ICAEW KNOW-HOW
TECH FACULTY
GUIDE: CORONAVIRUS (COVID-19)

MAINTAINING CYBER HYGIENE DURING CORONAVIRUS (COVID-19)

New
25 March 2020

This guide has been prepared by the ICAEW Tech Faculty. Recognised internationally for its thought leadership, the Faculty is responsible for ICAEW policy on issues relating to technology and the digital economy. The Faculty draws on expertise from the accountancy profession, the technology industry and other interested parties to respond to consultations from governments and international bodies. To connect with like-minded professionals within this community and, to gain access to the full suite of exclusive resources, visit icaew.com/techfac.

DISRUPTION BRINGS OPPORTUNITY

Unfortunately, criminals thrive in times of uncertainty and fear, and the UK's National Cyber Security Centre (NCSC) has already reported an increase in cyber threats which refer directly to the coronavirus. At the same time, many organisations have opened up new avenues for attack by suddenly moving all staff to home working. Staff may be using unfamiliar apps and controls may not be configured properly. Staff are also likely to be stressed and worried and may not think about cyber security.

This guide outlines the key steps to basic cyber hygiene and highlights some useful resources.

NEW THREATS TO LOOK OUT FOR

Coronavirus allows criminals to put a new spin on existing attacks. There have already been a number of new malicious websites set up for the purpose of infecting devices with malware. Be careful of newly created websites registered with the word 'corona', many of which could be suspicious. Watch out for sites with variants of Coronavirus(.)com or Corona-virus Map(.)com.

Spam emails try to grab your attention through offering goods that are now in high demand, such as masks, hand sanitizers or vitamins, for example. Alternatively, they might feed conspiracy theories about the pandemic.

Phishing scams can appear to come from organisations such as the CDC (Centers for Disease Control) or the WHO (World Health Organisation). The scammers have crafted emails that appear to come from these sources, but they actually contain malicious phishing links or dangerous attachments. There are also emails that claim to have a 'new' or 'updated' list of cases of Coronavirus in your area.

There has been a spike in fake internal HR or IT communication, such as coronavirus surveys impersonating your HR or IT department - the objective here is to steal usernames and passwords. For example, to access the 'document' or 'survey', the recipient has to provide their Office 365 credentials on a fake site, thereby compromising their account.

Cybercrime is also like to increase. Criminals may set up fake charities and send emails that ask for charity donations for studies, doctors, or victims that have been affected by the COVID -19 Coronavirus.

GET THE BASICS RIGHT

There are lots of simple guides to help small and medium sized organisations focus on the most important steps, including ICAEW's 10 steps to cyber security for smaller firms and the NCSC's Small Business Guide to Cyber Security.

Some of the key points to focus on at this point are:

- Keep software and anti-malware protection up-to-date and install patches as soon as they are made available. Anti-malware software should also be fully configured to integrate with email and web browsing. This helps to reduce vulnerability to attackers, as they often target unpatched systems. It also ensures that you have protection against the latest viruses.
- Have strong access control, including good password practices. Two factor authentication (2FA) is advised for important accounts or data, but following good practices around passwords is always essential. This includes having strong passwords or passphrases, changing default passwords and not reusing passwords. The longer the password, the better – using a password manager will enable passwords of 12 characters or more become the baseline length instead of just 8 characters.
- Back up your data and test your processes. This is critical to protect against ransomware attacks in particular, where data is encrypted by criminals who demand payment for unencrypting it. Do not rely solely on online backup services such as OneDrive of Google Drive.

WORKING FROM HOME

As this guide has highlighted, cyber criminals are targeting businesses and staff with new scams and phishing emails related to the coronavirus. Therefore, organisations should pay particular attention to home working practices to ensure that cyber risks are managed as far as possible. The NCSC has a guide to secure home working which includes a range of issues including:

- Developing a Bring your own device (BYOD) policy where staff are using personal rather than work devices
- The use of Virtual Private Networks (VPNs), which are the most secure way of connecting users remotely – these should be considered to add security when accessing the internet and cloud-based services
- Helping staff to look after devices and avoid the use of removable media
- Setting up new accounts securely.

In addition, ensure that staff have the resources they need to be able to operate securely - provide written guidance on any new software that staff are having to use, test that the software works as intended and produce a series of How Do I? guides for staff if needed

HELP USERS TO BE VIGILANT TO PHISHING EMAILS

Staff should be particularly vigilant at the moment when looking at emails and clicking on links. Phishing emails can be very convincing and professional-looking but there are some key things to look out for. NCSC guidance gives the following general tips around phishing emails, which you could share with your staff:

- Many phishing emails have poor grammar, punctuation and spelling.
- Is the design and overall quality what you'd expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.

- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to a secret part of the Internet.
- Your bank, or any other official source, should never ask you to supply personal information from an email.

It is also useful to hover over a link to see the actual hyperlink address that you are being directed to, not just the text in the email. Finally, if in any doubt, double check any claims made in the email, for example calling colleagues or banks to check whether they have sent the email in question.

PROTECTING SENSITIVE DATA

Businesses need to take additional steps to protect sensitive and personal data and working at home may change the way that data is handled. Established procedures may not be appropriate and therefore consideration should be given to sending out new guidance to staff who are handing such data at home. This could include:

- Not downloading any personal data onto non-work devices.
- Locking away documents containing personal data securely overnight.
- Not printing documents and/or emails containing personal data at home unless absolutely necessary.
- Shredding any documents containing personal data once you've finished with them. If staff do not have a shredder at home, they should be kept securely until the employee returns to work and can place them in the confidential waste bins (as appropriate).

The Information Commissioner's Office has published some FAQ related to Coronavirus if further information is needed.

USEFUL RESOURCES

The NCSC has a wealth of resources to help businesses of all sizes. As well as the Small Business Guide, they provide a free cyber security training course for staff that can be watched online. The NCSC also sends out a weekly threat report which highlights new or particular important threats or attacks.

ICAEW has a wide range of support for members on cyber which can be found at icaew.com/cyber. Free resources from the Tech Faculty include a short video giving an overview of the topic, as well as the 10 steps guide. We also have over twenty evergreen cyber security tips of the week on Tech News.

There are over 1.8m chartered accountants and students around the world − talented, ethical and committed professionals who use their expertise to ensure we have a successful and sustainable future.

Over 181,500 of these are ICAEW Chartered Accountants and students. We train, develop and support each one of them so that they have the knowledge and values to help build local and global economies that are sustainable, accountable and fair.

We've been at the heart of the accountancy profession since we were founded in 1880 to ensure trust in business. We share our knowledge and insight with governments, regulators and business leaders worldwide as we believe accountancy is a force for positive economic change across the world.

ICAEW is a founder member of Chartered Accountants Worldwide and the Global Accounting Alliance.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

T +44 (0)20 7920 8100
E generalenquiries@icaew.com