Safe Online
by CcHUB

WORKING FROM HOME

A DIGITAL SECURITY GUIDE

Co-Creation Hub

As the number of confirmed cases of CoronaVirus (COVID-19) increases across Africa, and indeed all over the world, many organisations have no choice but to shift to remote work as a way to protect their employees and slow the spread of the pandemic.

However, remote work is a seldom employed tool in these parts and companies, especially startups and SMEs, might struggle with the implementation of remote work policies. The world has never experienced remote work on the scale at which it is being employed presently, and for these reasons, the cyber security risks will be at unprecedented levels. So while there are many benefits to employees working from home, there are also a myriad of cybersecurity dangers that organisations cannot afford during these times of uncertainty, reduced productivity and general business disruption.

At GovLab by Co-creation Hub, we have put together this digital security 'Work-From-Home' guide. The guide serves to protect everyone working from home in these perilous times and beyond.

Why is this guide important?

Why is it important to stay safe online?

- The cybercrimes of today's world are both incredibly sophisticated and remarkably basic.
- Data breaches can cost companies anywhere from nothing to millions of dollars in losses.
- Your personal information is 'unique' and 'identifiable'. This can mean anything from a photo of you at 10 to the password to your internet banking/Instagram page.
- Spam emails are annoying but they can also be dangerous.
- Hackers are taking advantage of the panic caused by the COVID-19 outbreak.
- Your mental health and wellness in these times is important.

Content

- Build a Security Culture
- Device Security
- Network Security
- Email, File-sharing, Video Conferencing and Instant Messaging
- Data Classification and Data Loss Prevention
- COVID-19 Phishing Scams
- Mental Health in the Digital World

Build a Security Culture

The digital security and resilience of the average organisation at this time will depend on its security culture and the awareness of its employees. Just as one case of the Coronavirus can bring an entire city to its knees if the patient fails to adhere to basic health and safety protocols (like isolation), a single employee can cause serious damage to an organisation security-wise. This has always been true, but it is even truer in these times as employees switch to remote work. Whereas, an IT Administrator can configure firewall rules to block malicious inbound traffic into a company's network and minimize an employee's negligence, this is not the case when different employees are working from different points.

Organisations without an existing culture or value system on security will suffer. However, it is never too late to start building out and implementing one, even if you have sent your workers home already.

Here are the top 5 elements that should exist in every organisation's security culture:

A Low Power Distance Index
Here is a very simple way to look at the Power Distance Index in terms of security.

Awele, a 3 month old associate in the Accounting department has just received an irregular email from the CEO asking for the Quickbooks login to quickly verify transfers to a partner. The email looks legitimate but Awele is not too comfortable with the ask. Awele is at home and the Head of Accounts is unavailable and unreachable.

What is Awele's course of action? Does she just send the details because she is unable to question the legitimacy of the sender? Or does she wait until she is able to confirm from the Head of Accounts knowing that the delay will not reflect badly on her job?

Think about how Awele would react in your organisation. The Power Distance Index (PDI) of any organisation is reflected in how employees respond to the opinions and requests of higher-ranked or C-suite staff especially when they have a different idea or opinion. Individuals have different personalities and different levels of confidence, but an organisation that is digital security conscious will encourage a low PDI that encourages employees to challenge irregularities.

High Level of Individual Responsibility
Digital Security is everybody's problem, from the people at the frontdesk to the people in non financial positions. Employees should be groomed to understand their value as part of the organisation, and with that value comes a responsibility to protect the organisation. This means looking out for the next employee, protecting one's own space and pointing out anomalies where they appear.

Technology Use

This speaks to the responsible use of technology in an organisation. Organisations should develop an overarching policy that includes but is not limited to the use of emails, passwords and authentication, computers, phones, file-sharing, network, etc. While the consequences of misuse should not be the focus of the policy, it should set the tone for the consequences of misuse or noncompliance.

Investment and Leadership

How top management view, prepare for and respond to digital security needs is a great determinant of the success of the security culture in an organisation. Security is not cheap, but instead of seeing it as an expense, business heads should see security as an investment. The average cost of a data breach far outweighs the cost of forestalling its occurrence. In these times of remote work, leaders should be willing to invest to protect employees working from home.

Communication and Reporting

Staff should be encouraged to report incidents immediately they notice them and should be trained on an Isolate and Report (IR) protocol in this regard. It is important that employees are not made to fear any repercussions for reporting or shy away from the responsibility as hackers and malicious entities only need one unprotected system or negligent employee to cripple a business.

Device Security

In these times of social distancing, it is important to evaluate how safe our devices are. How do we protect smartphones, laptops, tabs, computers etc from unauthorised access? Keeping devices safe when working from home is important as poor device security practices opens doors to cybersecurity challenges.

Here are some simple tips to follow for employees:

- Enable full device encryption: Encryption is the process of scrambling information or data in such a way that makes it illegible to all but the intended recipients of that information. Among other things, encryption helps to keep the content on devices safe and protect against bypassing its password.

  Below are the 3 major encryption services for devices, and how to implement each one.

  Filevault (Mac)
  https://support.apple.com/en-us/HT204837

  Bitlocker (Windows)
  https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

  Veracrypt (Platform independent)
  https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html

- Enable password protection on all your devices.

- Make sure to use strong passwords. Check the strength of your password here. Strong passwords are typically between 8-12 characters long and contain a mix of alphabets, numbers and special characters.

- Set antivirus and system update to "automatic".

- Enable lock-screen and biometric security on devices (where it applies).

- Create a separate user account with limited privileges on work PCs. In the event of a theft or having to share the device with a friend or family member, this ensures a third party is unable to have privileged access to the device (and company's) resources and information.

Here are some guidelines for employers:

- Implement an acceptable-use policy for devices (this effectively sets standards and guidelines for how employees may use company devices).

  Ensure all work devices are registered and logged. In the event of a theft, details can be provided to law enforcement.

- Mandate the setting up/enabling of ‘Find My Device’ apps/settings on company devices. For example, with Windows 10, Microsoft includes a Find My Device ability for devices using the operating system. Ensure that employees enable this feature to help track when their laptop is missing. Where devices do not come with the features pre-installed there is a myriad of apps that provide the necessary functionality.

- Ensure that laptops and computers have antivirus installed and updated.

Network Security

Working from home means that employees are more responsible for their own internet connection than they are at work. This poses an issue for companies as the choice of the internet service provider is taken out of their hands.

Here are some network security tips to keep in mind:

For employees:

- Secure your home router or MiFi devices: The important considerations here are the encryption standard (security level) of the router (is it “WPA”? “WPA+TKIP”? “WPA2+AES”?) and the password strength of the router/MiFi devices. Routers with the encryption standard of “WPA2+AES” are recommended. Every router has a default password. It is recommended that this default password be changed. To change the password go to settings on the router. To access router settings see the steps in the box on the next page.
  (For more on creating secure passwords, refer to the section on Device Security)

- Limit network range or radius: Individuals who operate their own home network should ensure that the network radius is limited to the area of use. Networks visible/accessible outside the home can be a strong target for hackers, who can position themselves around long enough to get into the network.

- Network radius can be adjusted appropriately in the network settings on each router.

For Employers:

- Expand your acceptable-use policy[1] to cover and guide employees on preferred networking devices to use while away from work. This should cover routers and modems, encryption standards, passwords, etc.

Your router or MiFi device stores the settings for your home Wi-Fi network. To make the necessary changes, log into your router. A quick look at the user manual that came with your router will show you how to log into the router. From there, you can rename your network, modify the password, adjust the security level (“WPA2+AES”) and set up the network range to your preferred radius. Here is how to do it:

i While connected to your router, launch your internet browser application

ii Enter the IP address stated in the user manual (usually something like this: 196.168.1.1)

[1] Policy that details the acceptable ways in which employees can use office space, devices and networks.

iii A login window appears

iv Login with the default credentials (stated in the user manual, usually “admin” or “user”)

v Go to the menu (usually a side bar or a top bar)
Select “Settings”

vi In “Settings”, several options listed allow you to either rename your network, modify the router password, adjust the security level (“WPA2+AES”) and set up the network range to your preferred radius.

vii To adjust the network range for instance, select “Network Setting”, look for “Transmit Power” or “TX Power”

viii Adjust between “1” to “23”. “1” being the least distance and “23” being the longest distance range

Email, File-sharing, Video Conferencing & Instant Messaging

Email
Although the choice of email service providers are endless, the security challenges with emails(especially with the increasing number of people working from home) are fundamentally the same.

We have highlighted some of the most common challenges below:

Password Hijacking
This is a process where an attacker steals the email login credentials of an employee. This can be done in many ways such as by using a password-cracking tool, dumping a database,[2] redirecting a user to a malicious website that looks legitimate, looking over the shoulder of a user as he or she types their password, using a keylogger that records a user's keystrokes as they type in their passwords, etc.

The solutions to preventing email compromise are simple:

- **Change/Use Strong Passwords** Employees should use strong passwords as already mentioned in this guide. We also recommend that passwords be changed monthly. Changing passwords ensures that if your credentials have been compromised on another platform (e.g, LinkedIn), your email remains safe. Typically when a database is compromised in a data breach, users' information and credentials are sold for next to nothing on the dark web.[3]
  Employees should also ensure they use strong passwords.[1]

  (Employees can check if their emails have been compromised in a data breach here: *https://haveibeenpwned.com/*).

  Employers can mandate that employees change their password every month by implementing the Interactive Logon feature that prompts users to change password on a given date.

  This policy setting determines when users are warned that their passwords are about to expire. This warning gives users time to select a strong password before their current password expires to avoid losing system access.

- **Avoid Logging into your Work Email from "Unknown" Computers** Computers and devices not owned by employees (or the company) are unknown computers, as the software and programs running on them are not completely known to the employee and as such should not be used to login to work

[2] *When a database is dumped, it simply means it has been hacked, and the contents have been transferred by an unauthorized entity or hacker.*
[3] *The dark web is a special part of the internet accessible only with specific browsers and URLs, and is a hotbed for illegal transactions.*

emails. (Employers should include this in their general or email policy, if there is).

- **Understanding Phishing Scams** Phishing scams target unsuspecting users with legitimate-looking offers or propositions aimed at deceiving them into giving out information they should not give out.

  To learn more about phishing scams in these times go to chapter titled “COVID-19 Phishing Scams”.

Content Sniffing

Hackers can eavesdrop on content passing through a network which can allow them to get hold of credit card information, login credentials (usernames, passwords, phone numbers, etc) and even files shared. Content sniffing is common when users connect to insecure or public networks (refer to Network Security above for more).

Employees can protect themselves from this type of attack by:

- **Connecting Only to Trusted Networks** Working from home means that employees will work with whatever network available. This includes home network and public networks, and both come with different types of risks. Employees, especially those who work on sensitive materials or documents, should only connect to networks that have been tested to be secure (this eliminates using public networks altogether).

- **Email Encryption** Pretty Good Privacy (PGP) is a program that encrypts emails and renders them unreadable and unusable to third parties or unauthorized entities. Before now, this was a service used by organisations dealing with high-end classified information. However, with the risks posed by remote work, it has become essential for employees working from home.
  The most commonly used PGP service is Mailvelope. A step-by-step guide for installing and sending your first encrypted mail using Mailvelope can be found here: *www.mailvelope.com/en/help*

- **For Employers** Although companies do not need to implement the use of a PGP service for all staff, it is vital for employees handling sensitive data).

> *In these times it is important for organisations to offer virtual accessible training for any new technology that will be introduced or required.*
>
> *Communicate expectations for the deadline of general uptake and provide regular tips to help people who might be struggling.*

- **Using VPNs** VPNs, or Virtual Private Networks are essential for anyone working remotely - especially if you will be using a public wifi (like from hotels or cafes). A VPN "tunnels" or protects your connection to the internet and ensures that attackers monitoring a network can't get a hold of your data or communication.

  Employers should look at Investing in VPN solutions for staff. This is essential as it does not leave the decision and choice of what VPN to use solely in the hands of employees. Also, having a single choice of VPN for all employees means that it is easier to troubleshoot and have a uniform experience for all staff.

  Below are some good VPN options to consider

  ExpressVPN CyberGhost NordVPN® LANTERN

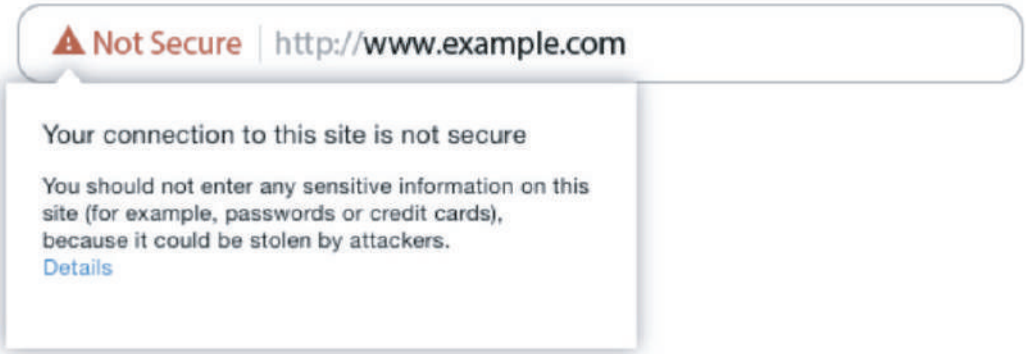
  PSIPHON

- **Using Secure Browsers** Using the right browser is vital for email (and communication) security.

  Below is a list of secure browsers you should (seriously) consider using as you work from home:

  THE ONION ROUTER Tor Firefox Browser brave IRIDIUM BROWSER

Avoid websites with HTTP and not HTTPS: Websites without a security certificate will display a “Not Secure” notice in the URL address bar. Such websites should either be completely avoided by employees, or they must avoid entering any vital information on such websites (like usernames, passwords, credit card numbers, etc).



Not Secure | http://www.example.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.
Details

Phishing

This is the fraudulent practice of sending emails claiming to be from a reputable or trusted source in order to induce individuals to carry out an action intended by the hacker or perpetrator. Phishing can be employed as a technique by hackers to compromise email addresses, steal login credentials and even eavesdrop on important conversations or exchanges.

Phishing is addressed in-depth in the “COVID-19 Phishing Scams” section.

File Sharing

In these times, it is more important than ever to share files securely.

Below is a list of secure file sharing platforms and tools to use for sensitive data/information:

Filezilla
THE FREE FTP SOLUTION

EGNYTE

securedocs

Dropbox

Google Drive

box

Password Managers

Under this topic of file sharing is also the sub category of the sharing of passwords for applications by teams. A password manager solves the problem of shared passwords while also giving employees increased management and security.

Here are some trusted password managers to consider for your teams:

Videoconferencing

Before COVID-19, videoconferencing was an important part of daily work for the average organisation. Communicating with partners, funders, clients and even teams across different locations have all been made possible because of teleconferencing solutions. Tele/video conferencing platforms will, however, now face the biggest tests (of stability, bandwidth and security) ever, owing to the increased number of people who will now depend on these platforms for business continuity. The biggest threats with using videoconferencing platforms are eavesdropping and privacy concerns. Platforms without end-to-end encryption pose the most risks, while others have been notorious for storing (and sharing) users' call logs.

Below is a recommended list of video conferencing solutions to consider for your business at this time.

Instant Messaging

An instant messaging service is key to the success of remote work. However, since a lot of important communication will be taking place over emails and instant messaging platforms, it is important to choose a secure and stable option as these platforms will increasingly become targets for hackers.

Here are some secure - and stable - instant messaging platforms to consider for your business in this period:

For a detailed comparison, see: *https://www.securemessagingapps.com/*

Data Classification and Data Loss Prevention

Data Classification

The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All data in the organization should be classified into categories. We have devised a sample classification below to aid you in that classification.

Confidential or Classified Data

Data should be classified as 'Confidential' when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the company or its affiliates. Examples of confidential data include login passwords (accounting software, server, password manager, etc), employee personal data, payroll, health data, business agreements, etc.

Internal Data

Data should be classified as 'Internal' when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk. A reasonable level of security controls should be applied to internal data.

Public Data

Data should be classified as 'Public' when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the organisation.

Examples of public data include press releases, workbooks, While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of some of it.

Table based on: Carnegie Mellon University
https://www.cmu.edu/iso/governance/guidelines/data-classification.html

Once the data in an organisation has been classified it becomes easier to see who should have access to what. This is important for remote work as restricting information to only necessary parties minimises the potential for a breach.

Data Loss Prevention

Organisations today are subject to either one or more data protection laws. These laws can range from The Nigeria Data Protection Regulation (NDPR) to Kenya Data Protection Act (KDPA) or even The California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). The protection of personal information is at the heart of compliance to these laws.

A survey by the Ponemon Institute revealed that the top 3 causes of data breaches are:

- Missing Devices (42%)
- Negligent Employees (16%), and
- Negligent Third Parties (10%)

With employees working from home, the risks of data breaches are significantly higher as very minimal control can be enforced by organisations (for instance, choosing and configuring network service tools) for the protection of sensitive data.

Enter Data Loss Prevention also known as DLP.

Data Loss Prevention is a security strategy (aided by a series of processes and software) aimed at preventing the conscious or accidental access, use/misuse, leakage or exfiltration of sensitive data.

It follows rightly classifying data (as Confidential, Internal or Public) and identifying which data sets need the most protection or safeguarding and includes the assigning of roles or privileges to specific individuals within the organization (like editing, copying, transfer, downloading, etc) so that access and misuse of data is minimized.

Here are a few DLP solutions organisations can implement

Symantec Data Loss Prevention

McAfee Total Protection

Check Point Data Loss Prevention

COVID-19 Phishing Scams

Phishing is a cybercrime where a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking details, and passwords.[4]

Already, hackers have begun taking advantage of the fear and panic caused by the Coronavirus concerns (An example is this widespread case leveraging COVID-19 live maps). As the virus spreads to new areas and as people are asked to practice social distancing; these scams will rise over the coming weeks and months.

Worst-hit countries like Italy, Spain and the USA have seen a spike in COVID-19 phishing attacks. The relative simplicity of these attacks coupled with what they exploit (fear and panic, urgency, trust and a need for remote access) make them a serious concern for any company.

The two trends we have seen (as detected and reported by Cynet) are:

Remote User Credential Theft
This phishing attack takes advantage of the need to access official files and resources from a remote location. Many companies with on-site servers will now necessarily have to invest in remote access software like Teamviewer, LogMeIn, Remote PC, etc. This increased use of remote tools has seen an equivalent rise in remote user credential theft. The logic here for hackers is simple: get hold of any employee's login credentials, and you have access to the company's files, documents, intellectual property, etc. The attack exploits users' inability to recognize legitimate and fake urls and websites. Hackers can clone or mirror a company's website and subdomains with the aim of directing unsuspecting employees to this resource where they may then log in with their legitimate usernames and passwords. More than ever, employers must now educate their employees on how to identify fake urls, and report them.

We have a detailed article on identifying phishing scams and fake urls here: *https://safeonline.ng/fundamentals/how-to-avoid-phishing-scams/*

Weaponized Email Attacks
Email-based threats have been growing rapidly over the last few weeks in COVID-19 hit territories. Weaponized email attacks have been around for a long while and the goal has not changed: to get the target to click on a link, download a file, or reply with vital information. Although this is an old form of attack, it has greatly evolved with new malware forms and evasion techniques that make it difficult to identify or track.

The advice to employees here are as follows:

[4] *https://www.phishing.org/what-is-phishing*

How to protect yourself from falling victim to Phishing

Scrutinize the sender's email address

Email addresses can be easily spoofed. An attacker may create an address very similar to the Manager's or CEO's asking an employee to urgently send a file or complete a transaction. An email like manager@litigation.com may look exactly like manager@litigation.com, however they are different. The first email address is on the domain LITIGATION.COM, while the second is IITIGATION.COM. Employees should scrutinize emails and pay attention to these nuances, especially if the sender is requesting you to click on a link, download a file or send critical/confidential information.

Analyse the tone of the mail

Phishing emails typically sound urgent or seek to instill fear or panic, or exploit the basic human tendency to trust.

Unsolicited mails that seem urgent (e.g, your CEO asking you to quickly make a money transfer to an unknown client) or attempt to exploit fear (especially around COVID-19) or appears legitimate but asks you to do something unprecedented or mistrustful (e.g, does your manager usually require your username and password because his unfortunately isn't working?).

> *Employers have a duty at this time to put in place extra levels of verification and make it clear to staff that they should not be doing things they are uncomfortable with, or that appear suspicious.*

Inspect the link or attachment

Attached links and files are the holy grails of phishing scams. As earlier mentioned, malware is evolving and becoming increasingly sophisticated and difficult to track or identify.

Downloadable files within emails don't have to be downloaded, and if they are from an unknown source, they shouldn't be downloaded at all. Employees can simply tap on the file (after steps 1 and 2 above have been ensured) and read the content of the file within the email itself without downloading. If the files can only be read when downloaded, DO NOT download them, instead, an extra level of verification must be used to ascertain the identity of the sender (either via instant messaging or direct calls).

Mental Health and Digital Wellbeing in a Pandemic

Hello!

We hope you have enjoyed this guide and have found it useful. Chances are that you are reading this at home. Amidst the uncertainty that this pandemic has brought, and the barrage of information, it is important that you stay safe online and that you protect your mental health. GovLab has put together a list of 10 things that you can do in these times to protect your space and the internet as a whole.

Take Media Breaks
Apart from the daily coverage of how the coronavirus is spreading, news platforms as well as social media platforms are in a state of information overload. There is information about what governments are doing and what they aren't, how the disease is being spread by people's negligence, number of deaths, the situation in hospitals and a barrage of details about the pandemic. To be constantly tuned in to this spiel of information can cause anxiety and affect your mental health. That in turn affects how you engage both online and offline.

Take Media Breaks. Commit to disconnecting from the news cycle and social media for a few hours everyday. You can commit to not checking social media while you are working or for designated times during the day.

Do not feed the trolls
In these times where information is uncertain, individuals may be purposefully incendiary or may try to make light of particular situations in order to gain a reaction. Do not engage. Engaging amplifies their voice and spreads their message.

Do not amplify fake news
Question everything twice and then question again before sharing information online and offline. Fake news is dangerous in these times no matter the intent behind distribution

Stay in contact with your work friends
Touch base with people from work from time to time. As you work in the same organisation they are well placed to understand your frustrations and can be a listening ear to let off some steam.

Stay active and healthy
This is important for both your mental and physical health. The recommended 30 minutes of exercise everyday is advised by medical experts around the world during this pandemic.

Practice kindness and compassion online
In these times, humanity needs as much compassion as it can get

Amplify the good stories
There are many stories online of human kindness in the midst of the pandemic. Share those stories as much as you can as they connect us to a shared humanity

Report instances of online violence
Most social media platforms have a report function. Please report all online bullying, harassment and violence that you see while using these platforms.

Be aware that there will most likely be a spike in cybercrimes
Children and teenagers are more likely to be the target of cyberbullying, sextortion and solicitation in these times. Be vigilant and report any strange activity you might notice to the relevant authorities.

Do not post or share private information in public online spaces
You never know who is watching. In these times of panic and scarcity it is advisable not to post private information online (especially pictures that may give clues about your house, your workspace or family).

CONTACT

Co-Creation Hub Nigeria,
6th Floor,
294 Herbert Macaulay Way,
Sabo, Yaba, Lagos.

T: +234 (01) 295 0555
E: info@cchubnigeria.com
W: www.cchubnigeria.com