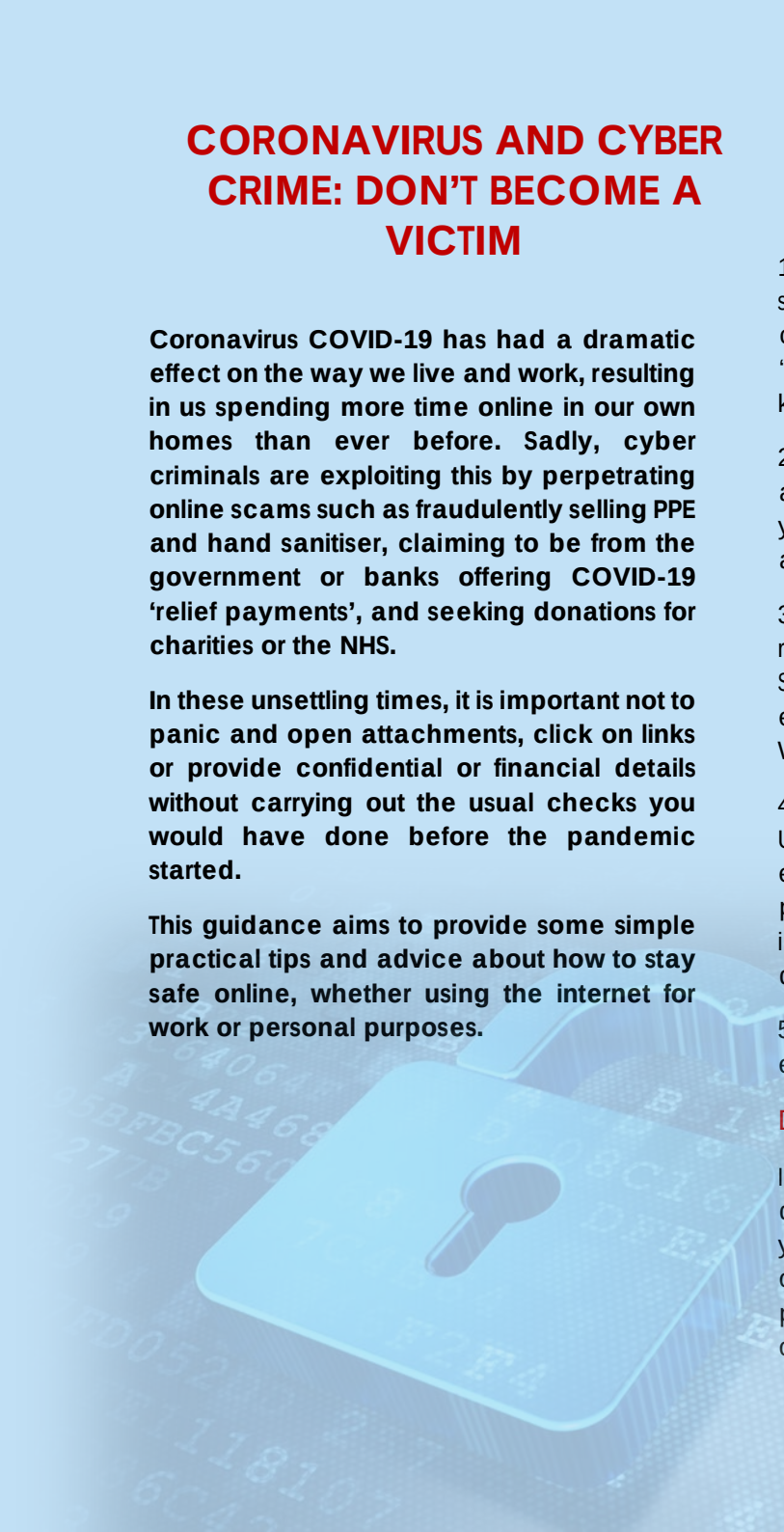
CORONAVIRUS AND CYBER CRIME: DON'T BECOME A VICTIM

Coronavirus COVID-19 has had a dramatic effect on the way we live and work, resulting in us spending more time online in our own homes than ever before. Sadly, cyber criminals are exploiting this by perpetrating online scams such as fraudulently selling PPE and hand sanitiser, claiming to be from the government or banks offering COVID-19 'relief payments', and seeking donations for charities or the NHS.

In these unsettling times, it is important not to panic and open attachments, click on links or provide confidential or financial details without carrying out the usual checks you would have done before the pandemic started.

This guidance aims to provide some simple practical tips and advice about how to stay safe online, whether using the internet for work or personal purposes.



Top 5 Tips for working securely online at home

1. Use strong passwords. The NCSC suggests three random words, including capitals, numbers and/or symbols, e.g. "Ta11officeme1on!". Passwords should be kept secure and updated every 6-12 months.

2. Install and update antivirus software and regularly test for viruses. Also ensure that your browser, operating system, and software are kept up to date.

3. Actively use your spam filter. If you receive an email that is Spam, mark it as Spam so that next time it is filtered. Check all emails in your Spam filter are Spam and Whitelist any legitimate contacts for next time.

4. Double-check before sending emails. Use bcc if recipients should not be aware of each other's contact details. Password-protect attachments containing sensitive information and send the password by a different means if possible (e.g. text).

5. Do not click on links embedded in emails and be aware of "phishing emails."

Don't forget paper records!

It is important that paper records are disposed of securely, ideally by shredding. If your paper recycling is easily accessible outside your house, anyone could extract private or confidential information about you or your work which you have thrown away.

CATHOLIC INSURANCE SERVICE LTD

How to Spot a phishing email

Phishing emails are fraudulent emails which seek to extract personal or financial information from you, or to corrupt your computer.

1. Be suspicious of any emails making offers, asking for your log in details or for money. Never click a link to enter your password unless you have requested the link. Never send money to a new supplier or to an existing supplier who has changed their bank account without calling a known contact first to verify the account details.

2. Be suspicious if an email or email address contains incorrect spellings (e.g. COVID-19 Relieve Payments) or capital letters in strange places. By clicking on the email address to see the full details, you may discover the email was not sent by the organisation it claims to be from.

3. Be suspicious if the email addresses you in vague terms, such as 'Dear Valued Customer'. If the sender does not know who you are, can you be sure you know who they are?

4. Banks will never put links in their emails asking you to enter log in information. Any emails purporting to be from your bank asking you for passwords or other confidential information are likely to be phishing emails.

The lockdown has resulted in many people using new forms of communication and social interaction online, such as using social networking sites to stay in touch with friends and family. It is important to remember that you never know if someone you communicate with via social media (e.g. Facebook) is who they say they are, so it is important to understand how to use these sites securely and to think carefully before posting anything.

If someone's behaviour online is worrying you or you think you may have fallen victim to a scam, tell someone. Most websites allow you to report suspicious or concerning behaviour to them so they can investigate and remove inappropriate content.

Top 10 Tips for using Social Media Safely

1. Use a strong password.
2. Use a different password for each of your social media accounts.
3. Set up your security answers for added security. This option is available for most social media sites.
4. If you have social media apps on your phone, be sure to protect your device with a passcode.
5. Use the privacy settings to control who sees what.
6. Don't give out personal information (e.g. your home address or mobile number). The more you post the easier it is to have your identity stolen.
7. Don't give out confidential information such as bank details or passwords.
8. Don't send pictures of yourself to anyone or ask them to send pictures to you.
9. Be selective with "friend" requests. If you don't know the person, don't accept their request. It could be a fake account.
10. Don't send messages that you wouldn't want "the world" to read.

Further resources

A free online Cyber Security course from the Open University has been made available during the lockdown:

https://www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-overview?active-tab=description-tab

The National Cyber Security Centre has a range of information and resources to help you learn about cyber security and to report scams:

https://www.ncsc.gov.uk

The NCVO offers cyber security guidance for small charities:

https://knowhow.ncvo.org.uk/organisation/operations/digital-technology/cybersecurity#

enquiries@catholicinsuranceservice.co.uk
www.catholicinsuranceservice.co.uk