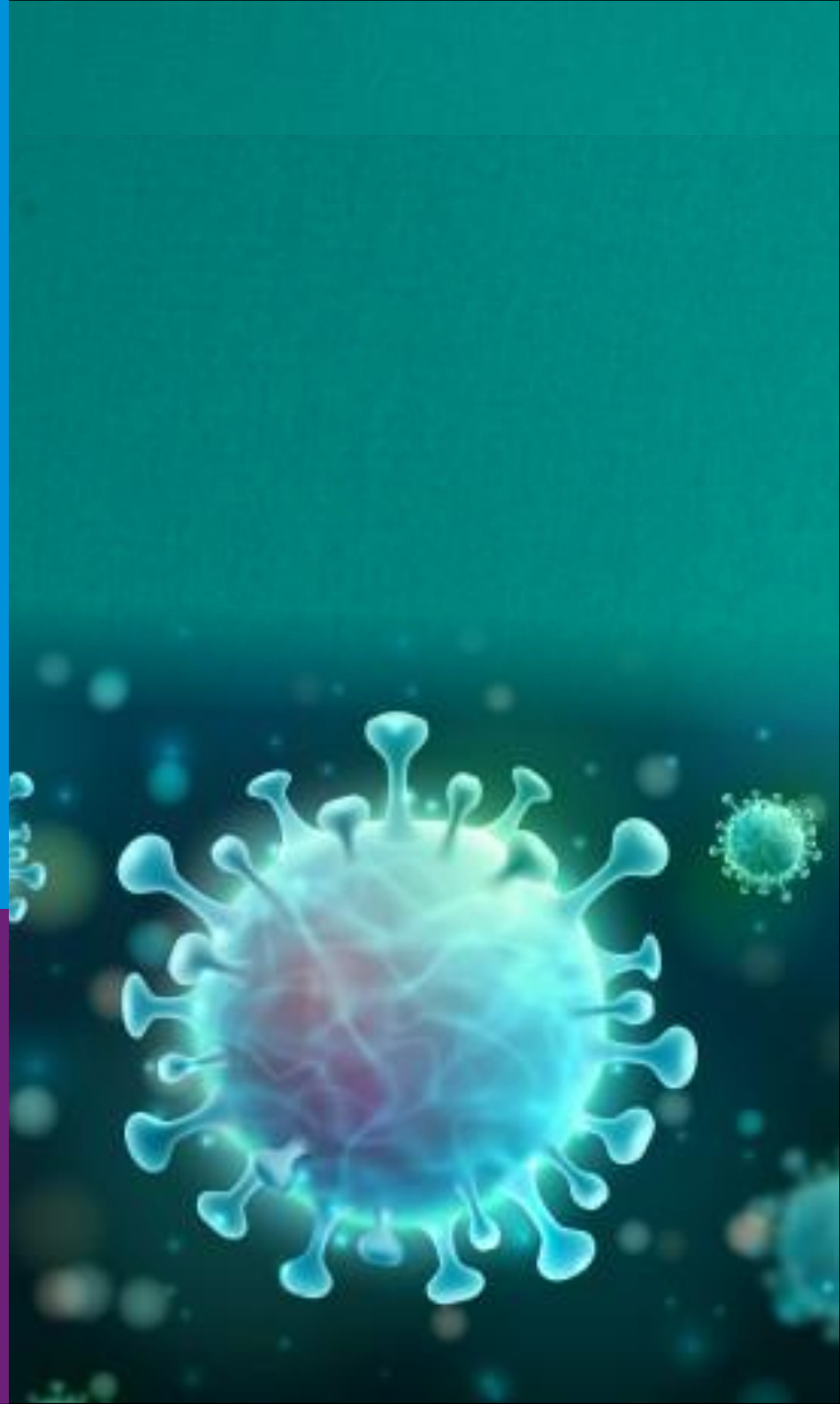
KPMG

Covid-19 : Cyber security implications for business

French Chamber of Commerce

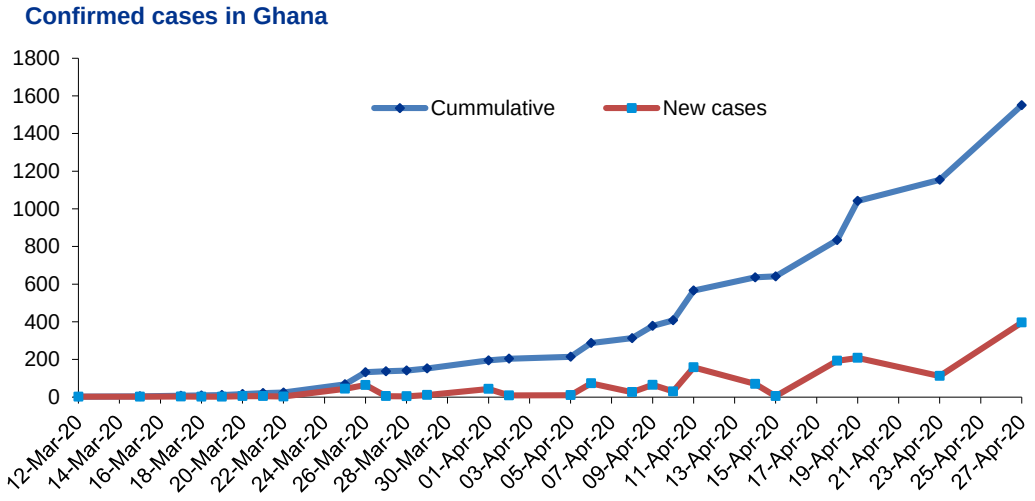
April 2020



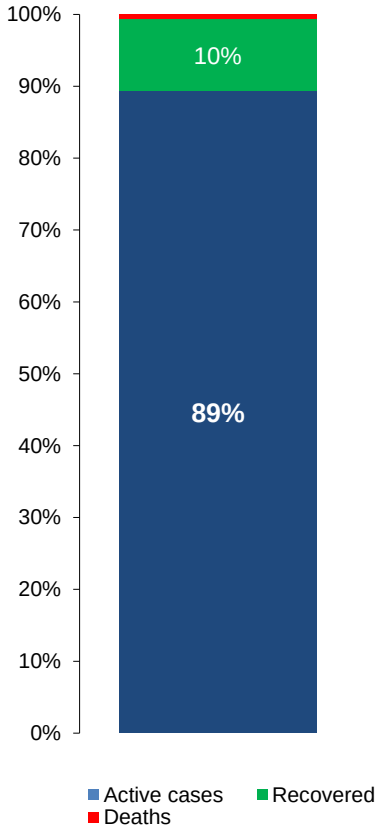
COVID-19 - Background & introduction

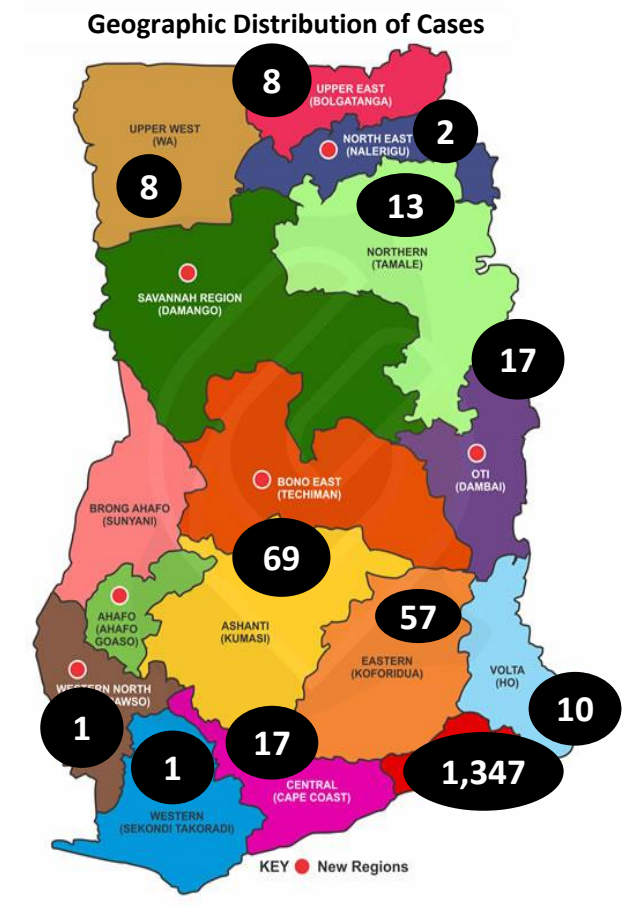
The World Health Organisation (WHO) on 11 March 2020 declared the novel corona virus (COVID-19) outbreak a global pandemic. Many countries globally have put in measures to control the spread of the virus. The President of Ghana announced some measures to curb the spread of the virus. Among these measures include the partial lockdown of some areas in the country as well as the closure of the borders into Ghana.

Ghana has recorded 1,550 cases with a 10% recovery rate and 1% death rate



- WHO classified Ghana among 13 **Priority 1** countries to be at risk due to its international passenger volume.
- Most parts of the Greater Accra and Ashanti regions were placed under a 21-day partial lockdown which was lifted on the 20 April 2020.





COVID-19 - Cyber security implications for businesses

The speed and breadth of the unfolding COVID-19 crisis is dramatically impacting lives, disrupting business operations and supply chains, slowing markets, and now posing the risk of a global recession. Concern over the spread, duration, scale and impact of COVID-19 pandemic is growing, prompting organizations to consider their response and the actions they need to take now to maintain their business.

Organizations are evaluating various deployment models based on the complexity, criticality and scale of remote working

Laptop to Home

Enable employees to work remotely with the organization's allocated laptop

Desktop to Home

Enable employees to work remotely by moving the organization's allocated desktop to home

BYOD with employer's secure container

Enable employees to work remotely using their personal device by ensuring organization's data remain safe and contained within the work profile on the device

Cloud VDI environment

- VDI set up and system provided by the organization to enable employees to access employer's data and applications
- Organizations set up VDI on temporary cloud environment and enable employees to login from their personal devices to access employer's data and applications

Teleworking

Enables employees to work remotely using modern technology and telecommunication to remain in touch with employer and the business (clients/customers)

COVID-19 - Cyber security implications for businesses

The COVID-19 pandemic is changing our lives, people are concerned, and with that concern comes a desire for information, safety and support. Organised crime groups are exploiting the fear, uncertainty and doubt which COVID-19 brings to target individuals and businesses in a variety of ways. There are also a number of cyber risks associated with the measures various organisations are putting in place to combat COVID-19 and continue business operations.

Business Disruption:

Increase in Covid -19 themed malware and spam campaigns:

- ✓ Health updates
- ✓ Fake cures
- ✓ Ghana Covid-19 case updates

- ❖ Denial of Service Attacks
- ❖ Ransomware Attacks

Fraud:

Covid-19 themed phishing campaigns to collect customer banking details, credentials of critical systems such as Microsoft Office 365 through:

- ✓ Fake websites
- ✓ Impersonation of Bank staff and customers
- ✓ Increase in CEO and CFO fraud
- ✓ Soliciting donations for non-existent COVID-19 charities using malicious online platforms

Critical Data Breach:

Loss of sensitive business and personal data:

- ✓ Ad-hoc remote working arrangements
- ✓ Use of personal devices with limited or no security protection
- ✓ Inadequate staff awareness
- ✓ Teleconferencing

COVID-19 - The threat is real

ZDNet

VIDEOS WINDOWS 10 5G IOT CLOUD AI SECURITY MORE

MUST READ: Developer jobs: Six tech roles companies want to fill despite the coronavirus lockdown

FBI says cybercrime reports quadrupled during COVID-19 pandemic

FBI official says foreign hackers targeted COVID-19 research centers.

MAGAZINE ABOUT US NEWS GET FEATURED VIDEOS MASTERCLASS ADVERTISE WITH US CISO MAG Events

NEWS THREATS

Hackers Attack Around 300,000 Devices in South Africa Amid COVID-19 Crisis

By CISOMAG - April 3, 2020 293 0

SHARE Facebook Twitter

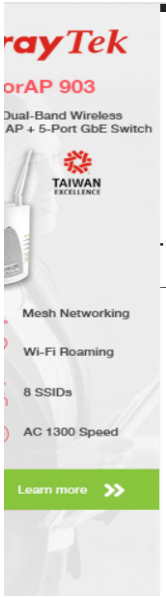
FOLLOW US FOR MORE UPDATES

Follow 14,083 CISO MAG Like Page

Follow @CISOMAG 985 followers

businesstech.co.za/news/banking/373900/nedbank-warns-clients-after-data-breach-1-7-million-clients-potentially-affected/

wn - Google Sea...



SAFETY FIRST. THEN INNOVATION. Speak to an Expert cisco Partner

Your email address Subscribe

BUSINESSTECH

BANKING BUSINESS FINANCE MOTORING INDUSTRY NEWS IT SERVICES MC

Nedbank warns clients after data breach – 1.7 million clients potentially affected

Staff Writer 13 February 2020

theguardian.com/world/2020/apr/04/fraudsters-exploiting-covid-19-fears-have-scammed-16m

Coronavirus outbreak

Fraudsters exploiting Covid-19 fears have scammed £1.6m

Criminals are escalating activity that targets the vulnerable, analysts have said

- Coronavirus – latest updates
- See all our coronavirus coverage

Mark Townsend *Home affairs editor*

@townsendmark

Sat 4 Apr 2020 17.29 BST

449

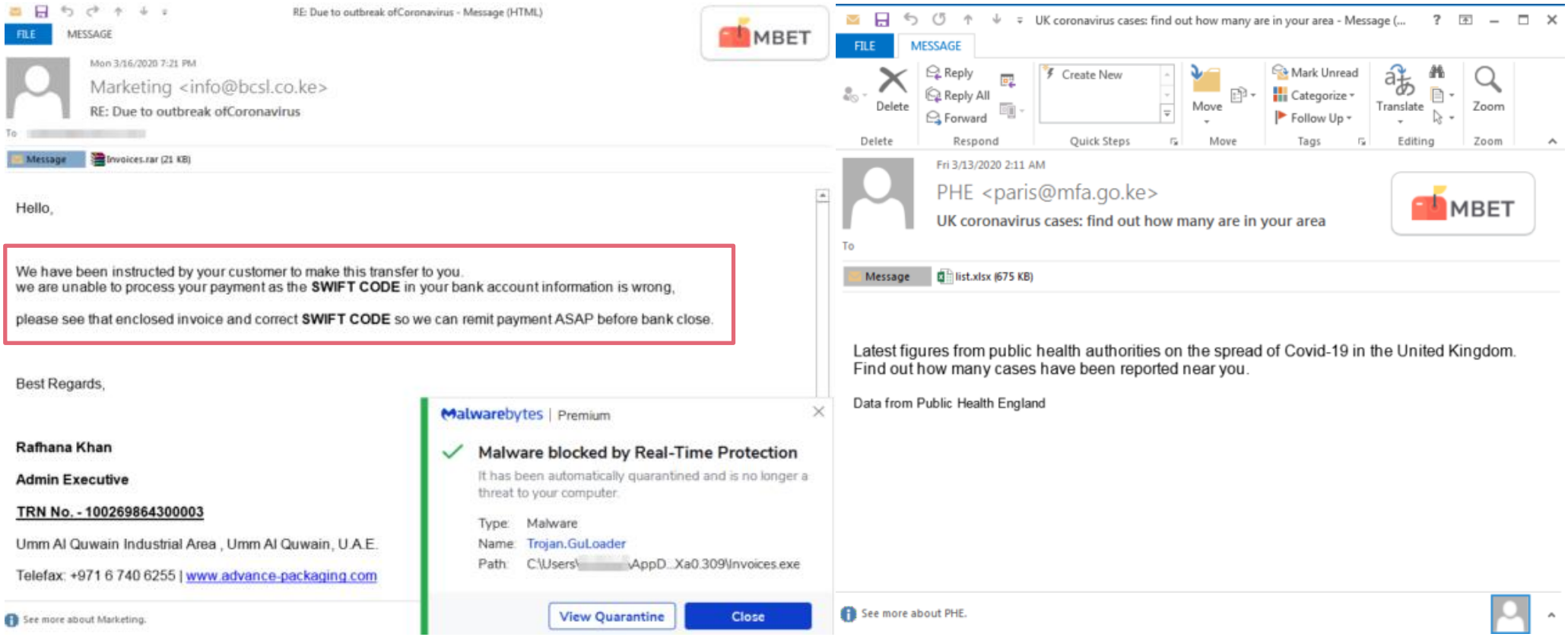
▲ The coronavirus crisis is providing fresh opportunities for fraudsters to strike. Photograph: Dominic Lipinski/PA

More than 500 coronavirus-related scams and over 2,000 phishing attempts by criminals seeking to exploit fears over the pandemic have been reported to UK investigators, figures reveal.

One of the latest scams being assessed by officials at the National Fraud

COVID-19 - The threat is real

Sample malicious emails



COVID-19 - Cyber crime facts and figures

01 FBI Report

3000 - 4000

complaints a day through their internet portal. Prior to the COVID outbreak, they typically receive 1,000 complaints a day

02 Forrester Research

600% increase in COVID -19 phishing attacks in the first quarter of 2020

1.8 million

daily COVID-19 specific phishing and malware attacks for the week ending 17 April 2020

03 US Federal Trade Commission (FTC)

$18 million

reported losses through COVID-19 related complaints

As at 21 April 2020, (FTC) had received 23,581 consumer complaints related to the outbreak, including more than 12,700 fraud complaints

04 Australian Competition and Consumer Commission (ACCC)

$130,000

in reported losses from over 1,100 reports about COVID-19 scams.

05 Travelex

$2.3 million

reported to have been paid out of an amount of

$6 million (£4.6 million)

demanded by ransomware operators.

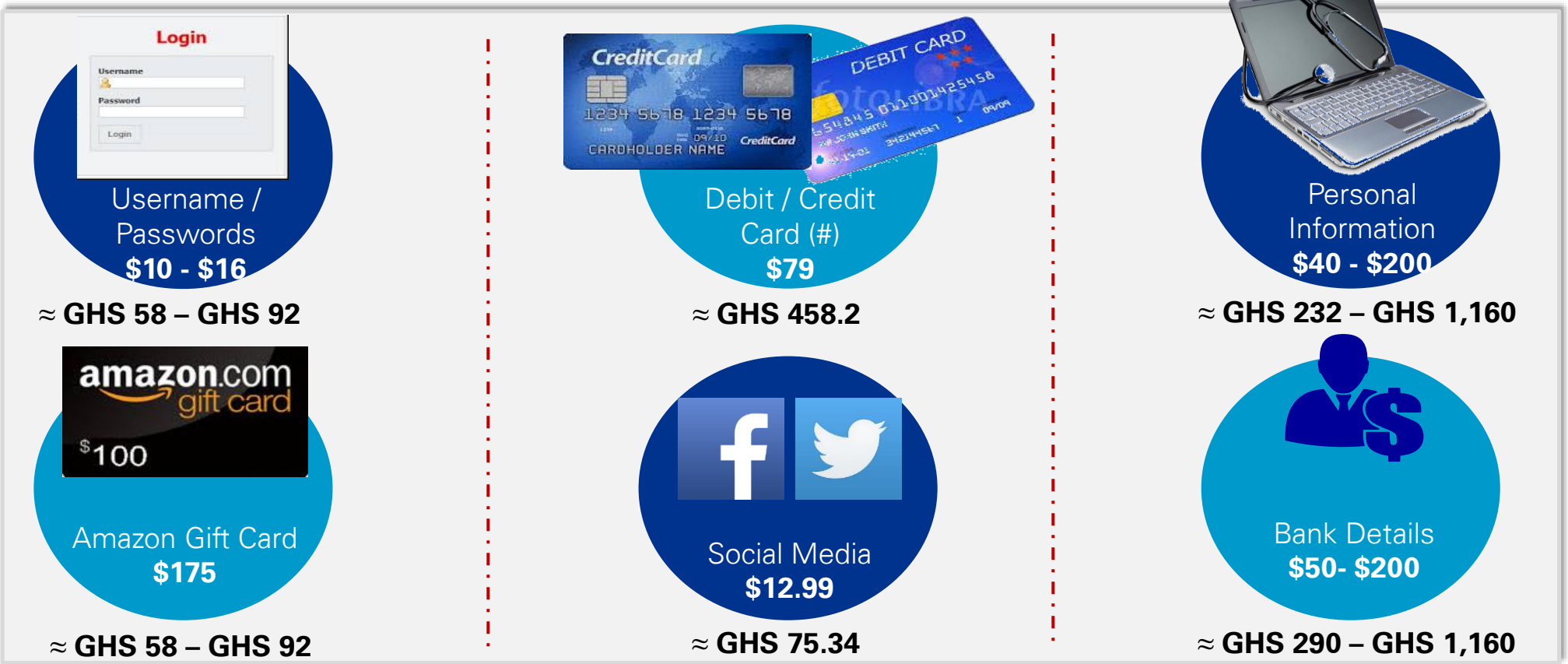
06 Garda National Economic Crime Bureau

€2.38 million

paid by a German company for the purchase of Personal Protective Equipment to a Fraudulent company.

COVID-19 - Cyber crime facts and figures

Information is very lucrative for hackers and scammers on the Dark Web. The prices (USD/GHS) of stolen data on the dark web are estimated as follows:



A database containing what appears to be the data of thousands of UniCredit S.p.A employees is being advertised for sale on cybercrime forums. Buyers can purchase the data for sale in units of rows. The cost of 150,000 rows of data is $10,000.

References:
https://digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ ; https://fortune.com/2018/03/07/apple-id-dark-web-cost/ ; https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

COVID-19 - Staying cyber secure

The Response

A simple request: Remain vigilant for malicious phishing emails seeking to exploit interest in the Coronavirus. Please exercise caution in handling any unofficial email with a subject line, attachments, or hyperlinks related to the Coronavirus, even if it appears to originate from a trusted source. Be wary of fraudulent social media pleas, calls, texts, or donation websites relating to the COVID-19. **Even these need to be Socially Distanced!!**

Below are some key steps you should take to reduce the risk to your organisation and your employees, particularly as you move to remote working:

1. Enhance cyber and information security awareness amongst your teams, warning them of the heightened risk of COVID-19 themed phishing attacks

2. Review the organisation's Risk Assessment and Business Impact Analysis (BIA) to confirm the critical business processes, sites, products, services, and a prioritised list of clients that will be the focus of continued operations during the pandemic

3. Share definitive sources of advice on how to stay safe and provide regular communications on the approach your organisation is taking to the COVID-19 pandemic

4. Access to the corporate network from the internet should be restricted via secure channels such as a Virtual Private Network (VPN)

5. Review access rights of employees and third parties to ensure access granted is on a business need basis.

COVID-19 - Staying cyber secure

6	Ensure increased monitoring of cybersecurity events and avoid the use of non-secure/public cloud channels for information transfer	
7	Back up all critical systems and validate the integrity of backups, ideally arranging for offline storage of backups regularly.	
8	Encrypt data at rest and in motion on laptops and storage media used for corporate activities	
9	Ensure finance processes require finance teams to confirm any requests for large payments during the COVID-19 pandemic. This confirmation can help to guard against the increased risk of business email compromise and CEO frauds. Ideally, use a different channel such as phoning or texting to confirm an email request.	
10	Improve vulnerability awareness and patch management process across your IT estate by applying the latest critical security patches and updating anti-malware software including on devices used to access corporate information.	
11	Run a helpline or online chat line which employees can easily access for advice, or to report any security concerns including potential phishing attacks	

Questions & Comments

Thank You

Contact Us

Andrew Akoto
Partner, Risk Consulting
Mobile: +233208174629
E-mail: aakoto@kpmg.com

Prince Yawson-Adjei
Manager, IT Advisory
Mobile: +233501324198
E-mail: pyawson-adjei@kpmg.com

Sam Aluko
Associate Director, IT Advisory
Mobile: +233501324121
E-mail: samuelaluko@kpmg.com