



superhighways

harnessing **technology** for **community** benefit

# Cyber security basics:

An introduction to cybersecurity  
for everyone

Paul Firby

#DigitalFoundations

# Some context about Cyber Attacks

## Question:

In the annual DCMS survey 2024/25, what percentage of charities reported having a cyber security breach in the last 12 months?

24% 30% 60% 76%

30% - charities over all

Rising to 60% for charities with income over £500,000



# Cyber security breaches survey 2023

Published 19 April 2023

Type of breach or attack in the last 12 months	Businesses	Charities
Phishing attacks	79%	83%
Others impersonating organisation in emails or online	31%	29%
Viruses, spyware or malware (excluding ransomware)	11%	9%
Hacking or attempted hacking of online bank accounts	11%	6%
Takeovers of organisation's or users' accounts	9%	5%
Denial of service attacks	7%	7%
Ransomware	4%	4%
Unauthorised accessing of files or networks by staff	2%	4%
Unauthorised accessing of files or networks by outsiders	2%	2%
Unauthorised listening into video conferences or instant messages*	0.5%	1%
Any other breaches or attacks	4%	4%

[Visit the full report](#)



# How are charities being attacked?

- **Business email attacks (phishing)**

Scam emails sent to people asking for sensitive information (such as bank details) or encouraging them to visit a fake website

- **Fake organisations and websites**

- **Ransomware**

A type of malware that makes data or systems unusable until the victim makes a payment.

- **Malware and Spyware**

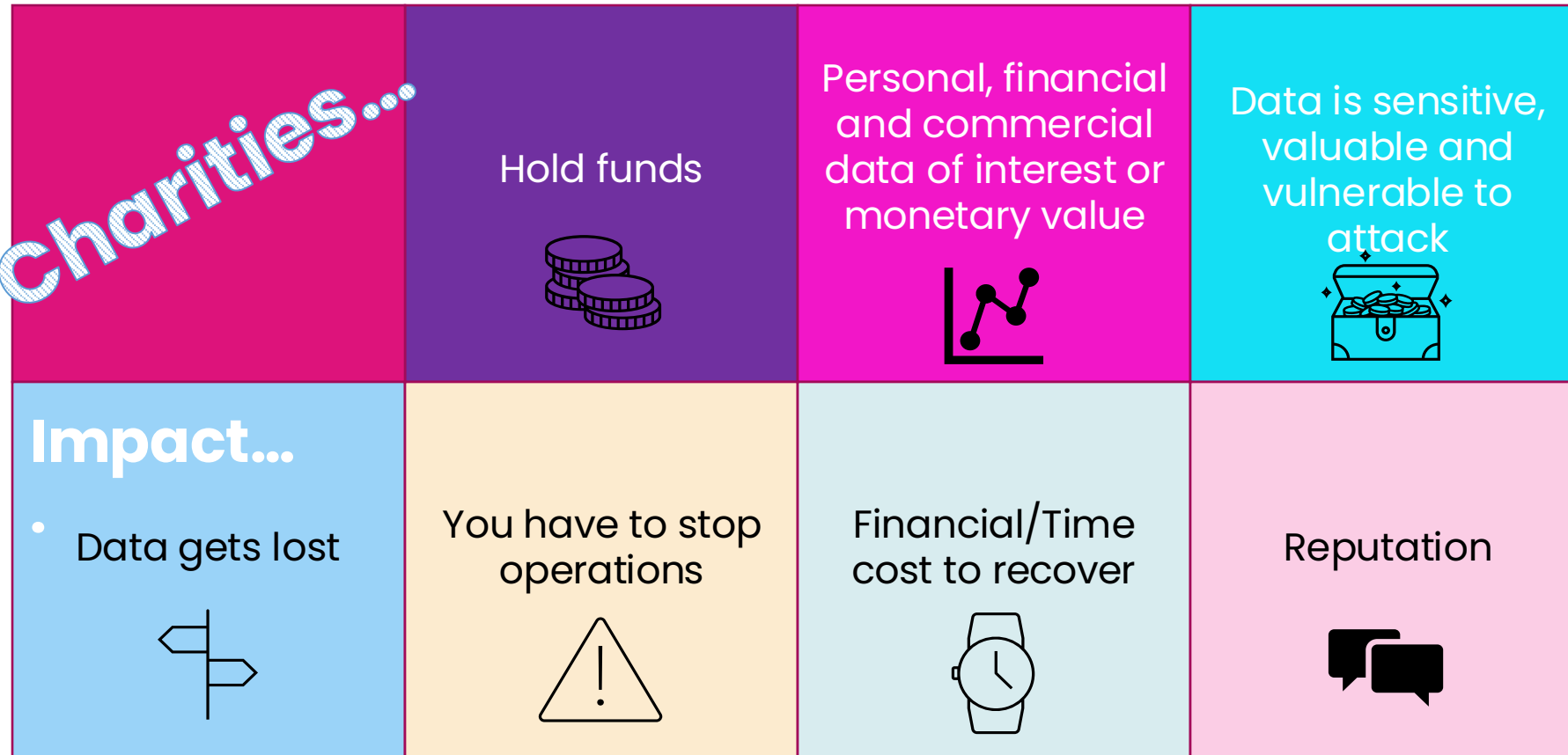
Malicious software that is designed to interfere with a computer's normal functioning and that can be used to obtain information and commit cybercrimes.

# 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



# Why are charities at risk?



Charities, in particular, remain a tempting prospect for cyber criminals, housing a wealth of data but with often limited resources to protect it.

# 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

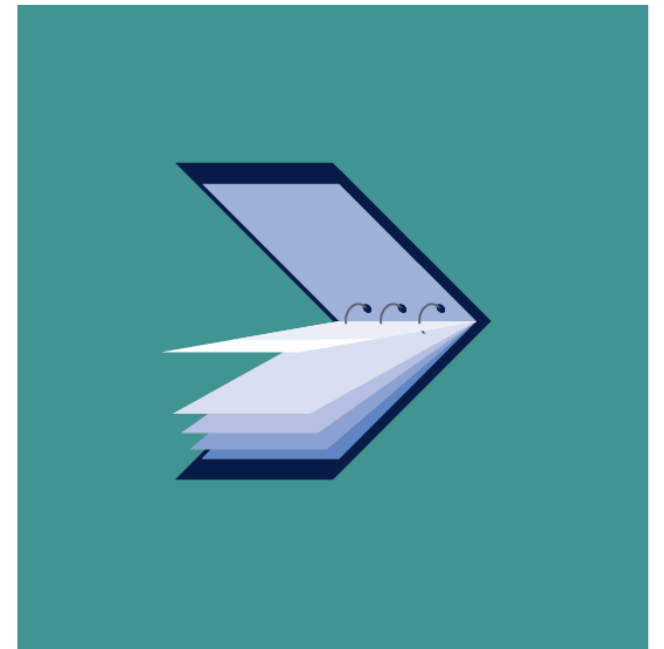
[Download the full guide](#)



**Cyber Security**  
Small Business Guide

Small  
Business  
Guide  
Collection

How to improve your cyber security;  
affordable, practical advice for businesses



## Cyber Security Small Business Guide

### Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
- **Ensure the device containing your backup is not permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

### Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at [www.ncsc.gov.uk/smallbusiness](http://www.ncsc.gov.uk/smallbusiness)

- Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked.**
- Keep your **devices** (and all **installed apps**) **up to date**, using the **'automatically update'** option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots – **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs.**
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

### Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.

- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and Internet.

### Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges.** This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

### 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).
- **If you forget your password** (or you think someone else knows it), tell your IT department as soon as you can.
- **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 their device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager**, which are tools that can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all of your other passwords, make sure it's a strong one, for example by using three random words.

# Passwords: protecting our accounts & devices

- ✓ Emails
- ✓ Files
- ✓ Databases / CRMs
- ✓ Microsoft 365
- ✓ Websites
- ✓ Social Media
- ✓ And more!

- ✓ Phones
- ✓ Tablets
- ✓ PCs & laptops

But also

- ✓ Firewalls
- ✓ Routers
- ✓ Servers





# Passwords: often the weakest link

How Secure is my password?

[Password Tester | Test Your Password Strength | Bitwarden](#)

Have I been PWNed?

[Have I Been Pwned: Check if your email has been compromised in a data breach](#)



# Creating a Secure Password

- ✓ Choose three random words
  - ✓ carrot printer sparrow
- ✓ Add some punctuation
  - ✓ carrot"printer"sparrow"
- ✓ Add some numbers
  - ✓ 20carrot"printer"sparrow"26
- ✓ You now have a 27-character password that's easy to remember!
- ✓ [Free Password Generator | Create Strong Passwords | Bitwarden](#)





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



# Multi (or Two) Factor Authentication

- ✓ Have you had to sign in to a website or service that requires two factor authentication?
- ✓ Describe the experience.
- ✓ What are the advantages and disadvantages of using two factor authentication?



# PINs and biometrics

- Switch on PIN / fingerprint /facial recognition recognition for all devices (maybe not facial on Android!)
- If using Windows laptops – new installations use the **Windows Hello** feature, where you choose a PIN specific to that device and with single sign on, signs on to your Office 365 account. But it can't be used to sign on another device. (See [Why a PIN is better than a password](#))



# 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



# 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?





[Phishing video from CommonCraft](#)



# What is Phishing?

- ✓ A scam in which a criminal impersonates a trusted online organisation, sending fake emails to thousands of people to trick them into handing over important sensitive information like account numbers and passwords, or containing links to bad websites.
- ✓ Scammers might try to trick you into sending money, steal your details to sell on, or send you to a dodgy website which could download viruses onto your computer or steal your passwords.



# Spotting Phishing Emails

This was put together by a team from Google

[Jigsaw | Phishing Quiz](#)

And try this one which changes monthly

[Phish Me If You Can – Phishing Simulator](#)



# Here's two phishing examples

## facebook

Hi,

Your Facebook account was recently logged into using a confirmation code and the email address [REDACTED] on April 16, 2022.

Operating system: Windows  
Browser: Chrome  
IP address: 36.87.22.189  
Estimated location: Clearwater, FL

If you did this, you can safely disregard this email.

If you didn't do this, please [secure your account](#) here or by scanning the QR code below.



Thanks,  
The Facebook Security Team



Dear Customer,

We tried to renew your services but the payment failed. The following services are due for renewal:

[REDACTED] [co.uk](#) 07/06/2025

We'd recommend taking the following steps:

1. Head to <https://my.20i.com/account/billing-details> and check your payment methods are up-to-date.
2. Try processing the renewals manually from <https://my.20i.com/account/renewals>. Select Renew on the services due for renewal.

Sometimes your bank will require the card holder to be present for the transaction due to new **Strong Customer Authentication** rules, a manual renewal of the services will resolve this.

If you're still having problems we'd recommend reaching out to the bank that issued the card for more information.

Please note that unless action is taken in the next 14 days these products may be suspended and eventually deleted. As per our terms and conditions, non-payment isn't considered cancellation of your service, if you have any questions regarding your account or billing, please login at <https://my.20i.com> and select Contact Customer Services.

Kind regards,

The 20i Team  
<https://www.20i.com>

[Other examples at Which Consumer Rights News](#)



# Know the obvious signs of phishing

A phishing attack is a type of cyberattack that tries to trick users into revealing their personal or financial information. Some of the common features of a phishing attack are:

- ✓ - **A fake sender:** The attacker pretends to be someone else, such as a trusted company, a friend, or a government agency. They may use a similar email address, logo, or website to fool the user.
- ✓ - **A sense of urgency:** The attacker creates a false sense of urgency or threat, such as saying that the user's account has been compromised, that they have won a prize, or that they need to update their information immediately.
- ✓ - **A request for information:** The attacker asks the user to click on a link, open an attachment, or provide their personal or financial information. The link may lead to a malicious website that looks legitimate, the attachment may contain malware, or the information may be used for identity theft or fraud.



# Spear-Phishing

## Check your digital footprint

- ✓ Attackers use publicly available information about your charity and staff to make their phishing messages more convincing, often gleaned from your website and social media accounts
- ✓ What do visitors to your website and social media followers need to know, and what detail is unnecessary (but could be useful for attackers)? What do trustees, staff and volunteers give away about your charity online?
- ✓ See the [CPNI's Digital Footprint Campaign's](#) useful resources including posters and booklets to help you work with staff to minimise online security risks.



# Spear-Phishing

Good example of spear-phishing in [Which](#)

## 4 ways you can avoid being spear-phished

1. Oversharing on social media:
2. Filling in data on dodgy websites:
3. Not having antivirus installed:
4. Speaking to scam callers:



# Text scams

## If you receive a suspicious text message

- ✓ Most phone providers are part of a scheme that allows customers to report suspicious text messages for free by forwarding it to **7726**.
- ✓ If you forward a text to **7726**, your provider can investigate the origin of the text and arrange to block or ban the sender, if it's found to be malicious.
- ✓ [Find further information on the Action Fraud website.](#)



# Phone scams

## If you receive a suspicious phone call

- ✓ Phone scammers will call you unsolicited, pretending to be from an organisation you trust, such as your bank, a service provider or even the police.
- ✓ These scam calls may be automated, or from a real person. They may ask you for your personal information like banking details, or tell you, you need to transfer money.
- ✓ If you've lost money or have been hacked because of responding to a call, you should [report it to Action Fraud online](#) or call 0300 123 2040.



# Report all attacks

- ✓ Encourage your team to ask for help if they think they might have been a victim of phishing and to raise as soon as possible
- ✓ Take immediate steps if you suspect a successful attack has occurred including scan for malware and change passwords as soon as possible
- ✓ **Avoid a blame culture** – this may discourage people from reporting in future
- ✓ If you believe you have been a victim you should report this through:
  - ✓ Action Fraud ([www.actionfraud.police.uk](http://www.actionfraud.police.uk))
  - ✓ Charity Commission – where there's been a serious incident
  - ✓ Information Commissioners Office – where this has led to a data breach



# Configure accounts appropriately

- ✓ Use the principle of 'least privilege'. Give trustees, staff and volunteers the lowest level of user rights required to perform their role, so if they are the victim of a phishing attack, the potential damage is reduced.
- ✓ Ensure users aren't logged on with Administrator privileges. Administrators can change security settings, install software and hardware, and access all files on the computer. An attacker having unauthorised access to an Administrator account can be far more damaging than accessing a standard user account
- ✓ Use two factor authentication (2FA) on your important accounts such as email. This means that even if an attacker knows your passwords, they still won't be able to access that account if someone has given away their password.
- ✓ Check what other security measures your tech providers offer e.g. Office 365 has features to detect spoof emails and e.g. quarantine them before reaching your inbox



# What is Malware?

- ✓ Malicious software that is designed to interfere with a computer's normal functioning and that can be used to obtain information and commit cybercrimes.
- ✓ **Ransomware** - a type of malware that makes data or systems unusable until the victim makes a payment



# NCSC's 5 tips to protect against malware

1. Use antivirus software on all computers
2. Patch all software and firmware
3. Control access to removable media
4. Switch on your firewall
5. Smartphone guidance



# Antivirus options

- ✓ Free or paid options – better to go with paid options (watch out for personal use vs organisational/business use criteria)



- ✓ [Security products catalogue](#) with discounts for registered charities including Bitdefender, Avast & Norton

- ✓ Alternatively purchase via e.g. Amazon
- ✓ Check pricing at point of renewal – it may be cheaper to rebuy the product



# Keep everything up to date

- ✓ Patch all software and firmware by promptly applying the latest software updates (don't ignore these!) provided by manufacturers and vendors
- ✓ This protects against identified vulnerabilities and is needed for PCs & laptops as well as mobile devices
- ✓ Use 'automatic update' options where available
- ✓ Be aware of software 'end of life' e.g. Windows & Office suites, where security updates are no longer provided



# Control software installation

- ✓ Only install approved software on tablets and smartphones from your relevant app stores
- ✓ Stop users from downloading third party apps from unknown sources
- ✓ Prevent users from routinely logging on with administrative privileges (limits potential damage malware can carry out)



## Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.



**Identify what needs to be backed up.** Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.



**Ensure the device containing your backup is not permanently connected** to the device holding the original copy, neither physically nor over a local network.



**Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

## Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.



**Switch on PIN/password protection/fingerprint recognition** for mobile devices.



Configure devices so that when lost or stolen they can be **tracked, remotely wiped** or **remotely locked**.



Keep your **devices** (and all **installed apps**) **up to date**, using the **'automatically update'** option if available.



When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.



**Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

## Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.



**Use antivirus software** on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.



**Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.



**Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.



**Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

## Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.



Ensure staff **don't browse the web** or **check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.



**Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).



Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

## 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.



# 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

Part of Kingston Voluntary Action – providing tech support to small local charities in London for 25 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

**PAUL FIRBY**

[paulfirby@superhighways.org.uk](mailto:paulfirby@superhighways.org.uk)

@SuperhighwaysUK

#DigitalFoundations