

# Keeping Cyber Safe

---

Process, People and Technology

## New programme against COVID-19



<GOV UK Notify>

### The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund (rebate)* of 128.34 GBP.

[Access your funds now](#)

The funds can be used to protect yourself against COVID-19( <https://www.nhs.uk/conditions/coronavirus-covid-19/> precautionary measure against corona )

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

**Subject:** All Staffs: Mandatory Corona Update

**From:** "Covid-19" [REDACTED]

**Date:** 16/03/2020, 10:28

**To:** [REDACTED]

### Important Covid-19 Updates & Measures

Dear all,

Important company policies regarding the Covid-19 Virus has been uploaded to OneDrive. It is important you read the procedures to keep everyone safe.

[Login here to action read](#)

Sincerely,

Admin



Re:SAFTY CORONA VIRUS AWARENESS WHO



World Health Organization



Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

[Safety measures](#)

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong  
Specialist wuhan-virus-advisory

**FAKE**



## Alert (AA20-099A)

[More Alerts](#)

### COVID-19 Exploited by Malicious Cyber Actors

Original release date: April 08, 2020

#### Summary

This is a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC).

This alert provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails. This alert provides an overview of COVID-19-related malicious cyber activity and offers practical advice that individuals and organizations can follow to reduce the risk of being impacted. The IOCs provided within the accompanying .csv and .stix files of this alert are based on analysis from CISA, NCSC, and industry.

**Note:** this is a fast-moving situation and this alert does not seek to catalogue all COVID-19-related malicious cyber activity. Individuals and organizations should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves.

# Key Themes & Points

---

- COVID-19 is now perhaps the biggest topic theme used by cyber criminals to launch attacks
- Phishing/Smishing/Vishing are just a launch mechanism, that needs some form of interaction for the next phase of attack
- Remote workers are not only isolated from team members, but also from internal security controls and best practices
- Internal policies and processes not written to deal with the complexities of remote working
- Personal IT and infrastructure used to support remote working

# Smishing Demo

---

# Phishing Demo

---

# What does the Attacker want?

---

- Your credentials
  - Username
  - Password
  - Bank account
  - Personal data
- Access to your Computer
  - Ransomware
  - BOTNET
  - Keyloggers
  - To simply take control and allow access to others

# What Can you Do?

- Process
- People
- Technology



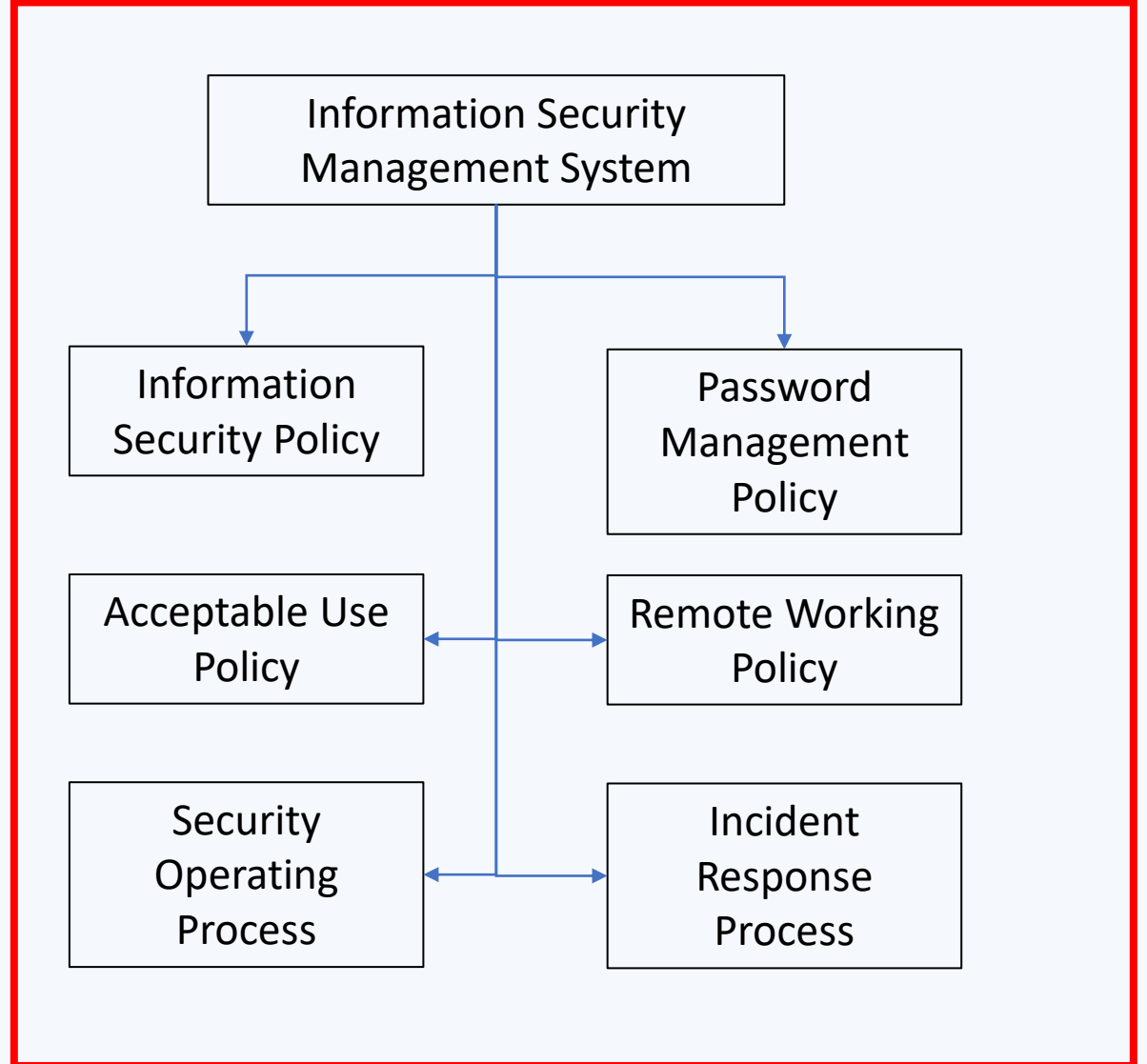
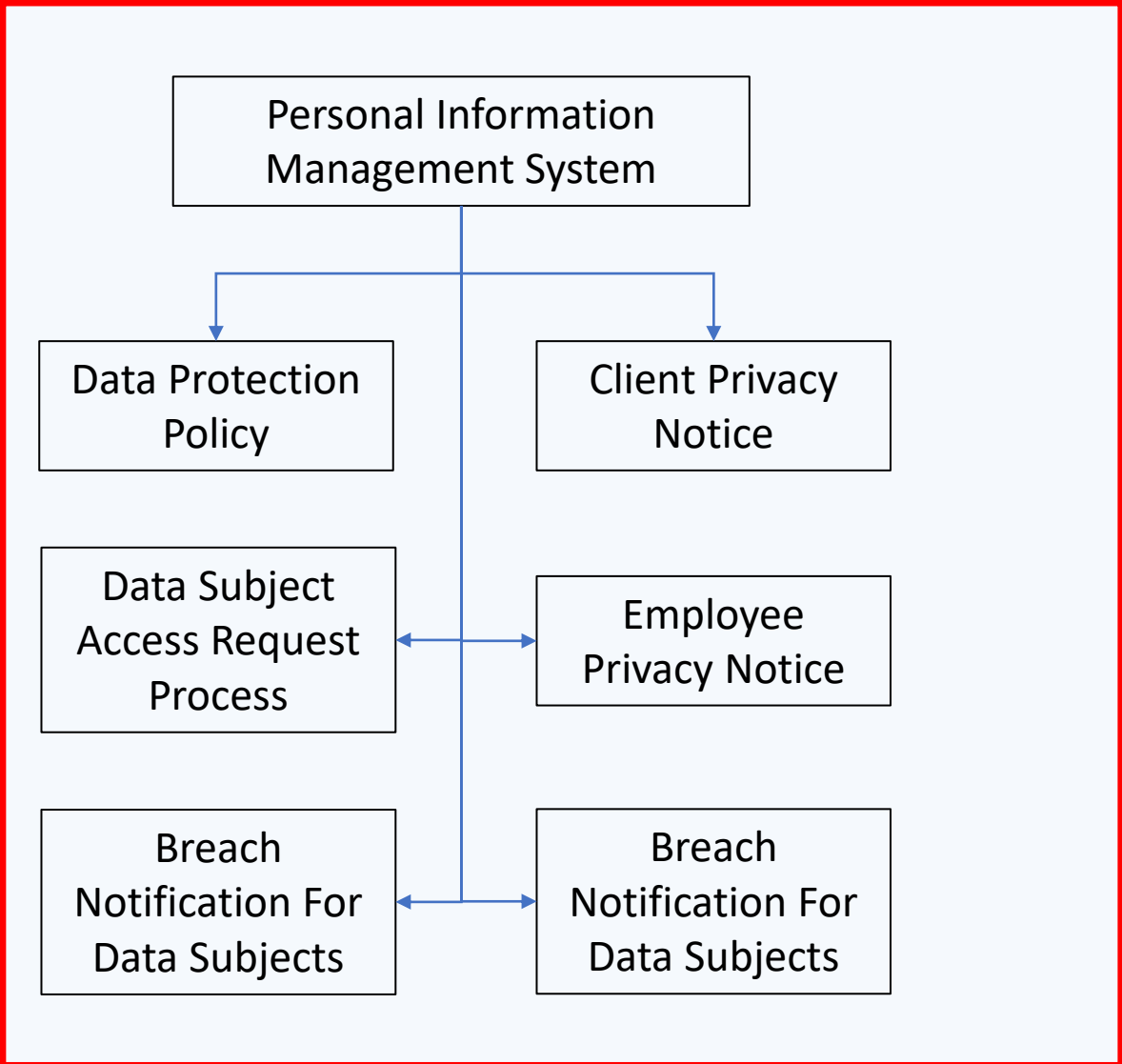




# Processes

What do we need in Place?

# Privacy Control Framework

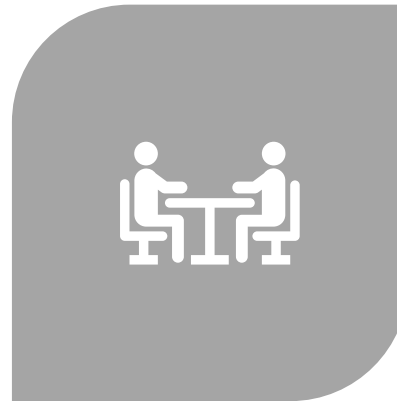


# Need to Adapt our Processes

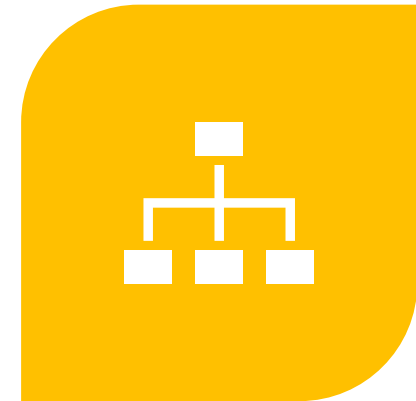
---



REMOTE AND FLEXIBLE WORKING  
WILL BE THE NEW NORMAL



REVIEW AND REWRITE AND  
ENSURE EVERYONE READS AND  
UNDERSTANDS



FOCUS ON HOW TO SUPPORT THE  
INDIVIDUAL AS WELL AS THE  
ORGANISATION

# Remote Working

---

- IT Infrastructure
  - Routers
  - Access and segregation
  - Location
  - Other devices
  - Protection
- Access Control
  - Local network
  - Passwords

# Incident Response

---

- Who do I report an incident to?
  - Email and phone number
  - Line Manager
- What to report?
  - Any suspected data breach
  - Any potential breach of credentials
  - Suspect material, websites, emails



People

Keeping us Safe

# Training and Testing

---

- Training through:
  - eLearning
  - Webinars
  - Discussions like today
- Exercises
  - Phishing campaigns
  - Virtual BCP and Incident Response

# Cyber User Awareness Training - Basic

Course Menu

EXIT

▶ Course Instructions

Introduction

What is Cyber?

The Cyber Threat

Password Management

Digital Footprints

Staying Safe at Work and at Home

Course Summary

Test your Knowledge

Learning Objectives

The Outsider Threat

Hackers & Hacktivists

Nation State

Industrial Competitors

Organised Crime

The Outsider Threat - Quick Quiz

The Insider Threat

Motivations

The Ultimate Insider Threat

Key:  Not started  Started  Completed

ZOOM

EDIT



## The Internet of Things

The Internet of Things or IoT is not a new concept or definition. It is about connecting devices over the Internet, and then letting them talk to us, applications, and each other.

A recent example is home heating: we now have the ability to control the temperature in our homes using our Internet-connected phones and tablets.

The IoT is not just limited to our homes - it extends into 'smart cities', where we have integrated traffic and energy systems.

It is estimated that **by the end of 2021, up to 25 billion devices will be connected to the Internet.** Click below to see what could be connected by 2021.

The IoT by 2021?

- Cars
- Aircraft system
- Electricity distribution
- Whole cities
- You and Me?



Although the IoT will give us great flexibility and access both now and even more so in the future, it will also give the **cyber attacker more targets to attack.**



## The Outsider Threat

There are many different types of outsider cyber threats. One of these is the Nation State Actor.



Which of these countries can be classed as a major cyber Nation State?

Iceland

Russia

Canada

Oman





# Technology

Vital for the cyber defence

# Ransomware Demo

---

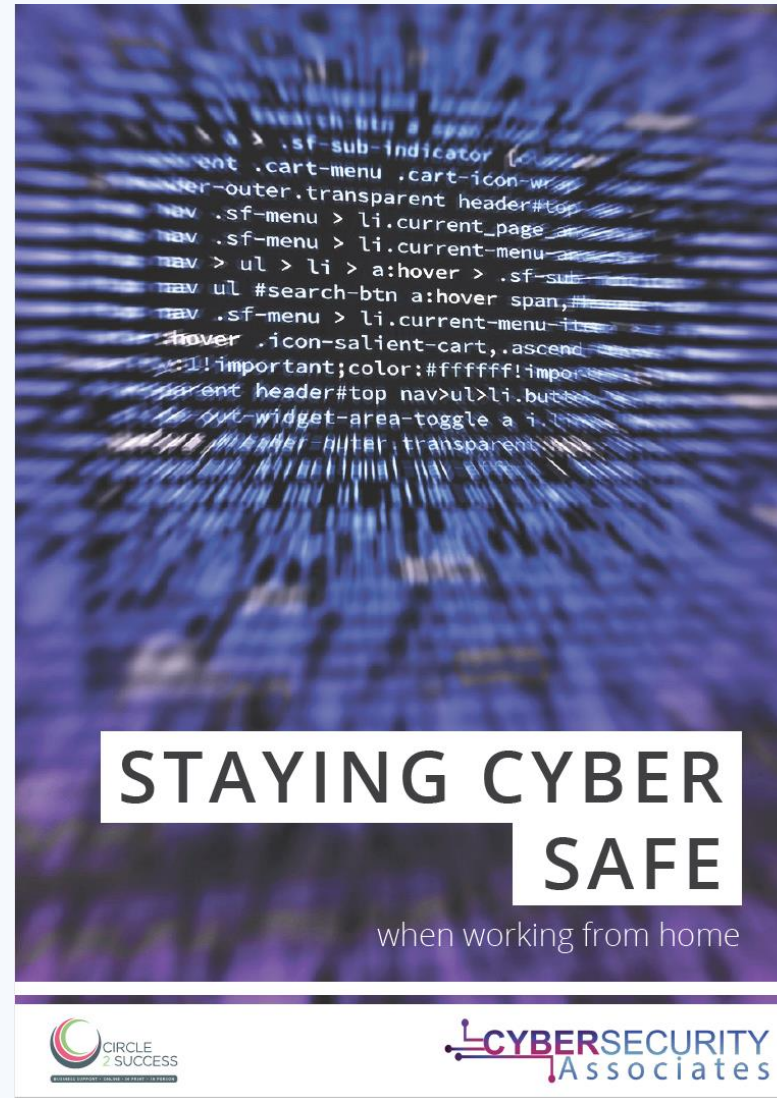
## In Summary

---

- Cyber security more in focus with remote working
- More focus on the individual
- Processes need to be reviewed and adapted
- People should be armed and trained against the cyber threat
- No reason why home IT cannot be upgraded to a excellent level of security


# Download Our Free Guide


---

The cover of a guide titled "STAYING CYBER SAFE" with the subtitle "when working from home". The background is a dark blue, abstract, digital-style pattern with glowing lines and a central perspective effect. The title is in large, bold, white, sans-serif font. The subtitle is in a smaller, white, sans-serif font. At the bottom left is the "CIRCLE OF SUCCESS" logo, and at the bottom right is the "CYBERSECURITY Associates" logo.

**STAYING CYBER  
SAFE**

when working from home

 CIRCLE OF SUCCESS

 CYBERSECURITY Associates