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 2025/26, what percentage of charities reported having a cyber security breach in the last 12 months?

12% 28% 57% 76%

28% - charities overall

Rising to 57% for charities with income over £500,000

Official Statistics

Cyber security breaches survey 2025/2026

Published 30 April 2026

Type	Businesses	Charities
Phishing attacks	88%	87%
People impersonating, in emails or online, organisation or staff	28%	26%
Devices targeted with malware (viruses/spyware)	16%	12%
Hacking or attempted hacking of online bank accounts	8%	4%
Denial of service attacks	6%	4%
Takeovers/attempts to take over website/social media accounts/email	5%	4%
Devices being targeted with ransomware	3%	3%
Unauthorised accessing of files/networks by staff, even if accidental	2%	2%
Unauthorised accessing of files/networks by people outside organisation (other than staff)	2%	1%
Unauthorised listening into video conferences or instant messaging*	0%	2%
Other types of cyber security breaches or attacks	4%	2%

Visit the full report

Why are charities at risk?

National Cyber Security Centre

Charities...	Hold funds 	Personal, financial and commercial data of interest or monetary value 	Data is sensitive, valuable and vulnerable to attack 
Impact... • Data gets lost 	You have to stop operations 	Financial/Time cost to recover 	Reputation 

Charities are often a target because they hold valuable data but have limited resources to protect it

How are charities being attacked?

- Business email attacks (phishing)

  Scam emails that ask people 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.

National Cyber Security Centre

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

[Download the full guide]

National Cyber Security Centre

Cyber Security

Small Business Guide

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**

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.
- 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.

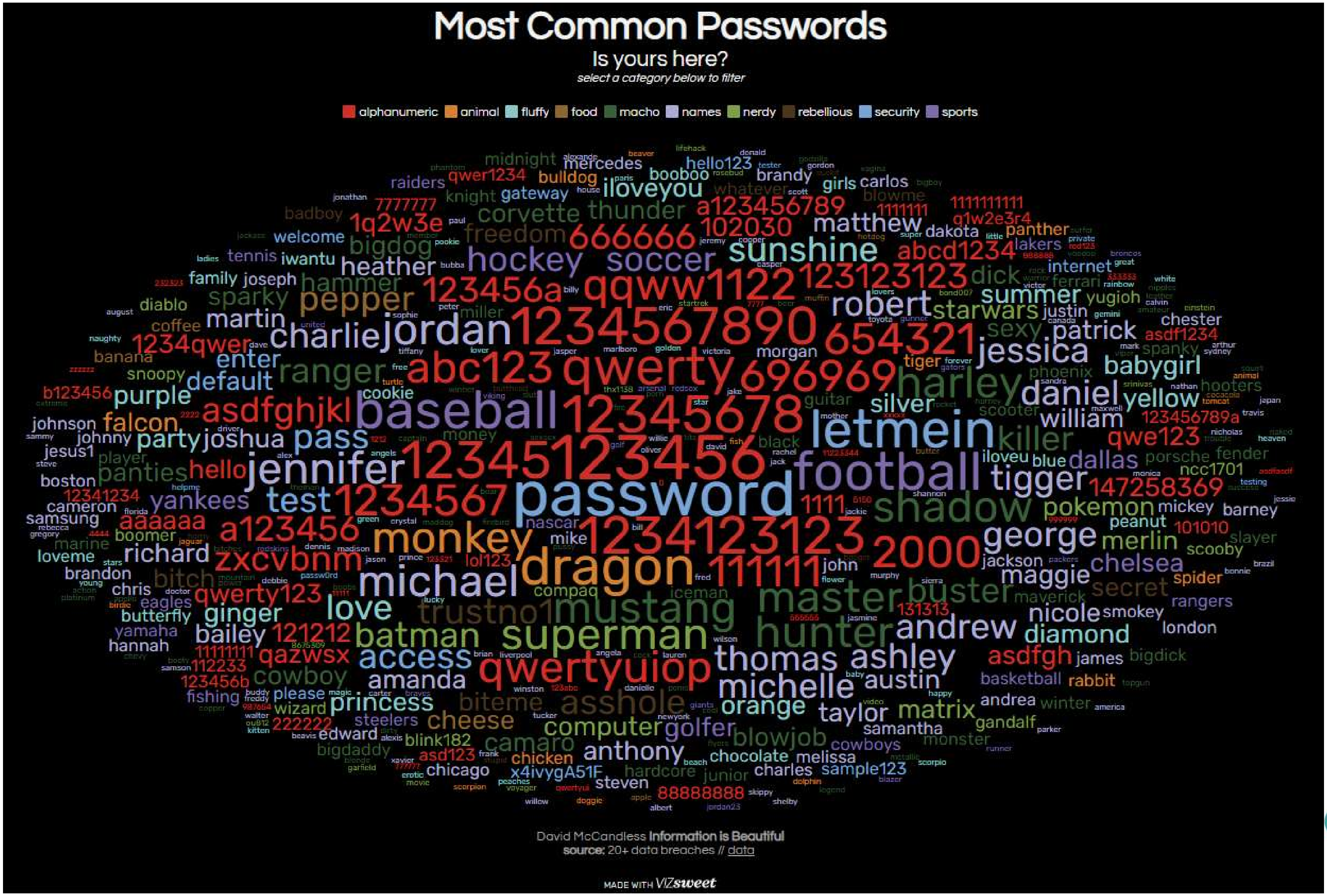
Passwords: protecting our accounts & devices

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

- ✓Phones
- ✓Tablets
- ✓PCs & laptops

But also

- ✓Firewalls
- ✓Routers
- ✓Servers



Most Common Passwords
Is yours here?
select a category below to filter
alphanumeric
animal
fluffy
food
macho
names
nerdy
rebellious
security
sports
1234567890
12345
123456
password
12345678
qwerty
abc123
baseball
football
letmein
1234567
dragon
monkey
1234123123
654321
696969
qqww1122
123123123
666666
111111
2000
michael
jennifer
jordan
mustang
superman
qwertyuiop
shadow
master
hunter
harley
jessica
robert
sunshine
soccer
hockey
charlie
batman
access
asdfghjkl
zxcvbnm
a123456
qwerty123
trustno1
asshole
michelle
thomas
ashley
andrew
george
tigger
killer
daniel
pass
test
love
David McCandless Information is Beautiful
source: 20+ data breaches // data
MADE WITH VIZsweet

Passwords: often the weakest link

How Secure is my password?

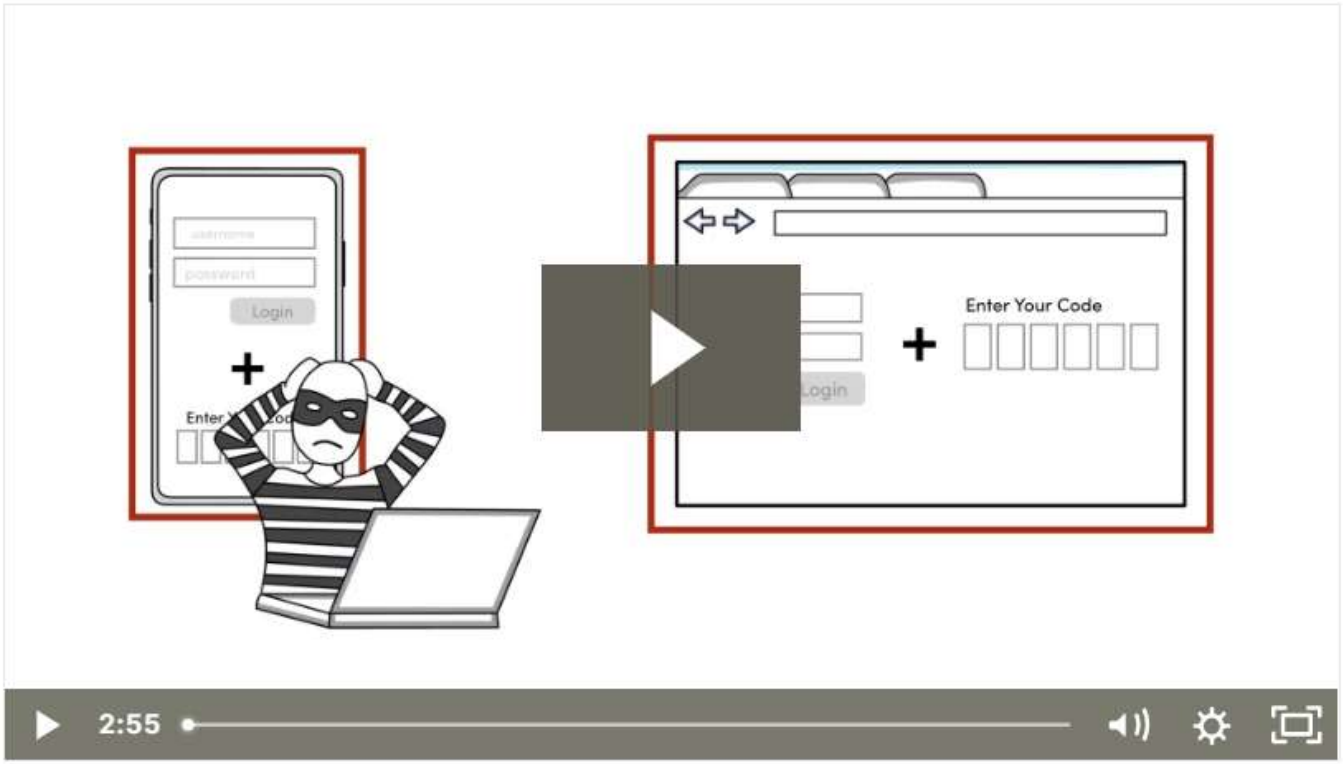
Password Tester | Test Your Password Strength | Bitwarden

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

- ✓It protects you even if your password is stolen
- ✓It significantly reduces the risk of account takeover
  - ✓Microsoft report it protects M365 accounts from over 99.999% of current attacks
- ✓It's quick and easy to use
  - ✓A small step that can protect your data and reputation

PINs and biometrics

- Switch on PIN / fingerprint /facial 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

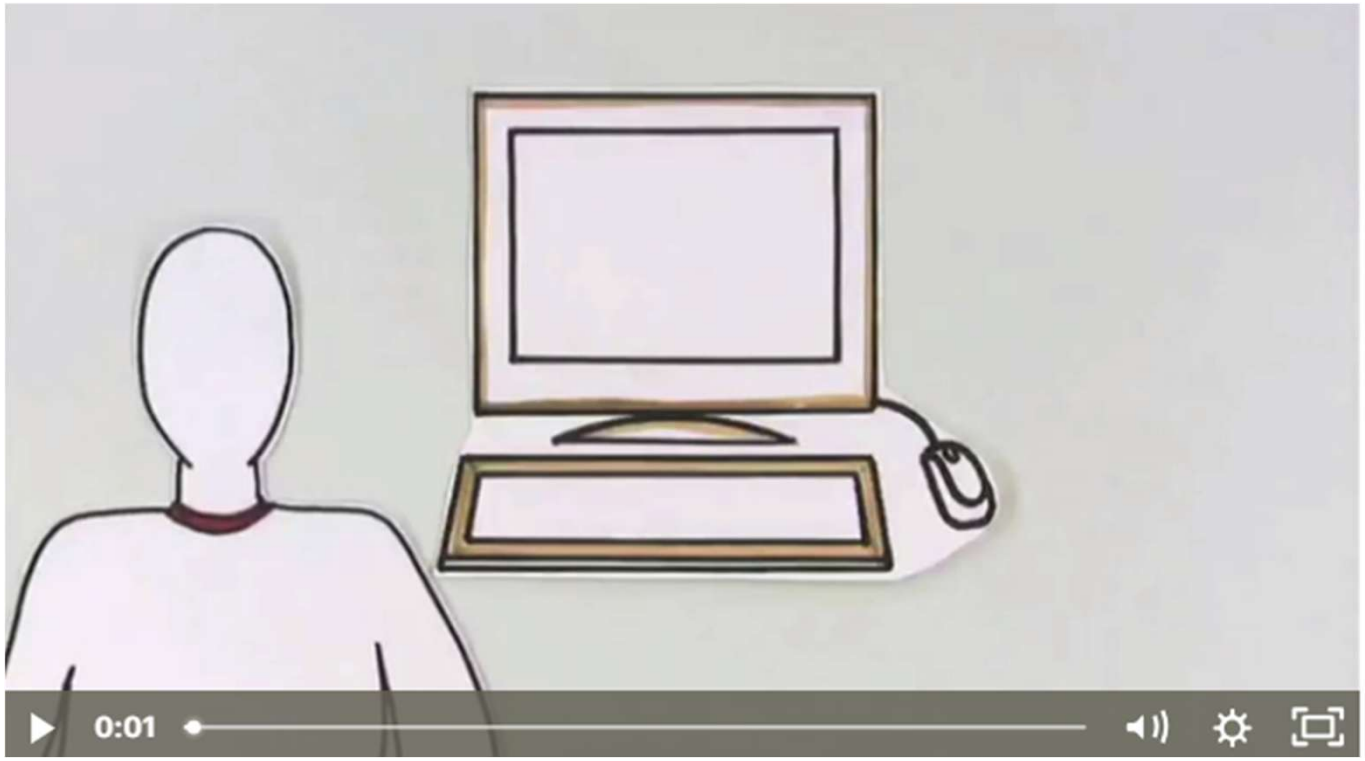
1. **Switch on password protection** - where this is not enabled by default
2. **Change all default passwords** – to mitigate against 'open door' access
3. **Avoid predictable passwords** – have an organisational password policy, implementing NCSC's 3 random words plus a number and symbol
4. **Use two 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?

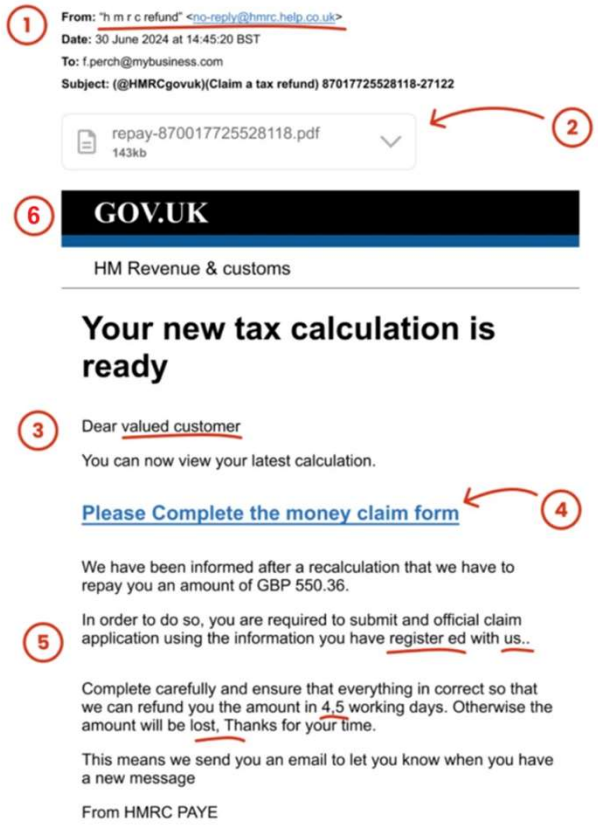
What is Phishing?

- ✓Phishing is when someone pretends to be a trusted organisation to trick you into sharing information
  - ✓By clicking a link or viewing a file
  - ✓Entering account details
  - ✓Entering a password
  - ✓Completing a form
- ✓This happens to organisations of all sizes
- ✓Most attacks rely on simple mistakes



Phishing video from CommonCraft

An example from the NSCS



1 **From:** "h m r c refund" <no-reply@hmrc.help.co.uk>
Date: 30 June 2024 at 14:45:20 BST
To: f.perch@mybusiness.com
Subject: (@HMRCgovuk)(Claim a tax refund) 87017725528118-27122

2 repay-870017725528118.pdf
143kb

6 GOV.UK

HM Revenue & customs

Your new tax calculation is ready

3 Dear valued customer

You can now view your latest calculation.

Please Complete the money claim form 4

We have been informed after a recalculation that we have to repay you an amount of GBP 550.36.

5 In order to do so, you are required to submit and official claim application using the information you have register ed with us..

Complete carefully and ensure that everything in correct so that we can refund you the amount in 4,5 working days. Otherwise the amount will be lost, Thanks for your time.

This means we send you an email to let you know when you have a new message

From HMRC PAYE

1. Misspelled email addresses
2. Unexpected attachments
3. Generic greetings
4. Links to unknown sites
5. Spelling and grammar mistakes
6. Poor quality / strange logos

Any doubts, call the organisation directly (don't use numbers from the email)

[Other examples at Which Consumer Rights News]

Spotting Phishing Emails

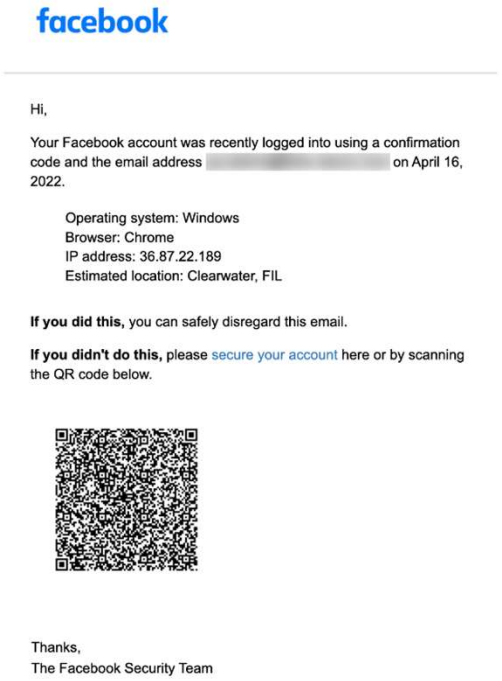
This was put together by a team from Google

[Jigsaw | Phishing Quiz]

And try this one which changes monthly

[Phish Me If You Can – Phishing Simulator]

Here’s two phishing examples



facebook

Hi,

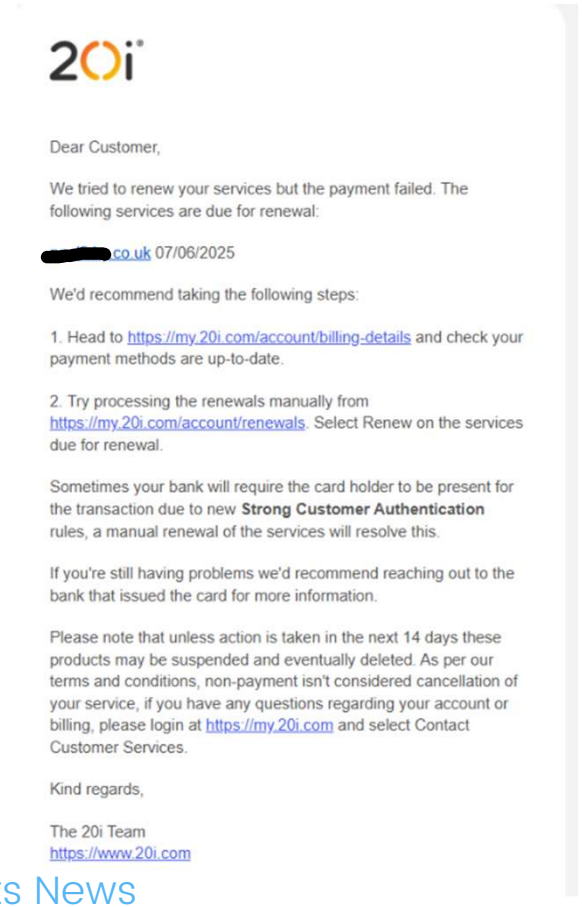
Your Facebook account was recently logged into using a confirmation code and the email address [redacted] on April 16, 2022.

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

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



20i

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

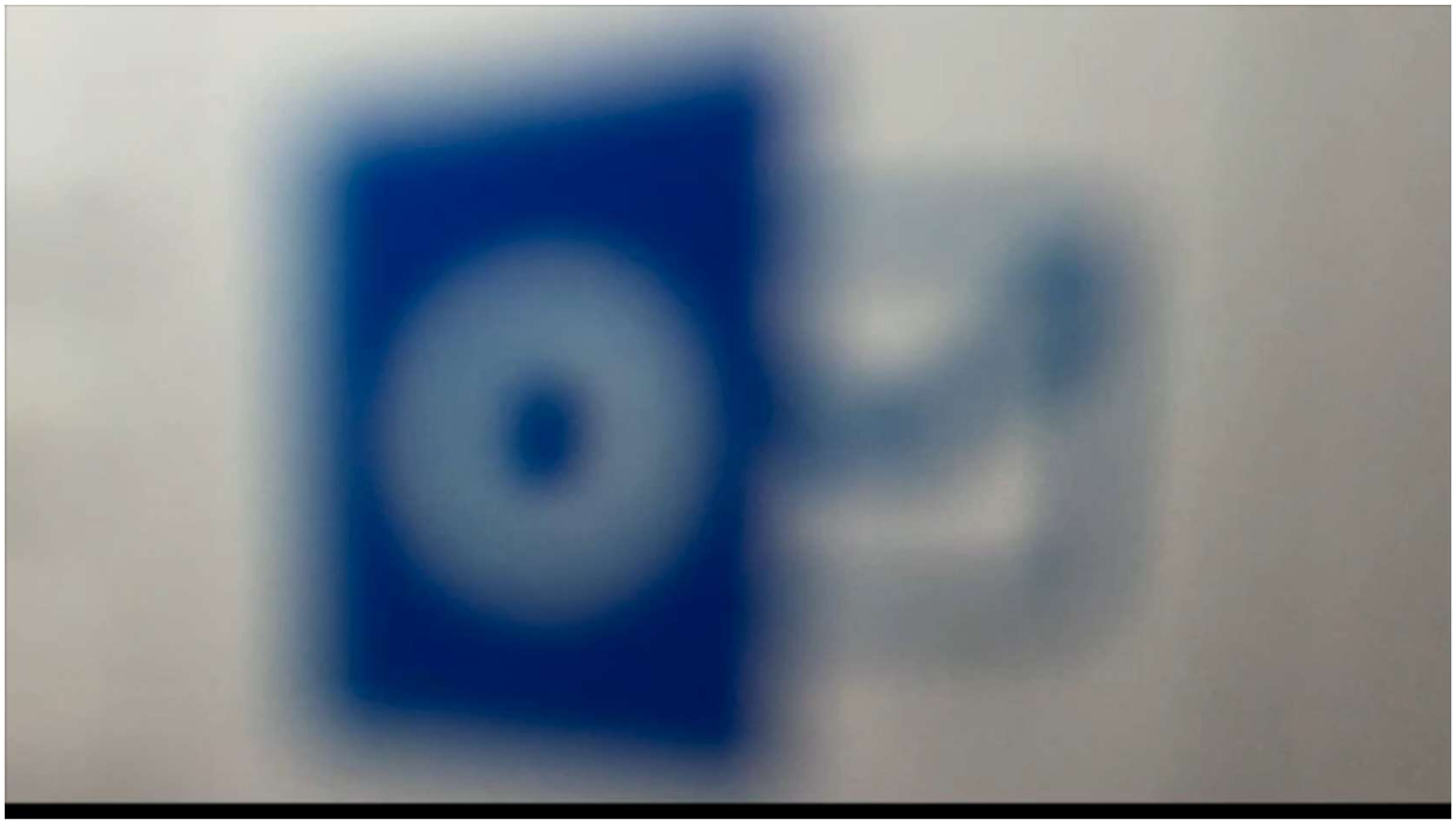
- ✓Attackers use publicly available information about your charity and staff to make their phishing messages more convincing, often gleaned from your website and social media accounts
- ✓What do visitors to your website and social media followers need to know, and what detail is unnecessary (but could 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:



https://youtu.be/TFlCLREWxfU

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)
  - ✓ 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

I'm pretty alert to scammers, I think I'm safe...

https://youtu.be/lc7scxvKQOo

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)

techsoup United Kingdom

- ✓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)

Control removable media

- ✓Control access to removable media such as memory cards and USB sticks
- ✓Consider disabling ports or limiting access to specific media (e.g. with shared PCs)
- ✓Encourage staff instead to transfer files via email or cloud storage

Switch on your firewall

- ✓Switch on your firewall to create a buffer zone between your network and the Internet
- ✓Included with most operating systems. If using Windows 10 or 11 follow these instructions to check if your firewall is on
- ✓If using a 3rd party anti-virus solution this might include an additional firewall

Mobile devices – what do you use?

- ✓Laptops
- ✓Desktop PCs
- ✓Smartphones
- ✓Tablets

- ✓Organisational devices

- ✓Personal devices

5 tips to keep mobile devices secure

Smartphones, tablets and laptops used outside the safety of the office and home need even more protection than 'desktop' equipment. The NCSC recommends you:

1. Switch on PIN /password protection / fingerprint recognition
2. Configure tracking on your devices
3. Keep devices up to date
4. Don't connect to public Wi-Fi hotspots
5. Replace older devices

Configure tracking on your devices

- Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked
  - For Android devices – find out how you can find, lock or erase here
  - For Apple devices – learn how to use the Find My service

- Remember if you are using cloud solutions e.g. Office 365 or Google Workspace – you'll have options to:
  - sign users out of devices
  - reset passwords / block future sign ins

Keep devices up to date

- Keep your devices (and all installed apps) up to date
- Don't ignore any update reminders!
- This protects against identified vulnerabilities and is needed for mobile devices as well as laptops & desktops
- Use 'automatic update' options where available – see further guidance from NCSC here
- Be aware of software 'end of life' e.g. Windows & Office suites, where security updates are no longer provided

Avoid using public Wi-Fi hotspots

- When sending sensitive data, don't connect to public Wi-Fi hotspots
- Instead use 3G, 4G or 5G connections (including tethering or hotspotting to your phone and wireless dongles) or use VPN's
- Read our Using public Wi-Fi securely guide

Replace older devices

- Replace older devices as these are more vulnerable to cyber attacks
- Cyber Essentials accreditation relies on confirmation that older devices using End of Life (EOL) operating systems that are out of regular support are not being used
  - These include Windows XP/Vista/Server 2003/Server 2012(as of Oct 2023), Mac OS Mojave, iOS 12, iOS 13, Android 8

Backing up your data:

- ✓ Why you need to back up your data
- ✓ Best practice when backing your data
- ✓ Different back up options
- ✓ How to use version history functions to restore individual files to previous saved versions

Why do we need to back up our data?

Quick small group conversations

- ✓Have you ever lost data?
- ✓How did this happen? What was the consequences?

Some common scenarios:

- ✓Lost or stolen device
- ✓Accidental deletion
- ✓Hard disk failure
- ✓Ransomware attacks
- ✓Fire or flood

NCSC's 4 tips re backups

1. Take regular backups (& check you can restore)
2. Identify what data needs to be backed up
3. Ensure backup devices are NOT permanently connected to your network
4. Consider backing up to the cloud – see https://www.ncsc.gov.uk/collection/cloud

Backup options

- ✓Floppy disks & tape machines (the old days!)
- ✓Memory sticks (make sure these are encrypted)
- ✓External hard drives (don't keep connected to your system)
- ✓In platform back up (included as part of the programme – check the specifics e.g. how far you can go back)
- ✓Cloud back up - see guidance https://www.ncsc.gov.uk/collection/cloud

Restoring your data

- ✓Check you know how to restore data
- ✓Check restoring data works (and that the backups have been working!)
- ✓Check what can be restored e.g. is it whole folders rather than individual files?
- ✓How far back can you go e.g. does your backup allow you to go back to last week, last month or a particular day?

What data do you need to back up and what systems are you using?

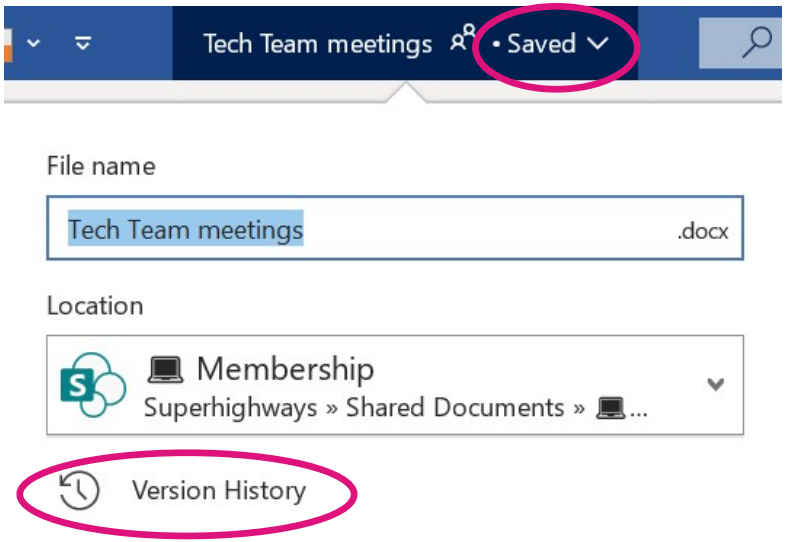
Data	Where stored	How backed up
Files	Office 365 – SharePoint & Teams	Office 365 back up
Emails	Office 365 - Outlook	Office 365 back up
Database	AIDE	AIDE do a backup
Photos	Teams	Office 365 back up
Website	Voice platform	Voice back up (versioning for each page - need to check how far back whole site back up goes)

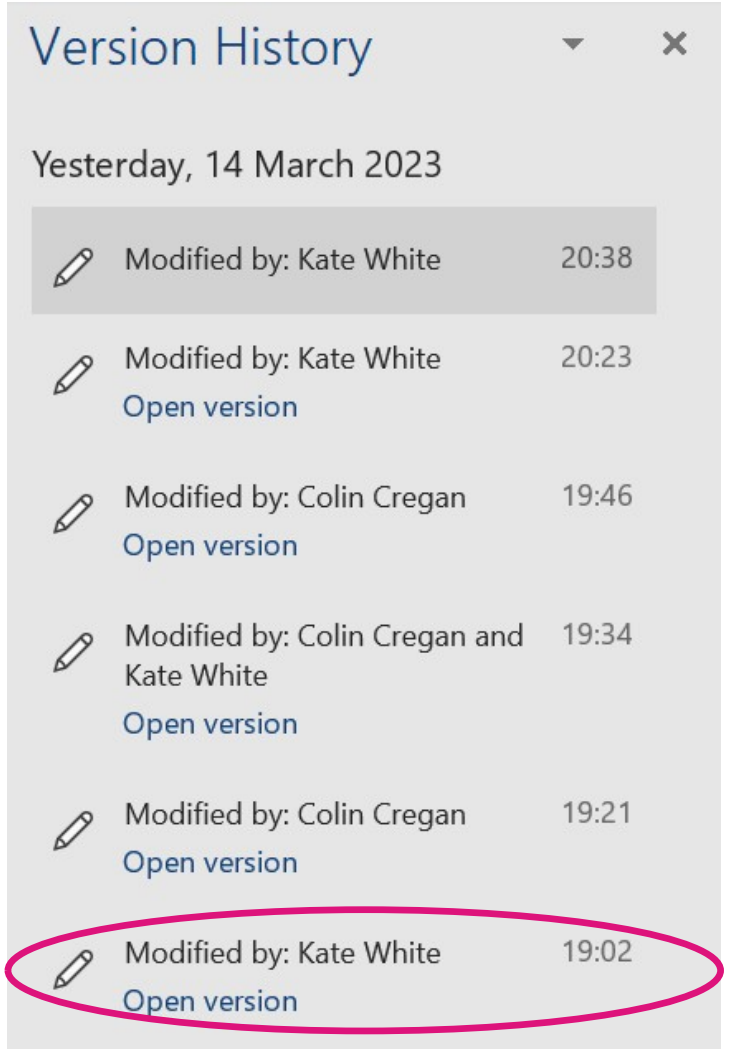
Backup devices not permanently connected

- ✓In office – best practice to take physical devices off site (minimises risk of e.g. fire, flooding etc)

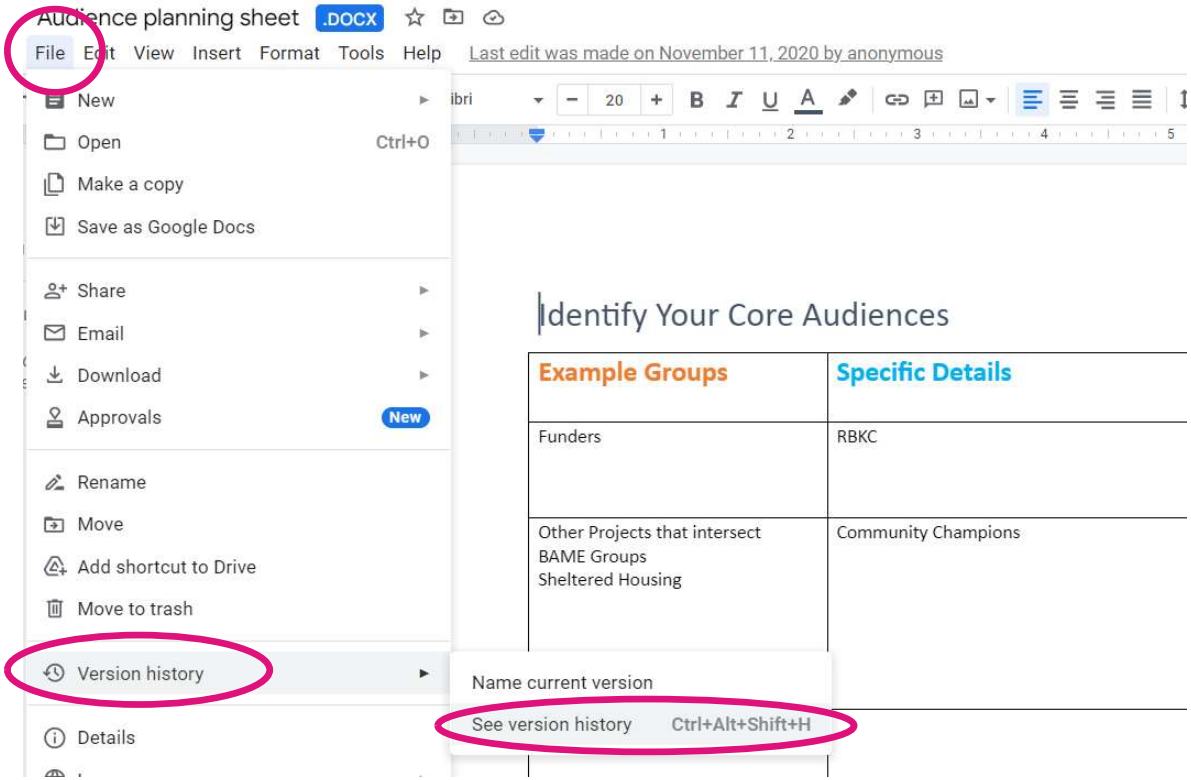
- ✓Important to not leave a backup device permanently connected e.g. an external hard disk to mitigate risks of a virus spreading from your system to the backup and then corrupting this, especially if Ransomware

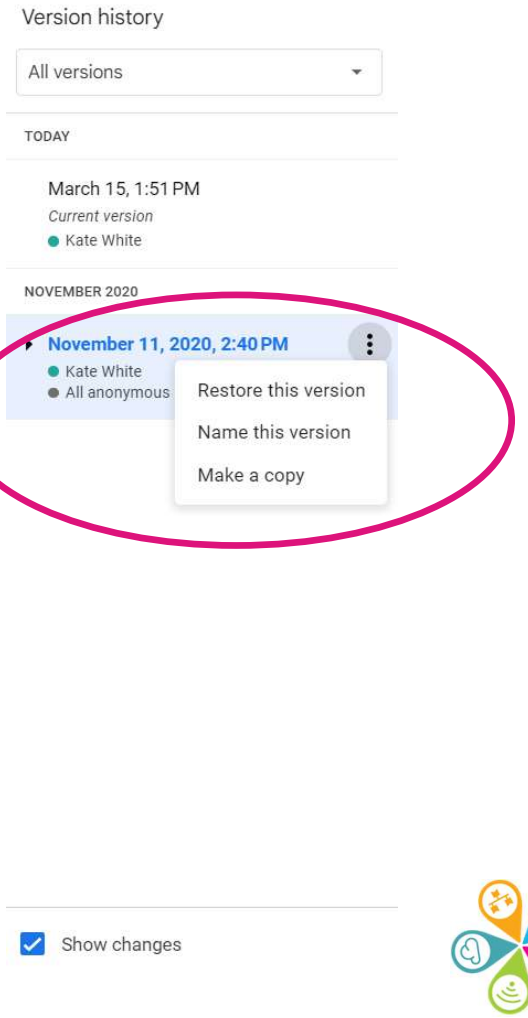
Office 365


Tech Team meetings
• Saved
File name
Tech Team meetings
.docx
Location
Membership
Superhighways » Shared Documents » ...
Version History


Version History
Yesterday, 14 March 2023
Modified by: Kate White 20:38
Modified by: Kate White 20:23
Open version
Modified by: Colin Cregan 19:46
Open version
Modified by: Colin Cregan and Kate White 19:34
Open version
Modified by: Colin Cregan 19:21
Open version
Modified by: Kate White 19:02
Open version

Google Drive





National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities 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/charity** .

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
@SuperhighwaysUK

#DigitalFoundations