



## Building resilience to cyber threats

### What is Phishing?

Phishing is a disguised email, that aims to hook the recipient into clicking a link or attachment that enables a cyber-attack to take place.

### Why have Phishing attacks increased since Covid-19?

In late March 2020, the Telegraph reported that phishing “attacks have increased 667pc since the end of February” There are two main reasons for this increase:

1. Attackers like to masquerade as a trusted entity and a pandemic provides the perfect opportunity for impersonation.
2. The move to remote working makes employees more vulnerable to cyber attack, from both a technical and behavioural perspective.

### What are the known Covid-19 phishing scams?

On the 4<sup>th</sup> April. The Guardian reported that “ The number of coronavirus-themed phishing attempts stands at 2,192”, and although it would be impossible to cover even a proportion of these, it is worth highlighting some of the more ‘convincing’ phishing scams:

#### Workplace policy

Cyber criminals are known to have been impersonating HR and IT departments, with emails such as the one below:

All,

Due to the coronavirus outbreak, [[company\_name]] is actively taking safety precautions by instituting a [Communicable Disease Management Policy](#). This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before [[current\_date\_1]].

If you have any questions or concerns regarding the policy, please contact [[company\_name]] Human Resources.

Regards,  
Human Resources

## HMRC

Cyber criminals are masquerading as HMRC via email and SMS. An example of a phishing email is detailed below. For further information, visit the [dedicated HMRC page](#).

— Forwarded message —  
From: GOV.UK Notify <danielnhs@pinkcontract.com>  
To: "  
Sent: Friday, 6 March 2020, 09:20:50 GMT  
Subject: UK Updates on COVID-19



**GOV.UK**

**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.

**From Government Gateway**

**This is an automatic email - please don't reply.**

## World Health Organisation (WHO)

WHO, the primary provider of Covid-19 information, has issued a stark warning “Beware of criminals pretending to be WHO”. An example phishing email is detailed below, with detailed advice and guidance from WHO on their [dedicated page](#).



Latest on corona-virus - Message (HTML)

File Message Tell me what you want to do...

World Health Organization: WHO <...> Latest on corona-virus

This message was sent with High importance.

MyHealth-Ebook.zip 22 KB



**World Health Organization**

**Corona-virus updates**

Concerning Corona-virus disease (COVID-19) outbreak, the World Health Organization brings you the Corona-virus E-Book and Guide.

Inside this E-Book (**My-health**), you shall find out the complete research/origin of corona-virus and the recommended guide to follow to protect yourself and others.

**Guidance to protect children and business centre;**

This guidance provides critical considerations and practical checklists to keep Kids and business centre safe. It also advises national and local authorities on how to adapt and implement emergency plans for educational facilities.

Health advice

Emails purportedly from medical experts in China, claiming to help protect against Covid-19 have also been circulating:



**WMR - Here to support you during Covid-19**

As we move to new ways of working, our organisations become more vulnerable to cyber attack. Offering a range of remote services, we can help you build resilience to evolving cyber threats.

**CYBER SECURITY EXPERTISE**

We have a long history and understanding of the threat environment. Working in the field of cyber and information security since the late 1980's, we have real world experience of dealing with cyber threats.

**TRUSTED PROFESSIONALS**

Entrusted by government departments to deal with threats from nation states in highly sensitive environments. We are trusted professionals who understand the importance of confidentiality to you and your clients.

**COLLABORATIVE APPROACH**

We adopt a collaborative approach to working. Gaining an in-depth understanding of the challenges you face, ensures that you receive the most appropriate services for your organisation.



hello@wmr.co.uk



+44 (0)800 002 5730



Warner McCall Resilience



WMR\_Cyber



wmr.co.uk