Back up your data

Take regular backups of your important data and test that it can be restored.

- Identify what needs to ne backed up. Usually this means documents, emails, contact details, legal documents, insurance certificates, calendars, supporters and beneficiary databases.

ENSURE THE DEVICE CONTAINING YOUR BACKUP IS NOT PERMANENTLY CONNECTED TO THE DEVICE HOLDING THE ORIGINAL COPY (PHYSICALLY OR BY NETWORK).

CONSIDER BACKING UP TO THE CLOUD. THIS STORES YOUR DATA AWAY FROM YOUR NORMAL LOCATIONAND MEANS YOU CAN ACCESS IT FROM AN LOCATION.

> “Like businesses, charities are increasingly reliant on IT and technology and are falling victim to a range of malicious cyber activity. Losing access to this technology, having funds stolen or suffering a data breach through a cyber-attack can be devastating, both financially and reputationally”.

Ciaran Martin Chief Executive Officer, National Cyber Security Centre (NCSC)

> “The valuable funds, assets and good reputation of charities are at risk from the increasing threat of cyber-crime. That is why everybody involved with charities - donors, volunteers, employees, professional advisers and, above all, trustees - have a role to play in protecting the charity sector from cyber-related harm.”

Helen Stephenson Chief Executive, Charity Commission for England and Wales

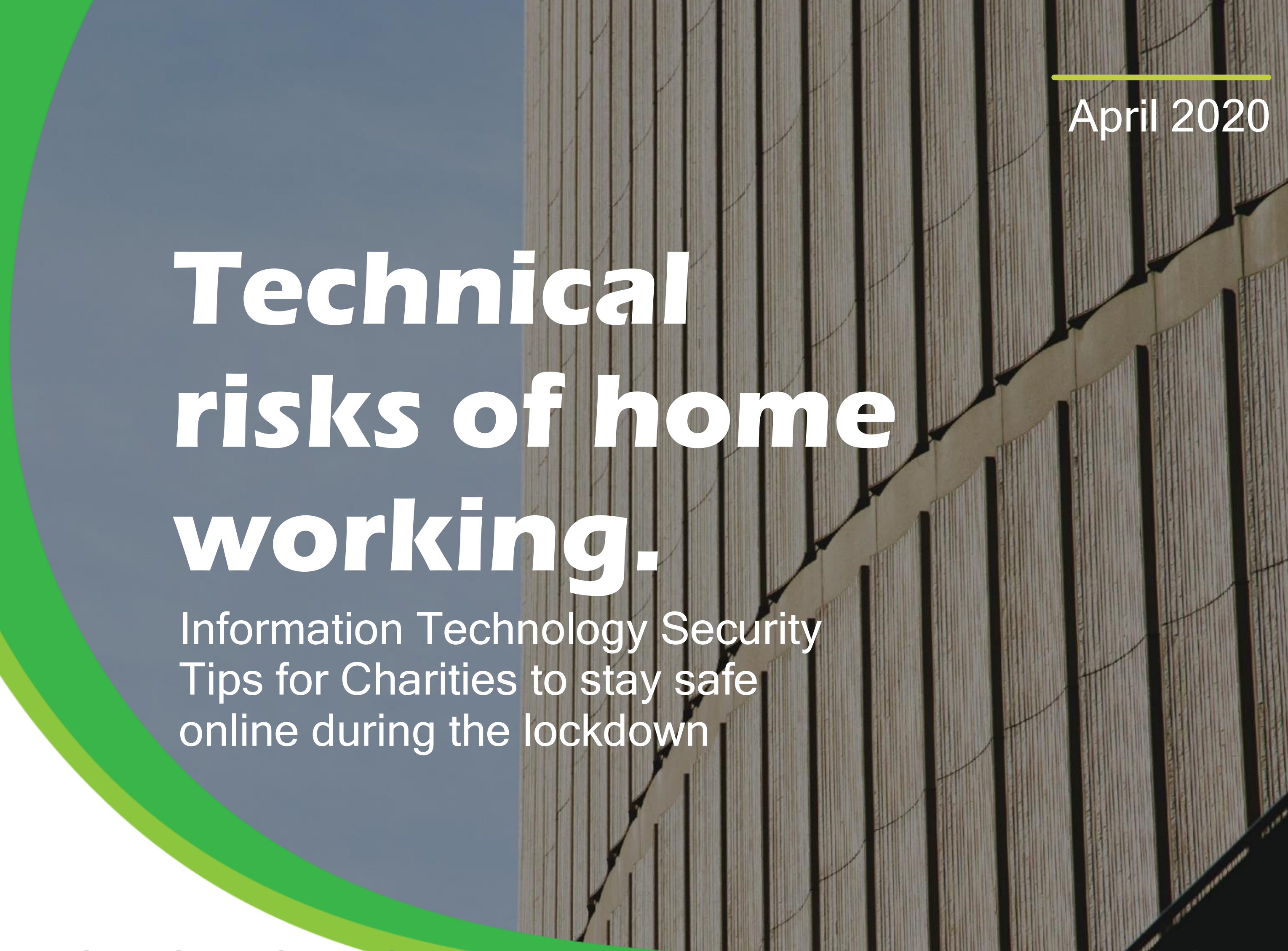
Keep your smartphones & tablets safe

BECAUSE THEY ARE OUTSIDE THE OFFICE ENVIRONMENT THESE NEED MORE PROTECTION THAN DESKTOPS.

- Switch on PIN/password/fingerprint protection.
- Configure devices so they can be traced if lost.
- Use the automatic update feature.
- Don’t connect to public Wi-Fi hotspots, these are often insecure. Use 4G instead.

5 TIPS FOR AVOIDING PHISHING ATTACKS

1. Only give trustees, staff and volunteers the lowest level of user rights for their role, so if they are targeted in a phishing attack, the potential damage is reduced.
2. Consider ways that someone might target your charity. Then make changes to the weak areas.
3. Make sure your trustees, staff and volunteers all understand your normal ways of working (especially regarding interaction with other organisations), so that they're better equipped to spot requests that are out of the ordinary.
4. Attackers use publicly available information about your charity/staff to make their phishing messages more convincing. This is usually taken from your website and social media, so check your ‘digital footprint’
5. Report all attacks.



April 2020

Technical risks of home working.

Information Technology Security Tips for Charities to stay safe online during the lockdown

PROTECT YOUR CHARITY FROM MALWARE IN 5 STEPS

1. Install (and turn on) antivirus software
2. Prevent trustees, volunteers or staff from downloading dodgy apps
3. Keep all your IT equipment and software up to date (patching)
4. Control how USB drives (and memory cards) can be used
5. Switch on your firewall

5 PASSWORD TIPS

1. If you’re mostly using fingerprint or face unlock, you’ll be entering a password less often, so consider setting up a long password that’s difficult to guess.
2. Use two factor authentication for 'important' accounts
3. Avoid using predictable passwords
4. Avoid ‘password’ overload by only enforcing password access if you really need to.
5. Change all default passwords

WATSON HEPPLE CONSULTING LTD.

INTERNAL AUDIT – TECHNOLOGY RISK ASSURANCE
COMPLETING THE PICTURE

Cranfield
TRUST