The Importance of Cyber Security in this COVID-19 Era

#WeDey4U #FightCoronaTogether

Bernard Acquah
CIO, MTN Ghana

Preamble

- Thanks to the internet and mobile devices, businesses have an ever-expanding online footprint with their operations digitized making them susceptible to security attacks.
- Reputations can be made or broken online. This means that information security plays a crucial role in business operations.
- Today's information security attacks with varying objectives are increasingly sophisticated and complex, driven by elaborate and resilient professional organizations that innovate faster than their targets.
- A single breach can cause a domino effect, culminating in loss of revenue and goodwill, regulatory scrutiny and fines, and even share price plunges.
- These trends mean information security cannot be confined to the IT unit. Information security now is a SHARED responsibility.
- Security has to be considered as the foundation on which we operate.

Information security is everyone’s responsibility.

Security Threats of 2020

- *Year 2020 will see a transition to a new decade. So will cybersecurity.*
- *Defenders will have to view security through many lenses to keep up with and anticipate cyber crime mainstays, game changers, and new players.*
- *Tried-and-tested methods — extortion, obfuscation, phishing — will remain, but new risks will inevitably emerge.*
- *New technologies will exacerbate human error. The future looks complex, exposed, and misconfigured — but it is also defensible.*

Security Threats of 2020

- **“Attackers will outpace incomplete and hurried patches.”**
  System administrators will need to be vigilant when it comes to not only the timeliness of patch deployments but also the quality of the patches they deploy.

- **“Banking systems will be in the cross-hairs with open banking and ATM malware.”**
  Operators of mobile malware dedicated to attacking online banking and payment systems will be prolific in 2020 as online payments see more activity because banks will confirm their support for mobile payments.

- **“Managed service providers will be compromised for malware distribution and supply chain attacks.”**
  Companies are increasingly relying on outsourcing for their day-to-day activities and needs. With that come apprehensions that attacks via the supply chain will bypass and jeopardize business processes and security measures.

- **“Deepfakes will be the next frontier for enterprise fraud.”**
  Anticipated that fraud advancing in 2020 with new technologies, specifically artificial intelligence (AI). AI technology is being used to create highly believable counterfeits (in image, video, or audio format) that depict individuals saying or doing things that did not occur — commonly referred to as “deepfakes.”

- “**Cyber-criminals will home in on IoT devices for espionage and extortion.”**
  Cyber-criminals and threat actors using machine learning and AI to listen in on connected devices enterprise settings, such as smart TVs and speakers. From there, they can identify a set of targets for extortion or gain a foothold for corporate espionage.

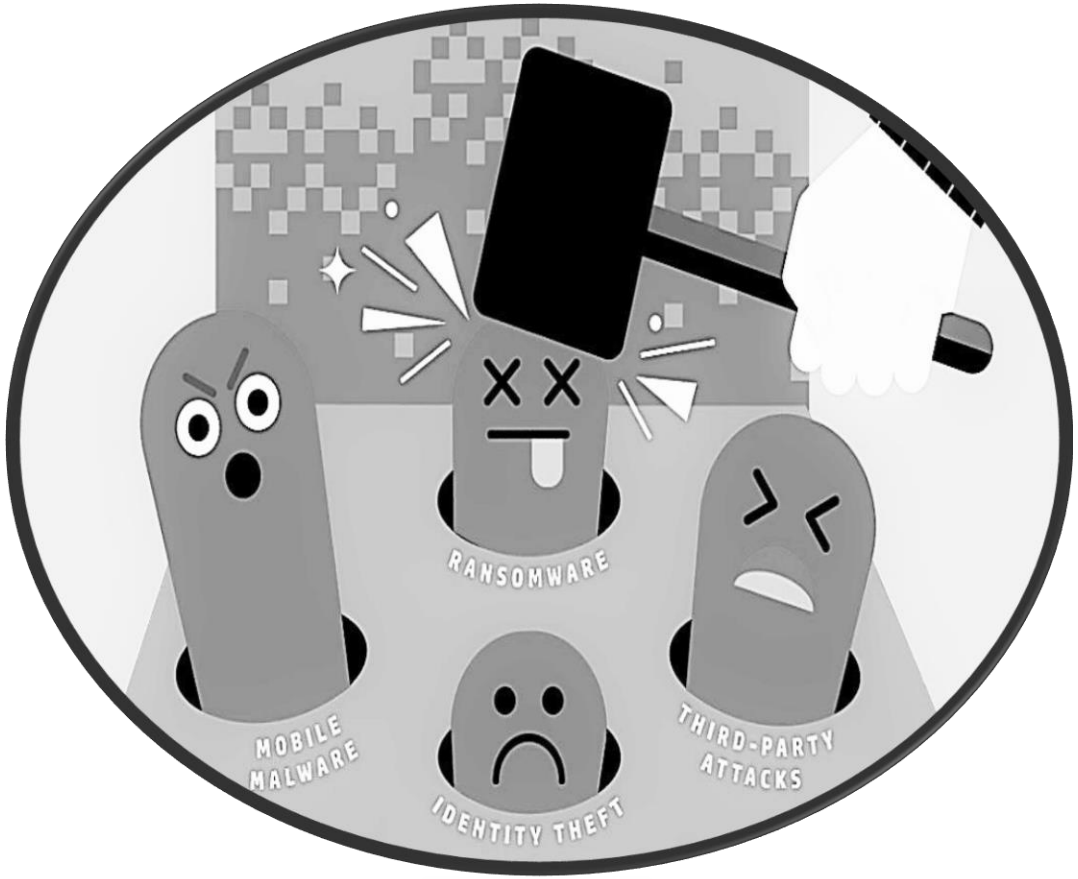
Security Threats of 2020 Cont'd

- **"5G adopters will grapple with the security implications of moving to software-defined networks."**
  As 5G rollout gains momentum in 2020, we expect a variety of vulnerabilities simply on account of the newness of the technology, including its codes and dynamic switching between environments.

- **"Critical infrastructures will be plagued by more attacks and production downtimes.."**
  Utilities and other critical infrastructures (CIs) will still be viable targets for extortionists in 2020. Extortion through ransomware will still be cyber-criminals' weapon of choice as the risk for companies is high.

- **"Home offices and other remote-working setups will redefine supply chain attacks."**
  Organizations will have to be wary of risks introduced by work-from-home arrangements and internet connected home devices that blur the lines in enterprise security. After all, working in home environments is not as secure as being in the corporate network. .

- **"Vulnerabilities in container components will be top security concerns for DevOps teams."**
  The container space is fast-paced. Releases are quick, architectures are continually integrated, and software versions are regularly pushed. Rapid development cycles may leave only little room for security and vulnerability testing. Attackers will find ways to take advantage of any weak link to compromise the DevOps pipeline.

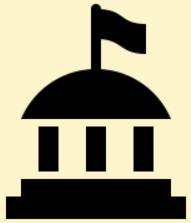


- Trend Micro (https://documents.trendmicro.com/assets/rpt/rpt-the-new-norm-trend-micro-security-predictions-for-2020.pdf)

Know Your Enemies: Threat Actors

Online criminals

Are really good at identifying what can be monetized, for example stealing and selling sensitive data, or holding systems and information to ransom.



Foreign governments

Generally interested in accessing really sensitive or valuable information that may give them a strategic or political advantage

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.

Political activists

Out to prove a point for political or ideological reasons, perhaps to expose or discredit an organization's activities.

Terrorists

Interested in spreading propaganda and disruption activities, they generally have less technical capabilities

Malicious insiders

Use their access to an organization's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest mistakes

Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address

Cybersecurity and COVID-19

"For health and safety reasons, we'll be transitioning to cyber crime."

The COIV-19 outbreak has threatened to overload healthcare delivery systems and the global economy. The impact is also being felt in the security industry.

Globally, there are reports of increased cybercrime and even though this is not yet significant there has been an alarming rise in coronavirus phishing attacks which have become the dominant method being adopted by cybercriminals.

Attackers have also been sending emails that feed on concerns about COVID-19 to spread malware. More than 4,000 coronavirus-related domains have been registered since the beginning of the year.

Threats observed include:

- **Phishing, using the subject of coronavirus or COVID-19 as a lure,**
- **Malware distribution, using coronavirus- or COVID-19- themed lures,**
- **Registration of new domain names containing wording related to coronavirus or COVID-19, and**
- **Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure like ours.**

With an increased number of us working from home, now more than ever is the moment to focus on cybersecurity, both individually and corporately.

Cybersecurity and COVID-19

As the corona virus pandemic continues to disrupt global health, economic, political and social systems, there's another unseen threat rising in the digital space: the risk of cyber-attacks that prey on our increased reliance on digital tools and the uncertainty of the crisis.

Here are three reasons robust cybersecurity measures matter more than ever.

1. **A heightened dependency on digital infrastructure raises the cost of failure.**
2. **Cybercrime exploits fear and uncertainty.**
3. **More time online could lead to riskier behavior.**

So what can we do?

Just as addressing the COVID-19 pandemic requires changing our social habits and routines to impede infection rates, a change in our online behaviour can help maintain high levels of cybersecurity.

1. **Step up your cyber hygiene standards.**
2. **Be extra vigilant on verification**
3. **Follow official updates.**

Cybersecurity and COVID-19

Step up your cyber hygiene standards.

In addition to washing your hands after every physical contact to prevent the spread of COVID-19 and using an appropriate alcohol-based cleaning solution on your phone, keyboard, game controllers and remote controls, take the time to review your digital hygiene habits.

- Check that you have a long, complex router password for your home Wi-Fi and that system firewalls are active on your router.
- Ensure you're not reusing passwords across the web (a password manager is a great investment)
- Invest in/strengthen your Spam Filters
- Use a reliable VPN for internet access wherever possible.

Be extra vigilant on verification

Digital viruses spread much like physical ones; your potential mistakes online could very well contaminate others in your organization, an address book or the wider community.

- Ensure the programs or apps you install are the original versions from a trusted source.
- Be far more careful than usual when installing software and giving out any personal information.
- Don't click on links from email – be very wary of phishing attacks
- Consider implementing 2FA (2 Factor authentication) on your systems
- When signing up to new services, verify the source of every URL

Follow official updates.

- Pay attention to only trusted sources of data on the spread and impact of COVID-19
- Be sure to update your system software and applications regularly to patch any weaknesses that may be exploited.

Step up your cyber hygiene Standards

APRIL 2020 | ISSUE 4

The increased prevalence of remote working due to COVID-19 by individuals and businesses including MTN has seen a parallel lift in cyber attacks. Now more than ever, it is important to

Step up your cyber hygiene standards

In addition to washing your hands after every physical contact to prevent the spread of COVID-19 and using an appropriate alcohol-based cleaning solution on your phone, keyboard and mouse, ensure you are practicing below digital hygiene habits.

- Ensure that all provided laptops have up to date anti-virus definitions and software updates.
- Be reminded to use strong passwords and under NO circumstance should you share your passwords.
- Be wary of unsolicited emails offering information supplies, or treatment for COVID-19 or requesting MTN or your personal information for medical purposes.
- Do not click on links or open email attachments from unknown or unverified sources. Doing so could download a malware onto your computer or device.
- Visit below recommended sites for updated information on COVID-19
  - "https://ghanahealthservice.org/covid19"
  - "https://www.who.int/emergencies/diseases/novel-coronavirus-2019"
- Report any suspected compromise immediately to your line manager or itsecurity.GH@mtn.com
- Lastly, remain VIGILANT and be on the ALERT always to avoid falling victim to any attack.

Connect With Us

itsecurity.GH@mtn.com

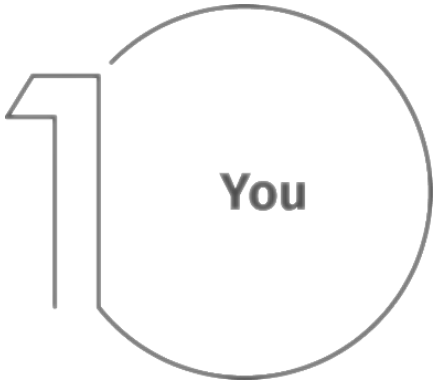
MTN

Working From Home Factsheet

Working from home may be new to some of you, perhaps overwhelming as you adjust to your new environment.

Here are five simple guidelines to help you work securely from home. The best part is all of these steps not only help secure your work, but they will make you and your family far safer as you create a cybersecure home.

Working From Home Factsheet



First and foremost, technology alone cannot fully protect you – you are the best defense.

Attackers have learned that the easiest way to get what they want is to target you, rather than your computer or other devices. If they want your password, work data or control of your computer, they'll attempt to trick you into giving it to them, often by creating a sense of urgency.

- **Ultimately the best defense against these attacks is you.**

Almost every home network starts with a wireless (often called Wi-Fi) network. This is what enables all of your devices to connect to the Internet. Securing your wireless network is a key part of protecting your home. Recommended steps to secure your Wi-Fi

- **Change the default administrator password:**
- **Allow only people that you trust to connect: Do this by enabling strong security** "password" **so that only people you trust can connect to your wireless network.**
- **Make passwords strong: The passwords people use to connect to your wireless network must be strong and different from the administrator password.**

Working From Home Factsheet

When a site asks you to create a password: create a strong password, the more characters it has, the stronger it is. Using a passphrase is one of the simplest ways to ensure that you have a strong password. Can't remember all those passphrases?

- **Use a password manager**
- **Finally, enable two-step verification (also called two-factor or multi-factor authentication) whenever possible.**

Make sure each of your computers, mobile devices, programs and apps are running the latest version of its software.

- **To stay current, simply enable automatic updating whenever possible.**
- **This rule applies to almost any technology connected to a network, including not only your work devices but Internet-connected TV's, baby monitors, security cameras, home routers, gaming consoles and more.**

Something you most likely don't have to worry about at the office is children, guests or other family members using your work laptop or other work devices.

- **Make sure family and friends understand they cannot use your work devices, as they can accidentally erase or modify information, or, perhaps even worse, accidentally infect the device.**

Security Myths Debunked…

Information security has its own set of misconceptions as well. Here are five.

Myth 1:

“Information security is just an IT issue."

Earmarking information security threats as something for IT is one of the best ways to help those threats proliferate. It’s important to remember that information security cuts across departments and is the same regardless of the IT implementation or vertical. Once information is digitized, everything from accuracy, privacy and availability to integrity needs to be protected. It is everyone's personal responsibility to practice safe computing and to protect not only your personal information but the organization's information as well

Myth 2:

“I have a MAC computer, they don't get viruses."

Most Malware and viruses are created to attack PCs with Windows Operating systems but that does not mean that the Mac OS is completely invincible. Mac users still have to be wary of malware that relies on the user falling for a cyber-trap. For example, a Mac user can be fooled into downloading malware disguised as an antivirus program. The best defense for Mac users against malware is to keep your operating system up-to-date.

Security Myths Debunked Cont'd…

Myth 3:

"Nobody wants to hack me! I'm not anybody important."

Thinking that it can't happen to you and acting on that falsehood is what leads to falling victim to cyber-crimes. Anyone connected to the internet is at risk of being hacked or falling into a cyber-trap.

Myth 4:

"My phone is safer than my computer or laptop because it can't get hacked!"

Most of the cyber security breaches you hear about involve computers but your smartphone needs protection too! They should be equipped with antivirus software that will help protect it from threats. In addition, you should always practice safe computing on your smartphone as you would on your computers!

Myth 5:

"My Antivirus software on my computer is enough to protect me."

Antivirus software is helpful and beneficial in containing the damage after a cyber-attack but it doesn't stop the attack from happening. A hackers job is to find ways around antivirus software and to go mostly undetected. Even with antivirus software installed, you still need to be careful and wary of your online activities.

Staying Safe Online

Here are our top eleven cyber security tips to help keep you safe online.

Stay Up to Date

- Don't ignore those important update notifications. Keep your operating system, anti-virus software, and other applications updated so you don't miss out on critical security enhancements.

Think Before You Click

- Be wary of strange links and email attachments. If you don’t know where the email is coming from, be extra wary before you open it.

Create Strong Passwords

- Choose long, complex passwords and change them often. Use different passwords for each account. Especially don't use your work-related password for other sites.

Be Camera Aware

- Cameras and devices can be accessed remotely or activated by apps. Cover the webcam on your computer/tablet when not in use.

Beware Open WI-FI Networks

- Only use secure networks when exchanging sensitive information i.e. Work-related information, bank and payment information, private/personal data, academic records, etc.

Secure your Social Network

- Strengthen your social network privacy and safety settings to keep prying eyes out of your private life.

Staying Safe Online Cont’d

Keep a "Clean" Machine

- Unknown programs, downloaded from the internet can open security vulnerabilities on your computer. Keep your machine clean and only use your organization’s approved and licensed software. If you absolutely need something else, check with your IT department first. Remember free software is not always free. Sometimes free software comes bundled with dangerous malware.

When in Doubt, Throw it Out

- Do not open suspicious links in email, tweets, posts, online ads, messages or attachments even if you know the source. You didn't win the Cayman Islands lottery and you are not the only person that can help that poor Nigerian prince. If that email seems too good to be true, it is. Don't respond to shady email solicitations!

Stay Watchful and Speak Up

- Keep an eye out and say something if you notice strange happenings on your computer or if you receive strange emails or password solicitations. If you see something, say something. You can report any security incident to your manager or Information Security department.

Get Two Steps Ahead

- Turn on two-step authentication – aka multi-factor authentication on your accounts where it is available. Available with some online services, two-factor authentication can use anything from a text message to your fingerprint to provide enhanced security to your online accounts.

And finally, If You Collect It, Protect It.

- Follow reasonable security measures to protect corporate or individuals’ personal information from inappropriate and unauthorized access. And while we don’t recommend it, if you must use a USB drive, encrypt it. If you are responsible for private information, keep it private!

THANK YOU

#WeDey4U #FightCoronaTogether

bernard.acquah@mtn.com

Questions

COVID-19 Prevention Alerts - #LetsFightCovid19Together

Tip 1

- Avoid touching your face, eyes, nose and mouth with your hands as much as possible.

Tip 2

- Wash your hands regularly with soap under running water or use alcohol-based hand rub.

Tip 3

- Social distancing is a must. Make sure you are 2 meters away from people around you to protect yourself and the people around you.

Tip 4

- Avoid close contact with anyone with cold and flu-like symptoms. Stay at least 2 meters away.

Tip 5

- Stay home when sick. If you have a fever, cough and difficulty breathing, seek medical attention and call in advance.

Tip 6

- If coughing or sneezing, cover nose and mouth with flexed elbow or paper tissue, dispose of tissue immediately after use and perform hand hygiene.

Tip 7

- Wear protective facemask if you have to go out. This will protect you and the people around you from the possible spread and infection of COVID-19.

Tip 8

- Stay informed on the developments about COVID-19 from authentic sources. Follow advice given by the national and local public health authority and your employer on how to protect yourself and others from COVID-19.