ONLINE SECURITY FOR MEDIA PROFESSIONALS

ROCK ADOTE

JULY, 2019

PROFILE

Rock is a cyber-security professional and a seasoned software programmer with over a decade experience in secure software development for the Nigeria Financial Services Industry. He holds a master's degree in computer systems. An EC-Council Certified Security Analyst. In partnership with several cyber security consultancy outfits, Rock has empowered personnels of several Nigerian Government Agencies on Cyber security amongst which includes Nigerian Apex Bank - Central Bank of Nigeria and Regulators such as Nigeria Deposit Insurance Commission. Having served as a Senior Solutions Engineer and Analyst for MI-C3 – a multinational who provides Software-as-a-Service, Infrastructure-as-a-Service, Platforms-as-a-Service and Business Process-as-a-Service that meets the operational demands of Africa's largest provider of telecommunication infrastructure, He is currently on the board of several technological start-ups across Africa and also the co-founder of protectyourdata.ng - A Cyber security Advocacy Group that aims to sensitize institutions on information security best practices.

KEY POINTS

GLOBAL CYBERSECURITY OVERVIEW

TRENDS IN NEW MEDIA AND JOURNALISM

THE IMPORTANCE OF ONLINE SECURITY FOR MEDIA PROFESSIONALS

21ST CENTURY REALITIES

CASE STUDIES

BEST PRACTICE FOR MEDIA PROFESSIONALS

CONCLUSION

GLOBAL CYBERSECURITY OVERVIEW

Information is one of the most powerful tools.

It influences political decision-making and public opinion and ultimately establishes most of the priorities and the agenda items of the international community. this makes the independence of journalists and the accuracy of their reporting particularly important, especially when covering security issues. Hence, inaccurate and misleading information can produce negative effects by creating improper policy responses or negative civil society reactions.

Information is the Currency of the modern age.

TRENDS IN NEW MEDIA AND JOURNALISM

Today's digital landscape poses new challenges and offers new opportunities for media professionals.

Technology has changed how journalists go about some of their most fundamental practices, like finding, verifying and securing sources, protecting sensitive information and conducting fact checking.

New technologies (i.e. reporting apps and desktop tools, electronic databases, unmanned aircraft and encrypted messaging platforms) have also created new opportunities for quality journalism.

THE IMPORTANCE OF ONLINE SECURITY FOR MEDIA PROFESSIONALS

As technology further advances, so does the potential for cyber threats and hacks. Whether journalists are reporting from war zones, crime-ridden countries, or within national borders, they are often at risk of digital surveillance from those who want to silence their voices.

Technology's advancements led to digital lives and physical lives moulding into one—people constantly carry their phones, computers, and other trackable devices.

If a person is targeted digitally, his or her life may also be under threat.

21ST CENTURY REALITIES FOR MEDIA PROFESIONALS

#FACTS

Today, there is no anonymity on the internet unless you take specific measures that include disguising your digital identity and activities and taking measures to secure your online communications but even so, it is not guaranteed that your communications are safe.

Someone, somewhere will be able to monitor your activities online.

People (whether they are your Internet Service Providers -ISP or national authority) out there who have access to your internet connection can monitor your activities online

They will be able to tell when and where you have visited certain websites or chatted with a particular person online via Skype.

INTERNET SURVEILLANCE

Private browsing - Cleaning your cookie and internet history is not enough. If you want to minimise the chance for internet surveillance, you can use Tor Browser so that no one can see what sites you have visited or track down your location. It will also allows access to websites not available for normal browsers.

Tools:

For Windows: TorBrowser || For Mobile: Orfox, Orkut

EMAIL SECURITY

- Using temporary email service to remain anonymous - Using temporary email service to remain anonymous if you want to avoid spam or don't want to give your real email address to strangers, you can use temporary email service to remain anonymous. The service provides you with an unique email address that you can dispose.

Tools for Email Service:
GuerrillaMai, Mailinator

Mail Encryption:
Mailvelope

BYPASSING CENSORSHIP

How to bypass internet censorship - In countries where internet censorship is a commom practice to oppress the media or critical voices, access to information or communication can be a problem for journalists and human rights activities. There are ways to bypass internet censorship that come at a very small price. You can rent a virtual private network (VPN) that will encrypt and redirect all your traffic from your computer to that VPN.

Tools for Bypassing Censorship:
YogaVPN, Betternet VPN and any 3rd Party VPN

MOBILE SECURITY

- We cannot remain anonymous using our mobile phones - because the same network that provides you with internet access also provides you with the mobile communications. The ISP can locate you even though your mobile phone is not switched on. In many countries, you are required to provide your ID in order to buy a SIM card.

Securing your mobile
FakeGPS – Obfuscate your location and fool tracking apps
Use mobile 3rd Party VPN to protect your online communication
Leave connections off when you don't need them

PROTECTING REALTIME COMMUNICATION

Securing instant messaging and audio/video conversations. Most popular instant messaging and audio/video platforms (such as Skype, Facebook chat, Google Hangout, etc.) that are owned by big corporations no longer provide the absolute privacy and anonymity you want. If you want to communicate sensitive information, you should use peer-to-peer online instant messaging and audio/video conferencing platforms.

Tools for Protecting Communication
Cryptocat, meet.jit.si, Whispersystems, Signal etc.

YOUR DATA YOUR GOLD

DATA MANAGEMENT TIPS

Deleting your data – You think by clicking the "delete" button, your file will be deleted forever? The answer is "no". The file you deleted can still be recovered even though it may no longer be visible. It is still somewhere in your computer or usb stick. In order to delete your file permanently, you can download free software (such as CC Cleaner) that allows you to delete your file permanently.

Recovering your data – However, journalists can use this to their advantage. If you are ever forced to delete your photograph by the authority, you can do so with the assurance that you can retrieve your photo when you get back to the office or home.

Metadata management - Always manage or delete your metadata because it tells people a lot about you and how the file is being created. If you do not want to remain anonymous or protect your sources, keep the meta data for yourself.

Secured data back-up - You should always have a back-up of your important data but use a secured back-up. If you don't want to carry sensitive data around when travelling, you should store your data in a secured drive (such as Mega.co.nz) that you can have access to wherever you go. Before storing your data, take one more security step to encrypt your data before storing them in a remote drive or cloud.

BEST PRACTICES

MAKE MISTRUST YOUR MOTTO

- Don’t work with your back to a window.
- When travelling by train or plane, put a privacy filter over your laptop screen to limit lateral vision.
- Avoid being separated from your equipment.
- Get a webcam cover.
- Don’t download any files or click on any links sent to you from unknown sources. Personalized phishing attacks are very common.
- Carefully check the email address or online presence of anyone who shares a link with you. If in doubt, verify the sender’s identity with other contacts or by using a search engine.

2 - PASSWORDS: SECURE YOUR CONNECTIONS

- Use passwords to protect your online activity.
- Use a pass phrase rather than a password.
- As a journalist, you should segment your digital activities and use several email addresses: a personal one, a professional one, one for online purchases and so on.
- Remember to disconnect whenever an online operation is finished.

3 - PROTECT YOURSELF FROM CYBER-ATTACK

- Online attacks, whether aimed at taking over an account or smearing a journalist's reputation, have the same objective: to discredit the messenger in order to kill the message.
- Check social network confidentiality rules and clean up your profiles, keeping in mind that doxxing, the aggressive use of personal details found online – especially on social networks – is increasingly employed in harassment campaigns against journalists.
- Use an antivirus AND an anti-malware such as Malwarebytes.
- Activate your firewall.
- Keep your operating system (Windows, macOS, etc.) up to date.

4 - DELETE YOUR DIGITAL TRACKS

- Use Namecheckr to check your online presence.
- Remember to disconnect after checking your email, Facebook account or Twitter account.
- Erase your browsing history.
- Never save a password in the browser of a public computer. If you have saved one by mistake, erase the browsing history when you finish working.
- Delete cookies. The way to delete this kind of data varies from browser to browser. A good way to avoid making any mistakes is to use the private browsing mode in Firefox or Chrome.
- at an advanced level, you can use Tails

5 - ENCRYPT YOUR ACCESS TO ONLINE SERVICES

- Use encrypted messaging apps such as Signal (while keeping up-to-date of any reports about vulnerabilities in these apps).
- FlowCrypt is a Chrome and Mozilla extension that enables end-to-end encryption of email.
- Privnote and ZeroBin are websites that allow you to send someone a link to an encrypted message that self-destructs after being read.
- To talk to your sources via the Internet use apps such as Jitsi Meet, a free and fully encrypted Skype equivalent.

6 - SECURE YOUR BROWSING

- Install a VPN in order to encrypt your Internet connections.
- Install the Tor Browser, which allows you to browse anonymously.

7 - IN A HOSTILE ENVIRONMENT, DON'T LET YOUR PHONE BECOME YOUR WORST ENEMY

- Don't put your contacts' real names in your phone's contacts list. Assign them numbers or pseudonyms so that others (the police, armed groups, and so on) cannot get the details of your network of contacts if they ever seize your phone or SIM card.
- Take spare SIM cards with you whenever you think your SIM card might be confiscated (at demonstrations, border crossings, checkpoints and the like). If you ever have to get rid of a SIM card, try to destroy it physically.
- Lock your phone with a password if it has this feature. Change the default PIN of your SIM cards and lock them with this code.
- Consider turning on your phone's flight mode in situations in which the security forces might target people with mobile phones (at demonstrations, during an uprising, or whenever a crackdown is possible). The authorities could later demand the call or SMS records or phone data of any individual at a given location at a given time in order to carry out mass arrests.
- Turn off geolocation in your apps unless you need to use it. If you are using your mobile phone to stream video live, turn off the GPS and geolocation functions.
- If your phone uses the Android operating system, software for encrypting your browsing, chats, texts and voice messages is available from the Guardian Project and Signal. When using your phone to go online, use the HTTPS Everywhere extension.

CONCLUSION

Journalism is one of the cornerstones that makes our democracy possible, but today journalists face constant digital threats to their ability to do their jobs as a watchdog for government and industry. Worse, journalists don't tend to be the most tech-savvy people in the world, and they struggle to defend themselves.

Hence opportunities like these aims to sensitize stakeholders on the trends and techniques available to ensure safe journalism in an inter-connected world.

THANK YOU