superhighways

harnessing technology for community benefit

# Cyber Security in 60 mins

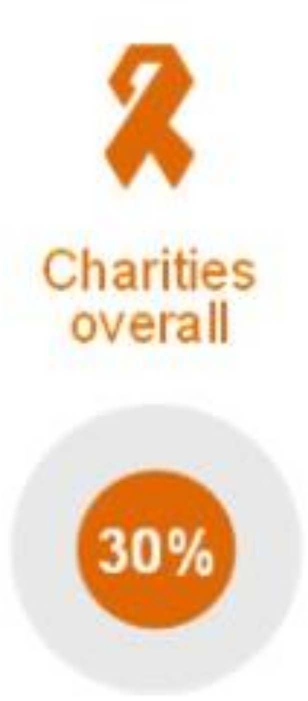
## Part 1: Passwords & Multi Factor Authentication

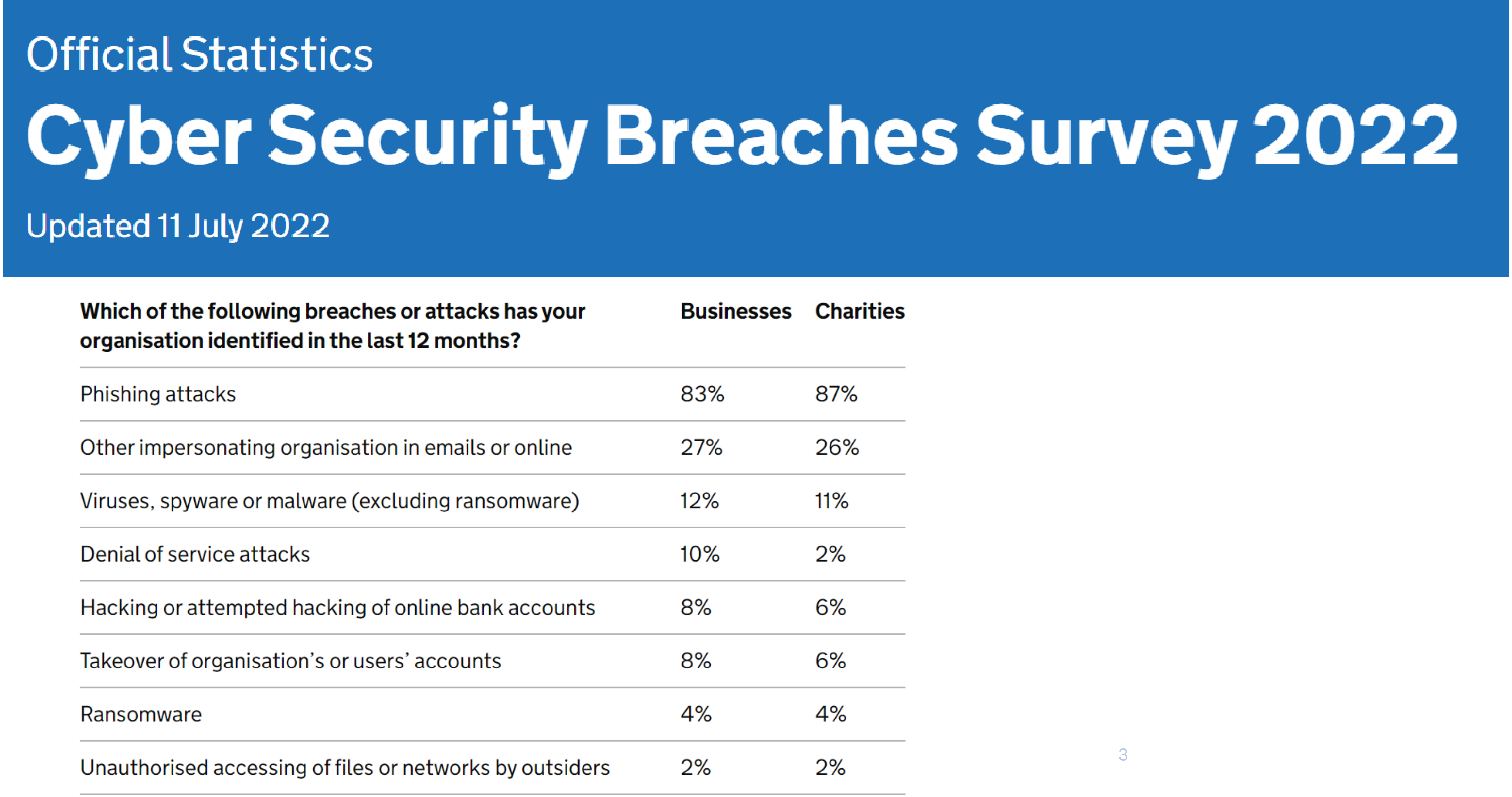
#DigitalFoundations

# Some context about Cyber Attacks

Question:

In the annual DCMS survey 2022, what percentage of charities reported having a cyber security breach in the last 12 months?





Official Statistics

# Cyber Security Breaches Survey 2022

Updated 11 July 2022

| **Which of the following breaches or attacks has your organisation identified in the last 12 months?** | **Businesses** | **Charities** |
|---|---|---|
| Phishing attacks | 83% | 87% |
| Other impersonating organisation in emails or online | 27% | 26% |
| Viruses, spyware or malware (excluding ransomware) | 12% | 11% |
| Denial of service attacks | 10% | 2% |
| Hacking or attempted hacking of online bank accounts | 8% | 6% |
| Takeover of organisation's or users' accounts | 8% | 6% |
| Ransomware | 4% | 4% |
| Unauthorised accessing of files or networks by outsiders | 2% | 2% |

Visit the full report

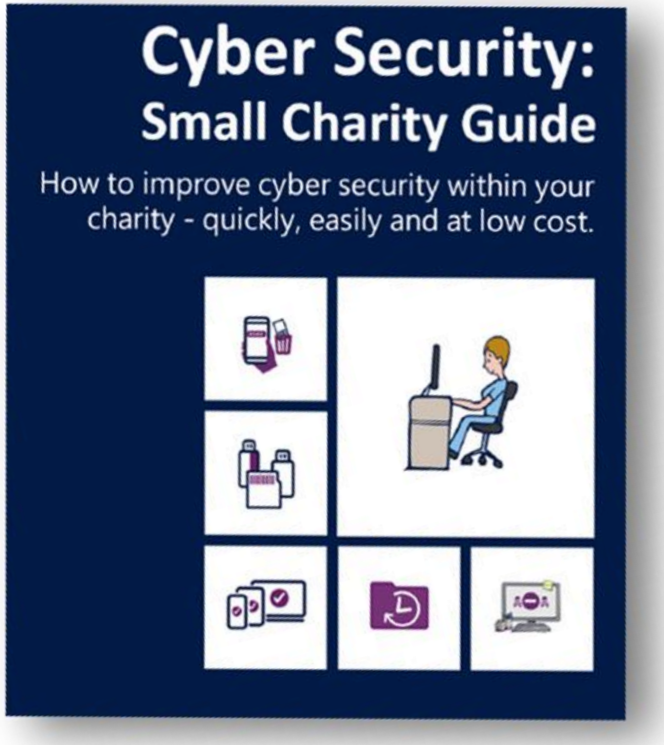
# Data protection – GDPR principles

1. Process lawfully, fairly and in a transparent manner
2. Collect for specified, explicit and legitimate purposes
3. Only keep what is adequate, relevant and limited to what is necessary
4. Store accurate information and keep up to date
5. Retain only for as long as necessary
6. Process in an appropriate manner to maintain security

# What can you do to protect your charity?

The National Cyber Security Centre's 5 quick, simple, free or low cost steps

1. Backing up your data
2. Protecting against malware
3. Securing your mobile devices
4. Password best practice
5. Avoid phishing attacks


Cyber Security:
Small Charity Guide
How to improve cyber security within your charity - quickly, easily and at low cost.

Download the full guide Download the infographic

# Passwords: protecting our accounts & devices

- ✓Emails
- ✓Files
- ✓Databases / CRMs
- ✓Websites
- ✓Social Media
- ✓And more!

- ✓Phones
- ✓Tablets
- ✓PCs & laptops

But also

- ✓Firewalls
- ✓Routers
- ✓Servers

# Passwords: often the weakest link

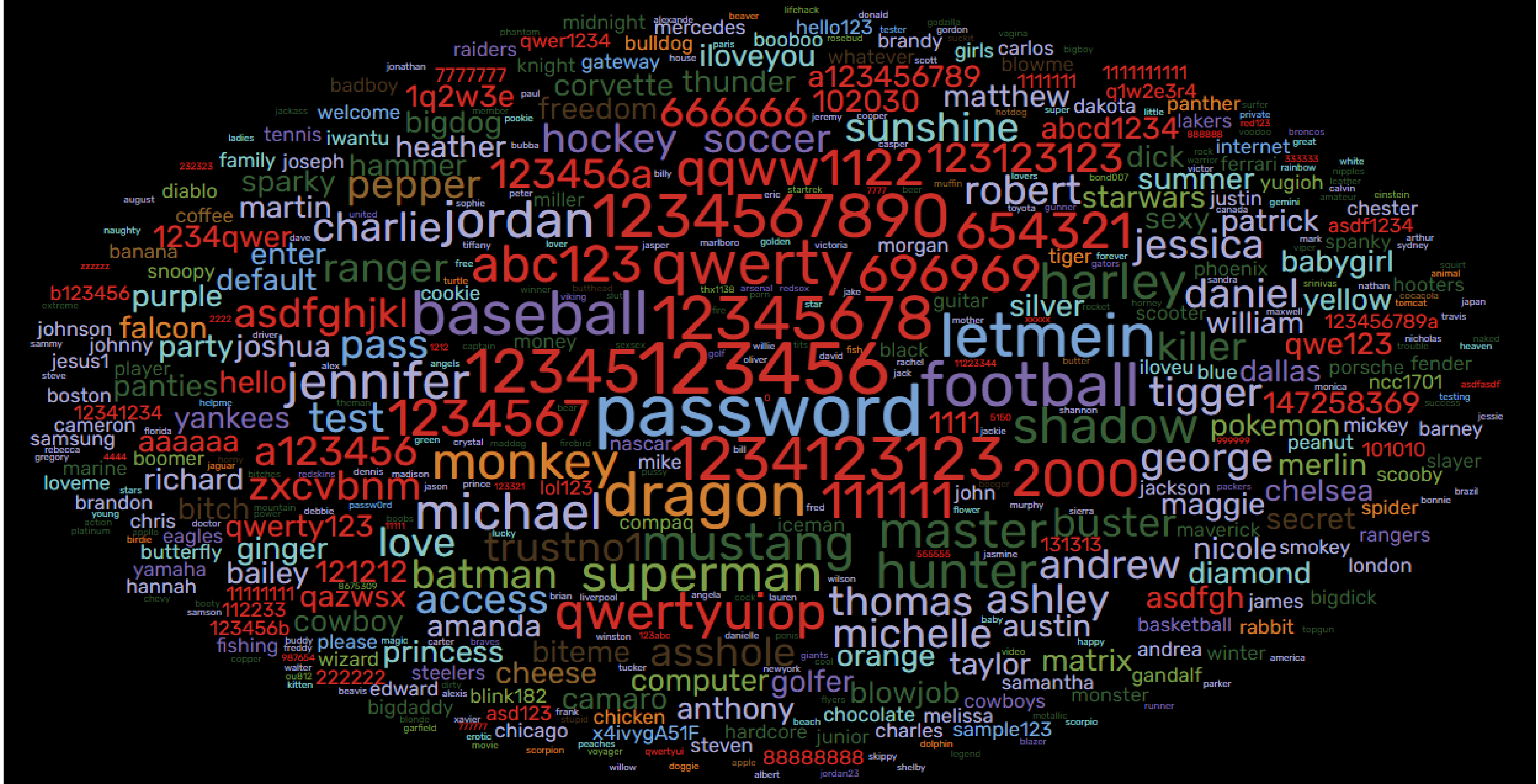
✓ What's your password video (Hollywood Boulevard)

# Most Common Passwords

## Is yours here?

*select a category below to filter*

🟥 alphanumeric 🟧 animal 🟦 fluffy 🟫 food 🟩 macho ⬜ names 🟩 nerdy 🟫 rebellious 🟦 security 🟪 sports



David McCandless **Information is Beautiful**

**source:** 20+ data breaches // data

MADE WITH VIZsweet

# Secure passwords

[Secure Passwords (captioned) Explained by Common Craft (VIDEO)]

# Discussion

✓What consequences may arise from using a weak password?

✓How might a strong password be compromised?

✓How long does it take to crack these passwords?

| | |
|---|---|
| ✓QwErTy987123! | 15 seconds |
| ✓CoffeeTinyFish | 6 hours |
| ✓CoffeeTinyFish#9 | 6 days |

# Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.

**Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.

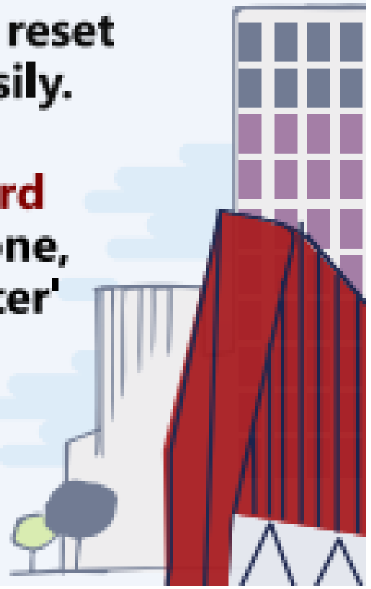
**Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

**Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

**Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

**Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.



# Multi (or Two) Factor Authentication

- ✓Have you had to sign in to a website that requires two factor authentication?

- ✓Describe the experience.

[Two Factor Authentication (captioned) Explained by Common Craft (VIDEO)]

# Discussion

✓ What are the advantages and disadvantages of using two factor authentication?

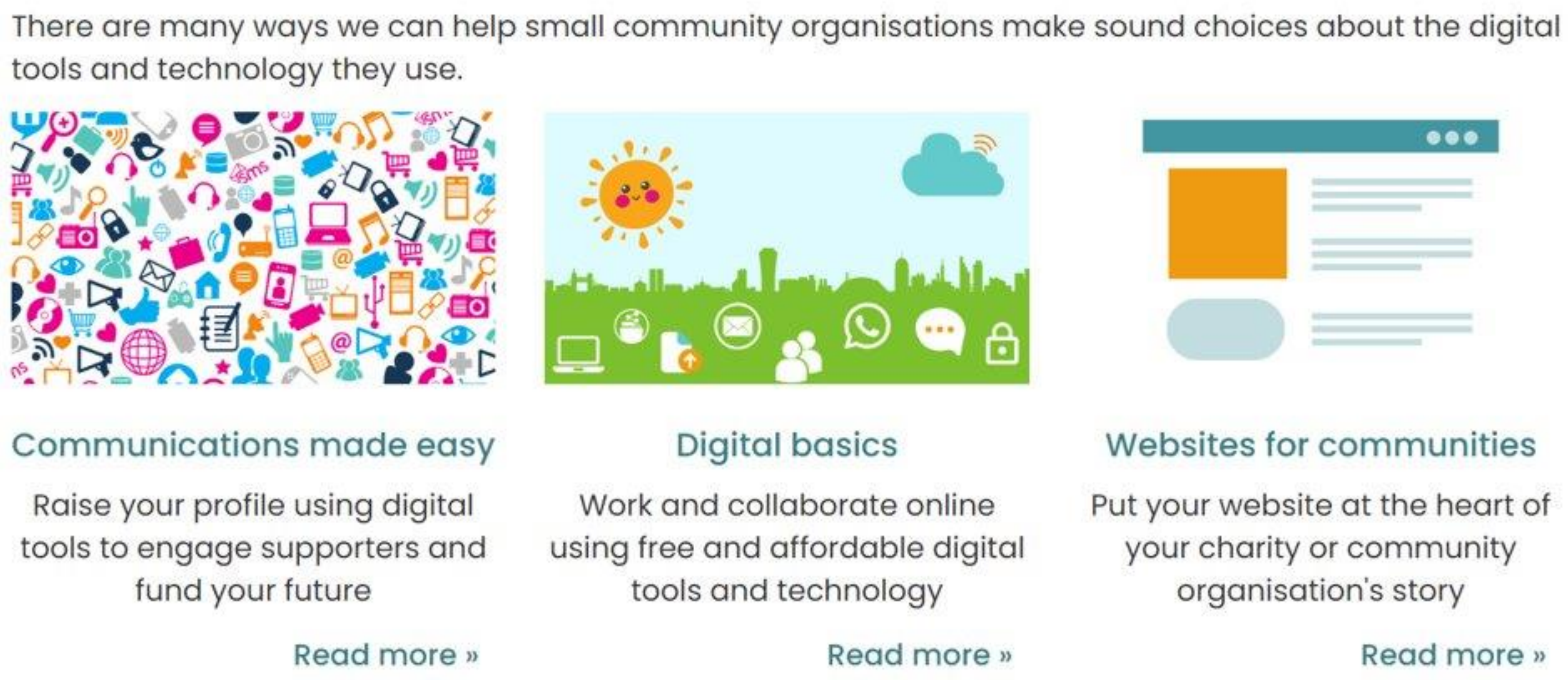
# Action planning – questions to ask

1. What accounts do you have? Which of these contain personal and potentially sensitive information? (prioritise these)
2. Are people using weak / ‘easy to crack’ passwords?
3. Can you enable multi factor authentication on your accounts?
4. Do people share account log ins?
5. Do you change passwords when people leave your organisation?

# Key takeaways

1. **Switch on password protection** - where this not enabled by default
2. **Change all default passwords** – to mitigate against ‘open door’ access
3. **Avoid predictable passwords** – have an organisational password policy, implementing NCSC’s 3 random words plus a number and symbol
4. **Use two factor authentication** – where available for the tools you are using
5. **Individual accounts for everyone where possible** – easier to control authorised access Remember to block accounts / change passwords when people leave your organisation

# Digital Foundations programme



There are many ways we can help small community organisations make sound choices about the digital tools and technology they use.

### Communications made easy

Raise your profile using digital tools to engage supporters and fund your future

Read more »

### Digital basics

Work and collaborate online using free and affordable digital tools and technology

Read more »

### Websites for communities

Put your website at the heart of your charity or community organisation's story

Read more »

Find out more about the Digital Foundations programme

# About Superhighways

Providing tech support to small local charities in London for over 20 years

✓ Support
✓ Training
✓ Consultancy
✓ Digital inclusion
✓ Datawise London
✓ See all services

✓ E-news sign up

superhighways
harnessing technology for community benefit

# Thank you for listening

KATE WHITE

info@superhighways.org.uk
@SuperhighwaysUK

#DigitalFoundations