Cyber Security Essentials

LLOYDS BANK FOUNDATION
England & Wales

Cybercrime is a powerful and growing threat to charities. The Department for Digital, Culture, Media and Sport's *Cyber Security Breaches Survey 2020* found that a quarter of charities reported having cyber security breaches or attacks in the last 12 months. For charities who fall victim to a cyber attack, the effects can be devastating with money, data and reputation all at risk.

Working with the Chief Security Office at Lloyds Banking Group, we've prepared a short, four-part guide to the essentials of cyber security. Broken down into chapters on Passwords, Phishing and Data, if acted upon, these simple measures will go a long way to helping protect you, your organisation and the people you serve.

£9,470

is the average cost of all breaches or attacks identified in the last 12 months by a charity[1]

47%

of charities have looked for external help with cyber security in the last year, up from 36% in 2018[2]

£100,000

Cyber security is now being seen as a high priority in 68% of charities with an income under £100,000[3]

1/4

of charities reported cyber attacks in 2019, according to the government's latest annual survey[4]

36%

of charities don't know which type of cyber-attacks they're most vulnerable to[5]

Contents

Click to read the DCMS's 2020
Cyber Security Breaches Survey

[1 2 3] 'How charities are responding to cyber security threats', GOV.UK
[4] 'Cyber Security Breaches Survey 2020', GOV.UK
[5] 'Charities at increasing risk of cyber-crime', SC Magazine

Why Cyber Security matters

On the 16 May 2017, Wiltshire's Dorothy House Hospice Care reported that they had fallen victim to a 'sophisticated criminal financial fraud', resulting in the theft of £130,000 from its bank account.

Thankfully their patient and family care services were unaffected and confidentiality was not compromised, however the fraud represents a significant financial loss for the charity. Sadly, Dorothy House is just one of many thousands of charities who have suffered such attacks.

"That such a despicable crime can be targeted at a charity like Dorothy House makes me extremely angry and is an affront to the amazing work and support of our community, staff and our volunteers," commented CEO John Davies.

Acting quickly, Dorothy House alerted all relevant authorities including the Police, Banks, their Trustees and Insurers, the Charity Commission and NHS Counter Fraud Support. Following an investigation by forensic experts, the charity were able to recover almost a third of the stolen funds.

Whilst the charity have since enacted a number of further protections, the attack represented a significant challenge even for a charity of its size. For smaller charities the damage could have been much worse.

> That such a despicable crime can be targeted at a charity like Dorothy House makes me extremely angry and is an affront to the amazing work and support of our community...

John Davies, CEO, Dorothy House Hospice Care

Time-strapped?
Here's what you can do in...

▶ Watch 'Introduction'

5 minutes

Create a unique and strong password for your email

Your email password is the gateway to all of your other accounts. See how to create one here

Click here

Update your devices

Software updates include crucial security updates. Make sure your devices are up-to-date

Click here

1 hour

Watch our Cyber Security Essentials videos

Learn the essentials of cyber security, so grab your lunch, tune in and share with colleagues

Click here

Install a Password Manager

Use a password manager to create and store strong, unique passwords

Click here

Set up two-factor authentication

Create an added layer of protection beyond your password with two-factor authentication

Click here

Half a day

Explore the National Cyber Security Centre

The National Cyber Security Centre is a free resource providing up-to-date advice

Click here

Perform a back-up

Create a copy of your files to protect against accidental loss and theft of your data

Click here

Reduce your digital footprint

Remove unused accounts and unnecessary information and upgrade security settings

Click here

Passwords

Watch the film

How to create a strong password

▶ Watch 'Passwords'

In 2019 the National Cyber Security Centre released the first UK Cyber Survey. Amongst the startling findings is that 23.2 million victim accounts worldwide used '123456' as a password.

A password comprising of six lower-case letters can be cracked by a computer system in just 0.0047 seconds. However a series of ten mixed case letters, numbers and characters could take approximately 2,740 years to crack.

A strong, unique password for **each** of your accounts is one of the most effective ways to keep your money, data and reputation safe.

The key to a strong password is a seemingly random mix of upper and lower-case letters, numbers and characters. This may seem daunting and impossible to remember for each of your accounts but there is a useful way of constructing your passwords to help.

1 Take a memory, boil it down to three words...

When Alice lost a **front** tooth and could **whistle** through the **gap**

2 Combine them in a random order

frontwhistlegap

3 Add upper and lower-case letters

FrontWhistleGap

4 Add special characters and numbers

Fr0ntWh!stl£G@p

Make it long

10 characters or more

Make it unique

No two passwords the same

Mix cases & characters

Use upper and lower-case letters and characters

Consider a password manager

A password manager is **an encrypted vault for your passwords**. It is a programme that either is installed on your computer, or functionality built into your browser. One master password is used to unlock it.

Safari, Firefox and Chrome all have built in password managers which will prompt you when entering a password whether you'd like to use it. There are a number of options for installed password manager with both paid and free options.

Click to read CNET's article on **'The best password manager to use for 2020'**

Using two-factor authentication

Watch ‘Passwords’

You may have purchased a device recently that allows you to unlock it using your fingerprint or even a pattern drawn with your finger. Many agree that **a simple password is not sufficient as threats become more ambitious and nuanced.**

In addition to passwords, many companies have adopted what’s called ‘Two-factor Authentication’ (sometimes known as ‘Two-step Verification’ or ‘2FA’). This is an additional layer of security where they’ll double-check it’s really you using an alternative method of communication. For example, your bank may send you a code in a text to your phone to input before a purchase is confirmed.

Many websites and apps will prompt you to switch on two-factor authentication, however you can do it manually.

Click to read The Verge’s guide on **How to set up two-factor authentication on all your online accounts**

Phishing and Social Engineering

Watch the film

What do we mean by Phishing?

Watch ‘Phishing’

You may recall a strange email with an alarming alert or promise that was too good to be true. It was likely an attempt to steal your data or breach the security of your device. Perpetrators of this form of cyber crime are called ‘Social Engineers’ as they use human psychology to exploit their victims.

There are a few forms of phishing, but they all involve a communication sent from a person or group masquerading as a legitimate organisation. They will attempt to direct you to a website, often through an attachment or URL link, in order to steal personal information or infect your computer or device with harmful malware (malicious software).

Here are some of the most common forms:

Phishing

Most phishing attacks are through email. The sender will use a fake web address that attempts to mimic a real organisation. **Watch out for spelling errors and strange email addresses**. Verify via a known method and **never forward a suspicious email.**

Baiting

Similar to phishing except with a shiny prize or promise to entice its victim in. It can come in both digital and physical forms such as post or flyers. **If it’s too good to be true, it probably is!**

Smishing/Vishing

Like Phishing, Smishing uses text messages whilst Vishing uses a real telephone conversation. The commonly request card and private details. **If in doubt, hang up and call back via a known number.**

Spearphishing

A more sophisticated form of phishing, **it will contain identifiable information such as name, job title, employer etc...** in an attempt to convince you it’s genuine.

Whaling

Like spearphishing, Whaling targets its victims but at a much more senior level. **They may impersonate a colleague** to trick the recipient into parting with information or files.

Remember, if the message gives you any strong emotional reaction, whether happy, sad or anxious: stop, think and check before you click!

Why cyber security matters

Watch 'Phishing'

On 2 July 2019 St John Ambulance was the victim of a ransomware attack, a form a malware (malicious software) that prevents you accessing your computer or files until a payment or other demand is met. The attack temporarily blocked the prominent first-aid charity from accessing data customers had supplied when booking a training course.

Ransomware attacks take advantage of the value of data and the importance of access to vital files and infrastructure. It often involves the threat of publishing the data unless the demand is met. Whilst the cause of the breach is not known, such attacks often come from phishing.

Thankfully for St John Ambulance the data, related to their training course delivery, was not shared outside the organisation. "We work as hard as we can to protect our data systems from these types of attack and employ a range of third-party partners and cyber-crime solutions to continually update our protection," said a spokesperson to Computer Weekly. Within 30 minutes the charity had isolated and resolved the issue and reported the incident to the police, the Information Commissioner's Office and the Charity Commission.

"This serves as a reminder that organisations should train their staff on being able to identify a phishing email and not click on malicious links," said Javvad Malik, a security specialist at KnowBe4, quoted by Computer Weekly.

> This serves as a reminder that organisers should train their staff on being able to identify a phishing email and not click on malicious links.
>
> Javvad Malik, KnowBe4

Take action against phishing in all its forms with these steps:

1. Report

Report messages that you're suspicious of to whoever they purport to be from. Verify the sender and don't forward any suspicious materials, screenshot if needed.

2. Install

Ensure your anti-virus software is up to date and any and all updates are up-to-date on your's and your team's devices.

3. Update

Ensure your anti-virus software is up-to-date on your's and your team's devices.

4. Back-up

Know that your data and information is backed-up by using an external hard-drive or cloud-based solution. Ensure any physical back-up is stored securely, remotely and encrypted.

Data

Watch the film

Classify and encrypt your data

Watch ‘Data’

Our data is very valuable to us, we work hard to collect it, analyse it and keep it safe. It’s also highly sought after by those who hope to use it for their own means, especially if it has a financial element.

Classifying data essentially means deciding how important it is. It’s advisable to encrypt more important (more confidential) data. This means scrambling the data so that no one but the person with the ‘key’ can unscramble it. Without that ‘key’, the data is useless.

Some programmes such as Microsoft Office have built-in password protection to help secure files being passed around. You can also encrypt external hard drives.

Consider how you label your communications and data to signify its classification, whether that’s in an email subject line, or via your file structure.

Opposite is a table to help decide what information is important to you. Fill in the table with a few examples from your work and share with your colleagues for them to have a go too. In this way you can agree a uniform approach that is understood across your charity.

Click for more on encrypting data from **The Information Commissioner’s Office**

Classification	**Public**	**Limited**	**Confidential**	**Highly confidential**
	Information we’re happy to share with the public	Information that is for internal and trusted partner use only	Detail that is for select eyes only	Protected, perhaps damaging, information
Encryption	None	None	Encrypt when sending outside organisation	Always encrypt

Example	“Mike is fundraising for us” - ideal for social media, website etc...	“Mike from our accounts team” - known within the organisation but could potentially make him a target	Mike’s full name, address, date of birth for booking travel - identifiable, private information, not for whole organisation	Mike’s medical history around mental health - deeply personal, private and potentially harmful if made public

Print this page for your work area

Simple steps to avoid a cyber security breach

If a USB is lost or stolen you don't know where that data may end up. If you need to use one, make sure you encrypt it.

Spelling errors in email addresses are easy to make but you don't know whose inbox it may land in.

Beware phishing. They may ask for data and may seem genuine but verify and ask why they need this data.

Do not email data to a home address, this increases the risk of it being intercepted or mismanaged.

Who to inform if a breach occurs

Make a list of essential people to inform if a breach occurs. This should include whoever is manages your IT, your Chair of Trustees, perhaps a contact at the bank etc...

Name	**Role**	**Number**

Other organisations you may need to inform:

Action Fraud (The National Fraud & Cyber Crime Reporting Centre)
0300 123 2040

Charity Commission Serious Incident Report
charitycommission.gov.uk/report-a-serious-incident

The Information Commissioner's Office
ico.org.uk/for-organisations/report-a-breach/

Now you've mastered the essentials of Cyber Security, put it to the test…

1. Who might you inform of a data breach? (Multiple choice)

□ a. Your Trustees
□ b. Your IT Manager
□ c. The Police
□ d. The Charity Commission

2. Which of these is the strongest password?

□ a. mypassword
□ b. BigGreenEye2
□ c. C0ffeeTra1nF!sh
□ d. 16284633837

3. Which of these pieces of information might be used in a 'spearphishing' attempt? (Multiple choice)

□ a. Your job-title
□ b. Your email address
□ c. Your employer
□ d. Information from your social media profile

4. Which of these are ways to avoid data breaches? (Multiple choice)

□ a. Avoid using USB memory sticks
□ b. Double-check spelling of email addresses
□ c. Avoid sending data/files to home email addresses
□ d. Verifying emails that seem suspicious

5. What is the fourth action to take to protect against phishing? Report, install, update and….

□ a. Delete
□ b. Back-up
□ c. Share
□ d. Restart

6. What classification would this piece of information require? *'A spreadsheet containing a list of donors and their email addresses'*

□ a. Public
□ b. Limited
□ c. Confidential
□ d. Highly confidential

Answers at the bottom of the next page

More resources

Information Commissioner's Office
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
ico.org.uk

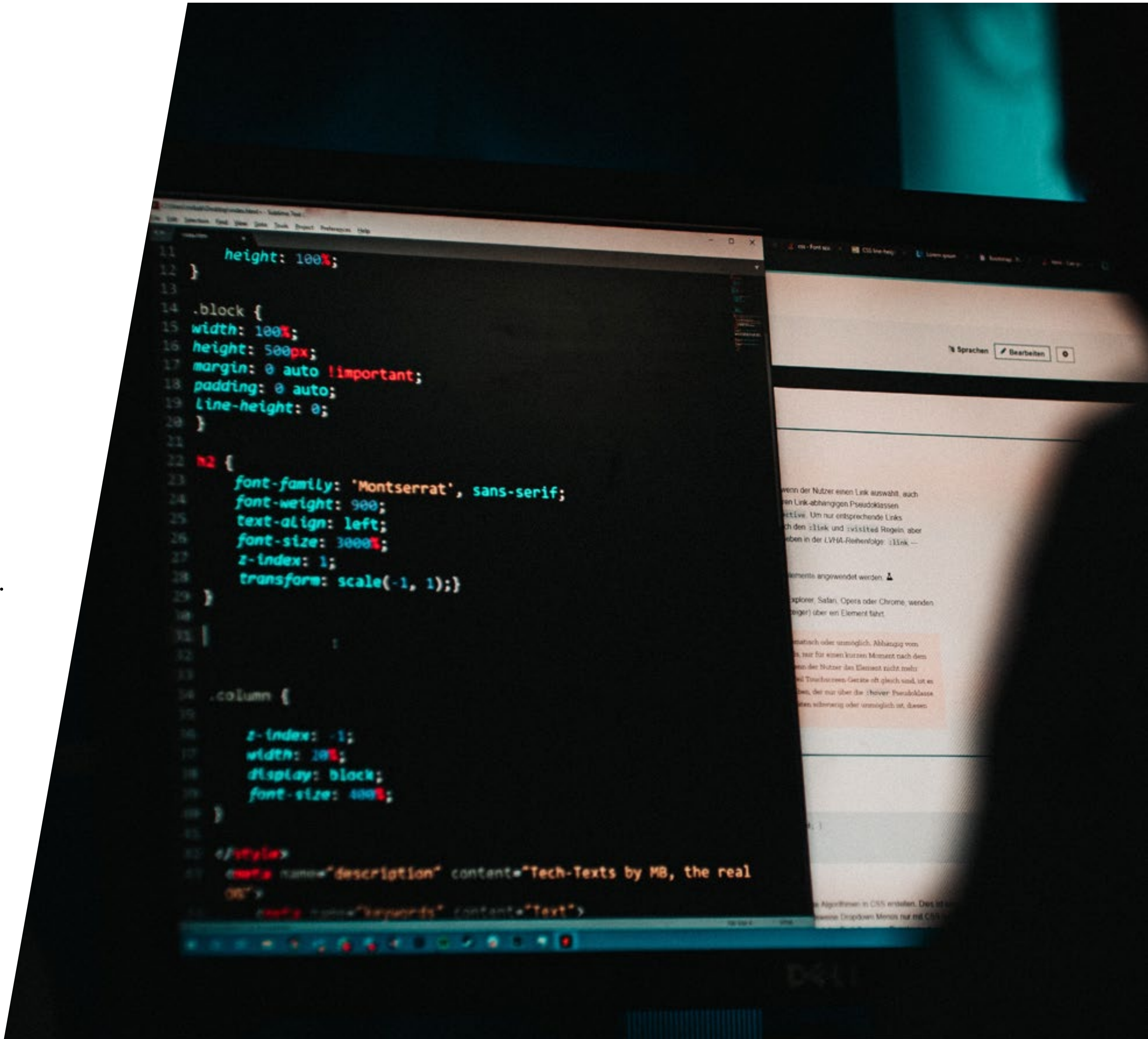
National Cyber Security Centre
Supports critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public.
ncsc.gov.uk
'Charity Security: Small Charity Guide'

NCVO
NCVO Knowhow offers advice and support for voluntary organisations. Learn from your peers and from experts, and share your experiences with the community.
knowhow.ncvo.org.uk

Charity Retail Association
Membership organisation for charity shops in the United Kingdom.
charityretail.org.uk

Charity Commission for England and Wales
Preventing Charity Cybercrime Insights and Action Report
assets.publishing.service.gov.uk

Crisis Communications Plan
When a crisis occurs, make sure you have a plan to combat it. Charity Comms has a downloadable Crisis Communications plan template that's a good place to start.
Crisis Communications Plan

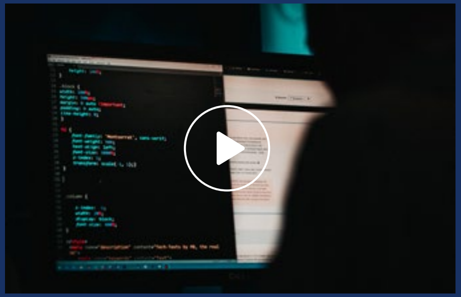


```
    height: 100%;
}

.block {
width: 100%;
height: 500px;
margin: 0 auto !important;
padding: 0 auto;
line-height: 0;
}

h2 {
    font-family: 'Montserrat', sans-serif;
    font-weight: 900;
    text-align: left;
    font-size: 3000%;
    z-index: 1;
    transform: scale(-1, 1);}
}

.column {
    z-index: -1;
    width: 20%;
    display: block;
    font-size: 400%;
}

</style>
<meta name="description" content="Tech-Texts by MB, the real
OG">
    <meta name="keywords" content="Text">
```

Answers: 1. a, b, c, d; 2. c; 3. a, b, c, d; 4. a, b, c, d; 5. d; 6. c

More from Cyber Security Essentials

Passwords



Phishing

Data

Lloyds Bank Foundation for England & Wales partners with small and local charities who help people overcome complex social issues. Through long-term funding, developmental support and influencing policy and practice, the Foundation helps charities make life-changing impact. The Foundation is an independent charitable trust funded by the profits of Lloyds Banking Group as part of their commitment to Helping Britain Prosper.

lloydsbankfoundation.org.uk

@LBFEW

/lloydsbankfoundation

Contact Us:

Pentagon House
52-54 Southwark Street
London SE1 1UN

enquiries@lloydsbankfoundation.org.uk

Registered Charity No. 327114
Company Limited by Guarantee
Registered in England and Wales
Company No. 1971242

LLOYDS BANK
FOUNDATION
England & Wales