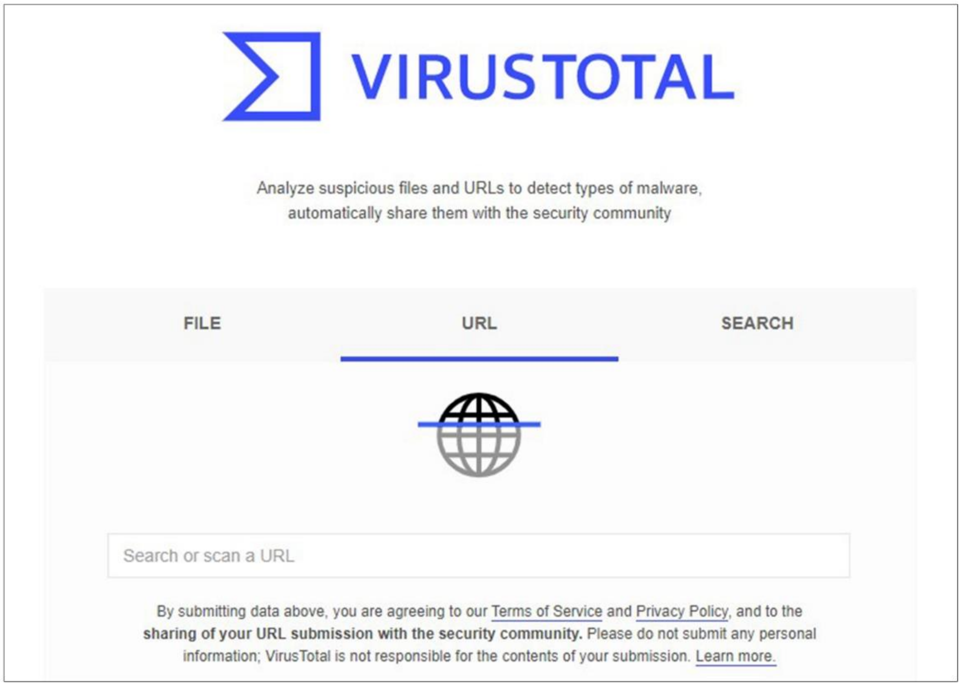
Because we are so used to receiving emails and clicking on links, it is often difficult to un-learn that habit, however, whenever you do receive an email, especially if it is out of the blue, make sure you're doing the following:

1. Run a quick Google search for recent phishing attacks. Attackers often mask themselves as large companies like Facebook.

2. Check the email and link for spelling errors. This is the easiest way to decipher a phishing attack link.

3. If the link is from someone you know, ask them on a separate platform what they've sent you and why.

4. Run the link through a checker like VirusTotal.



VIRUSTOTAL

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your URL submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

DATA PROTECTION AND BACKUP

You are most likely working from home, or remotely. Even if you are going to the field to report, there are lots of resources that are not available to you anymore. These are resources and securities that being in an office or a newsroom give you. Being at home, or working remotely puts a lot more responsibility on you to protect yourself, your devices and your data. It is important to keep some basic habits in check.

‘Remote Work Data Checklist’

1. **BACKUP BACKUP BACKUP**
2. **Establish one device as your ‘work device’**
3. **Password protect your folders**
4. **If you can, avoid using a shared device for your work files**
5. **Maintain your backups constantly**

A couple of these might need a little explanation so here we go:

- Establishing one device as your work device is important because of the nature of your work. As a journalist, you have lots of data coming in, files to download etc. If you have one device where all of this data is in, it makes it easier for you to transition back to work whenever offices do resume. It is important to start thinking about how you’re going to go back to normal life, and that also includes how you’re going to go back to the office.

- Having a separate device for yourself is considered a privilege in a lot of parts of the world. However, if you can manage to get a device from your employer or already do have a work-issued device then it is crucial that you maintain it and make sure no one else uses it.

- You need to keep and maintain a backup for your data. You could save it using a cloud service or use an external hard drive. Having a backup is important because it ensures, to a certain extent, that your data is safe in the case that you lose it on another device.

CAUTION: 📢

Do not download files on multiple devices or on an ad-hoc basis. Working remotely can be challenging but one must always try to be organized and collected. This helps to keep you productive as well as helps you track all your data.

HOT TIP: 💡

When starting up a backup, a fun way to think about it is the 3-2-1 method.

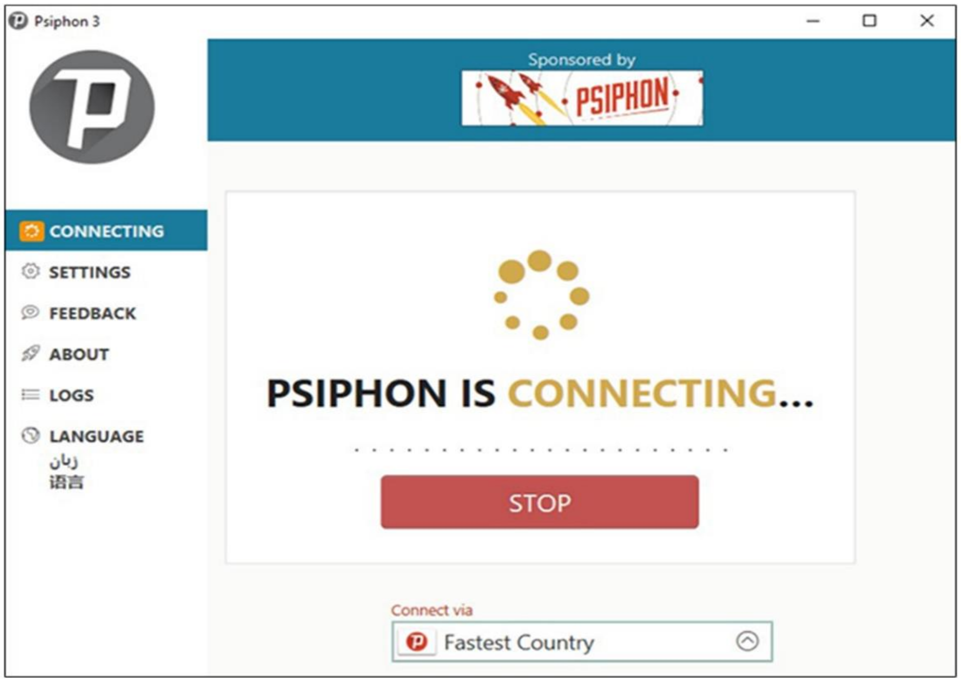
- Have three copies of the files you want to back up
- Two copies should be saved at a location that is easily accessible to you
- One copy should be saved at an offsite location, which nowadays would be a cloud service or platform.

PRIVACY:

Privacy is an important part of keeping yourself safe in the digital sphere during this pandemic. In a lot of countries world over, the COVID-19 lockdown has been taken as an excuse by governments to increase their surveillance on the general public and this also includes journalists, especially those covering the outbreak and how it is being dealt with.

A Virtual Private Network (VPN) is quite a powerful tool to have with you during these times. A VPN is able to mask your IP address and make it seem as though you are a user from another country. This makes your movements online harder to track and watch and also gives you a more secure internet connection. It is important to remember, however, that some VPNs still keep a record of your online activity so it is best to do your research before installing and using any particular VPN.

A VPN that we recommend during our training sessions is PSIPHON.



PSIPHON IS CONNECTING...

Connect via

Fastest Country

It is also important to focus on messaging apps and tools that you may use on a frequent basis. As mentioned earlier, some video conferencing services fell victims to attacks by cybercriminals as these calls were intercepted and disturbed. This is a serious violation of privacy and the same thing happens when we use messaging services, it's just that it is much more subtle. Most messaging service providers save copies of your messages, pictures, and videos on their own servers.

If the contents of your conversations are sensitive, or if the person you are speaking to is high profile then you must consider using services that are genuinely 'end to end encrypted'. Apps like Signal and Jitsi Meet offer such services and have been proven to be safe. With a lot more traffic on the internet in general, safety and privacy are concerns that have become magnified, and we must all take the precautions we can.

HOT TIP:

As the internet is becoming a lot more burdened, video calls may not work as they once did. Opt for voice calls and enjoy better service, while also getting through those important meetings and phone calls.

MOVING FORWARD:

Now that we're going ahead and working remotely or from home, it is important that you and your colleagues decide on some protocols for digital security. This can be something that you decide at an organizational level or at an individual level, depending on if you're working on a freelance basis or a permanent basis.

Digital security is about community, and you will only be stronger if everyone around you is strong.

When thinking of ways to formulate a plan of action, think about the following prompts:

1. Are there any existing policies in place? Do they need revising?

2. On average, how many people have access to your work device at home?

3. How much data do you go over a day for your work/ pitches?

4. How many other people are using the internet wherever you're working currently?

5. Are you able to access cloud services or external hard drives?