

# Protecting you and your organisation from fraud & cyber crime

---

**Chen TSUI**

Cyber Prevent & Protect Officer  
Serious Fraud & Cyber Unit  
Hertfordshire Constabulary

**Email: [hertscyberprotect@herts.police.uk](mailto:hertscyberprotect@herts.police.uk)**

# Cyber attack: Data from charities stolen in ransomware attack

17 April 2023

## Top UK charities hit by major hack attack on data firm

**Ransomware costs £95,000**

Basic cybersecurity hygiene measures could have helped prevent ransomware attack, says Edinburgh Festival Fringe boss at Glasgow event

Leading UK charities – including the RSPCA, Dogs Trust, Battersea Dogs & Cats Home and Friends of the Earth – have been caught up in a major cyber attack on a third-party supplier, putting hundreds of thousands of supporters at risk.

A hospice in the West Midlands experienced a Business Email Compromise attack, resulting in a financial loss of **£17,000** fraudulent transfers, which represented a significant proportion of their operating budget, impacting their ability to provide essential services to patients.

hackers  
ata on  
rname,  
the affected  
started emailing victims to warn them of the breach.

# Why charities are at risk from fraud & cyber crime?

**Many charities use digital systems such as computers and the internet to:**

- store sensitive data about employees, volunteers, donors and beneficiaries
- use online banking
- deliver online services
- fundraise online

# Why charities are at risk from fraud & cyber crime?

- High volume of staff who work part time, including volunteers, and so might have less capacity to absorb security procedures.
- Staff using personal IT / BYOD (Bring Your Own Device) which is less easy to secure and manage than centrally issued IT.
- Impact of any cyber attack on a charity might be particularly high as charities often have limited funds and minimal insurance coverage.

# A sector under siege

**32%** of UK charities have reported a cyber security breach or attack in the last 12 months.

**38%** of them directly impacted service delivery, with 19% leading to negative outcomes for those the charity serves.

**26%** of charities have conducted cyber security risk assessments in 2023, highlighting a significant gap in preparedness.

# Between Nov 2023 – Oct 2024

The Charity Commission:

- opened 603 cases relating to fraud,
- has 99 cases relating to cyber crime issues in the last year, and
- has identified that the most common type of cyber-enabled fraud experienced by charities is phishing attempts.

# Will 2025 be worse?

Several converging factors point to an escalation of the cyber threat to charities in 2025:

- **AI-powered attacks**: lower barrier of entry for criminals
- **Geopolitical instability**: global tensions and conflicts
- **Increased regulatory scrutiny**: tightened data protection regulations
- **The evolving threat landscape**: new attack vectors/emerging threats
- **Economic pressures**: funding cuts, increased demands on services

# Estimated cost of global cyber crime in 2025

**Expected to cost \$10.5 trillion annually by 2025**

(Source: World Economic Forum)

**If cyber crime were a country, it would have the third largest Gross Domestic Product worldwide**

Rank	Country	GDP in trillions
1	United States	\$28.78
2	China	\$18.53
3	<b>Cybercrime</b>	<b>\$10.5</b>
4	Germany	\$4.59
5	Japan	\$4.11
6	India	\$3.94
7	United Kingdom	\$3.5
8	France	\$3.13



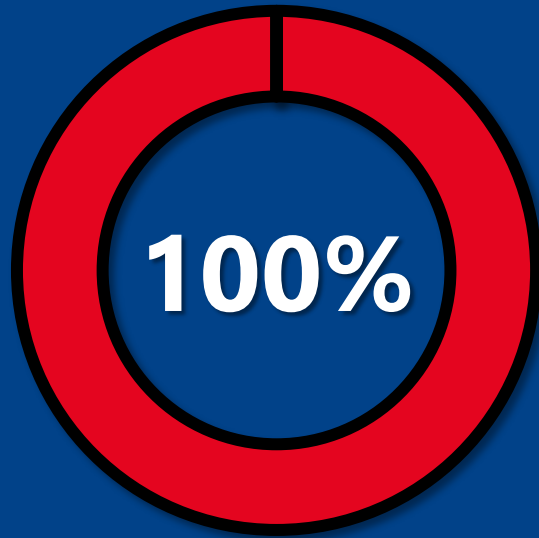
HERTFORDSHIRE

CONSTABULARY

**Pre**vention First



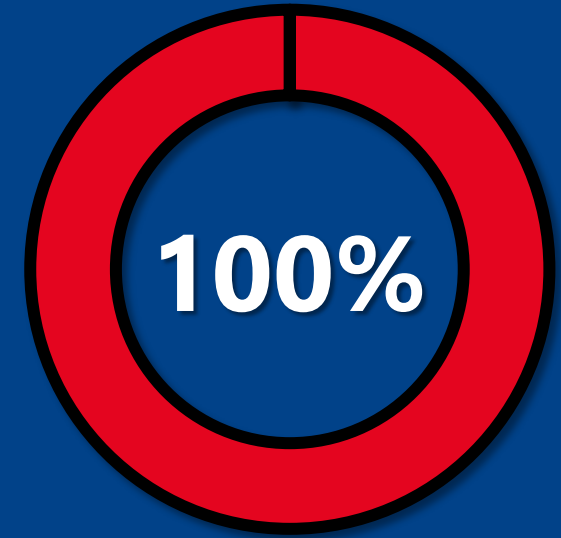
# Key Findings



**Hackers hack first,  
*ask questions* demand  
later.**



**Hacking is on the  
rise.**



**Common  
misconception that  
cyber attacks are only  
a "big brands"  
problem.**

# Protecting your charity is a team sport!

**Cyber-attacks can have a huge impact on your charity.**

A charity could lose money, sensitive data, and/or damage its reputation.

Simple measures can be put in place to protect your charity.

**Staff, management, trustees** must:

1. be aware of the risks to your charity from cybercrime,
2. take reasonable steps to protect your charity from cyber crime, and
3. respond to cyber-attacks properly to reduce the harm to your charity.

# Fraud and cyber crime guidance available

The Charity Commission published a bespoke guidance on how to protect your charity from cyber crime, and a guide on fraud last November 2024.

It sets out the importance of:

1. establishing an internal culture of fraud and cybercrime awareness,
2. links to free online training modules,
3. respond to cyber-attacks, and
4. report fraud and cyber crime.



# NCSC resources

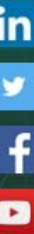
**Small Charity Guide** and the dedicated information for **small & medium sized organisations** provides you with:

- guidance about how to improve cyber security
- prepare their response, and
- plan their recovery to a cyber incident.
- [www.ncsc.gov.uk](https://www.ncsc.gov.uk)

The screenshot displays the NCSC website interface. At the top, the NCSC logo and navigation links (ABOUT NCSC, CISP, REPORT AN INCIDENT, CONTACT US) are visible. Below the main navigation bar, the 'Information for...' section is active, showing a grid of categories: Individuals & families, Self employed & sole traders, Small & medium sized organisations (highlighted), Large organisations, Public sector, and Cyber security professionals. The 'Small & medium sized organisations' page is shown, featuring the NCSC logo and the title 'Cyber Security: Small Charity Guide'. The subtitle reads: 'How to improve cyber security within your charity - quickly, easily and at low cost.' Below the text, there are illustrations of a smartphone, a laptop, and a person sitting at a desk.

# Providing Cyber Security & Resilience Guidance for Businesses Of All Sizes

We exist to support and protect businesses and third sector organisations in the region against cyber-crime.



[www.ecrcentre.co.uk](http://www.ecrcentre.co.uk)

A police-led initiative, provides some specialist cyber services to organisations to aid in their protection against fraud and cybercrime.

**FREE membership** provides practical advice on building your cyber resilience.



## WELCOME TO POLICE CYBERALARM

Helping organisations monitor and report the malicious activity they face from the internet



[www.cyberalarm.police.uk](http://www.cyberalarm.police.uk)

A **FREE monitoring tool** that helps identify suspicious activity entering your network and highlight some of your potential vulnerabilities online.

Its purpose is limited to monitoring, rather than active defence, to support you in protecting your personal data, trade secrets, and intellectual property, all of which are valuable target assets for cyber criminals.

# Training by your local Cyber Protect Officers

- Bespoke training, approximately 90-120 minutes
- In-person / over Ms Teams
- General cyber security and fraud awareness training
- Exercising your incident response plan

**Talk to us! Email us at [HertsCyberProtect@herts.police.uk](mailto:HertsCyberProtect@herts.police.uk)**

# Preview of our training



# Social engineering

Criminals attempt to trick users into doing '*the wrong thing*'.

Scam messaging typically:

1. are from an **authority / organisation / person you heard of.**
2. appeal to your **emotions.**
3. have a sense of **urgency.**
4. are topical / current **events.**

email/online  
'Phishing'



text  
'SMShing'



phone  
'Vishing'





# Employees will fall for phishing

- **1 in 3** employees are likely to click the links in phishing emails.
- **1 in 8** employees are likely to share information requested in a phishing email.
- **60%** of employees opened emails they weren't fully confident were safe.
- **45%** click emails they consider to be suspicious "just in case it's important."

Source: Verizon






HERTFORDSHIRE


CONSTABULARY

**Pre**vention First

# Phishing Emails

22:11

 63

 Apple Security

Wednesday  
3 July 2024

**Important notice. Your device is currently infected with a Trojan virus!**


Your phone's memory is already having 17% of damage. Prompt action is required, otherwise, the device will become defective and all your data including **accounts, photos and payment data will be available to third parties.**

**Immediately install trusted free app from AppStore to remove the virus and secure your device.**

0 minutes 44 seconds


[Remove Virus](#)


## Delayed Parcel delivery



Over £4,000,000 in Offers given out so far!

Survey About




2024 

Dear Asda Shopper,

We would like to offer you a unique opportunity to receive a brand new **Tupperware 36-piece set!** To claim, simply take this short survey about your experience with Asda.

**Attention!** This survey offer expires today

[START SURVEY](#)



Dear ,

We attempted to contact you recently but couldn't get through. It seems the phone number we have outdated.

continue  
important updates  
count, please  
late your contact  
specially your  
r.

# Phishing

- Emails sent en masse

# Spear Phishing

- Personalised to their targets

# Whaling

- Targets high-level decision makers

**Emails you receive may contain:**

- attachments or
- links you are asked to click on.

**Don't click on links unless you can verify where they came from. Call the sender to check it's genuine. If in doubt, keep them out.**

# Change our attitudes to data privacy, especially on social media



Watch this video: <https://youtu.be/yrjT8m0hcKU?feature=shared>



# Scam Ads & V

**Important: Vehicle Tax payments must be update and action is required now**

**GOV.UK**

Welcome,

Our records show that you are overdue on your vehicle tax.

This is your urgent reminder.

Your vehicle is not legally permitted to be on the road without tax.

Please complete the form below to ensure compliance with DVLA regulations.

**START NOW**

Louisa's Tips  
Sponsored •

**Enter your  
DOB and we'll  
check if Black  
Horse owe you  
£5,318.25**



DD

MM

YYYY

**FREE CHECK**

## Blackhorse Is Refunding!

Enter your DOB and we'll check for free if you're owed £1000s!

Did you take out a car finance agreement (PCP/ HP) between the years of 2007-2021? If you did, you could be owed £5,318.25 per agreement.

Use the FREE check below to see if you're owed a refund, it takes less than 30 seconds

Ad relates to mis-sold car finance\*

Dear Customer, Due to the closure of our physical stores, to facilitate inventory clearance at these locations, we are offering an 80% online promotional discount. This week only. All inventory must go! Quantities are limited. Get it now before it's out of stock!



DDIXV.TOP

Direct clearance from the store, discount up to 80%

Best Selling

**Shop now**



**Stop and think before you  
post, click and link!**



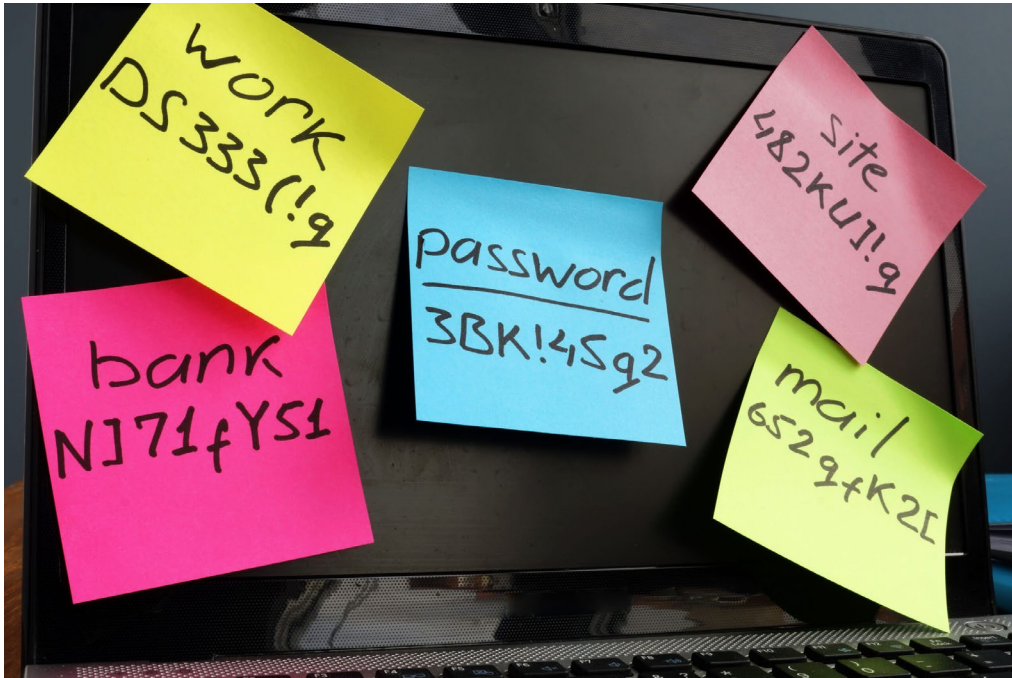


# Protect yourself



**How many keys do you have?**

# Most common passwords 2024



1. 123456 – used 4.5 million times!
2. admin
3. 12345678
4. 123456789
5. 1234
6. 12345
7. password
8. 123
9. Aa123456
10. 1234567890

# Create a strong password using 'Three Random Words'

Strength of the password:	Examples of passwords:	How long it takes for a computer to guess the password:
Very, very weak	blue	Less than a second
Very weak	waterblue	13 seconds
Weak	blueredgreen	2 minutes
A bit stronger	waterbluechair	12 hours
Strong	water!bluEchAir5	A few months/years



# Turn on your **2FA** (2-Factor Authentication) or **2SV** (2-Step Verification)



Something  
you know



Something  
you have or are



If both correct,  
then access is  
granted



# Have your emails ever been in a data breach?

You can check using  
[www.haveibeenpwned.com](https://www.haveibeenpwned.com)

The screenshot shows the homepage of the 'Have I Been Pwned' website. At the top is a navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is a large rounded rectangle containing the text '';--have i been pwned?'. Below this is a subtitle: 'Check if your email or phone is in a data breach'. A search bar is positioned below the subtitle, with the placeholder text 'email or phone (international format)' and a 'pwned?' button. Below the search bar is a section for password generation, featuring an information icon, the text 'Generate secure, unique passwords for every account', a link to 'Learn more at 1Password.com', and a link to 'Why 1Password?'. The bottom section displays statistics: 521 pwned websites, 11,145,906,797 pwned accounts, 114,031 pastes, and 199,732,579 paste accounts. It also lists 'Largest breaches' and 'Recently added breaches' with icons and links to specific breach data.

Category	Count	Item
pwned websites	521	
pwned accounts	11,145,906,797	
pastes	114,031	
paste accounts	199,732,579	

Largest breaches	
772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts

Recently added breaches	
509,458,528	Facebook accounts
11,498,146	Unverified Data Source accounts
297,744	Carding Mafia accounts
11,788	WeLeakInfo accounts
465,141	Liker accounts
637,279	Travel Oklahoma accounts
66,521	Gab accounts

# Protect against malware

Malicious software: ransomware, viruses, spyware and more.

Aim: steal data and damage or destroy computers and computer systems.

- Beware of links and attachments in messaging.
- Update your operating system.
- Make sure your antivirus product is turned on and is up-to-date.
- Switch on your firewall.



# Back-up data

Make copies of things that are important including emails, invoices, contacts, and orders.

Making regular back-ups to multiple external locations and keep them somewhere physically separate.

- separate hard drives or computer
- thumb drives/memory stick
- cloud





# Keeping devices up-to-date

**Patching** – any device needs regular maintenance and servicing to ensure they work effectively and securely.

**End of support/life** - hardware and software have reached a point where they're no longer usable.



# Keep devices safe

Store away your devices when not in use, especially if you use them for both business and personal work.

Web-based tools to enable you:

- switch on password protection.
- use an encryption product.
- track the location of the device.
- lock it remotely.
- erase data remotely.
- retrieve a backup of data stored on the device.



# Be mindful of Artificial Intelligence



**Please do not let AI systems  
teach you how to set up a  
camp site....**

**or how to do your job!**



# Charity AI Task Force to bring third sector up to speed

FEBRUARY 17, 2025 11:54 AM



**An AI ‘charity task force’ has been launched to champion the responsible, inclusive and collaborative use of the technology across the social sector amid fears that charities are being left behind in the AI race.**

Created through a collaboration between the Centre for the Acceleration of Social Technology (CAST), and AI consultancy Zoe Amar Digital, the Charity AI Task Force has been backed by more than 20 member organisations, including The National Lottery Community Fund, King’s College London, The Prince’s Foundation, Wales, Shelter, and Charity Digital.

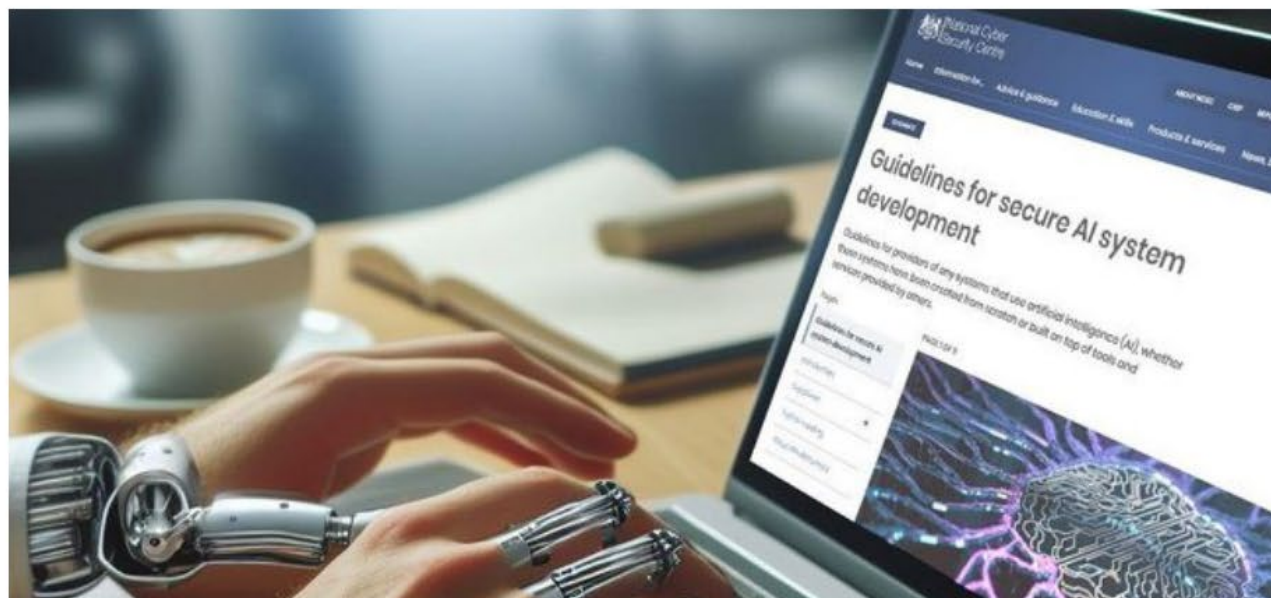
**51% of people working in the Charities sector said that their organisation was providing no AI training.**



## GUIDANCE

# AI and cyber security: what you need to know

Understanding the risks – and benefits – of using AI tools.

[Download / Print Article PDF](#)[Share](#)**PUBLISHED**

13 February 2024

**REVIEWED**

13 February 2024

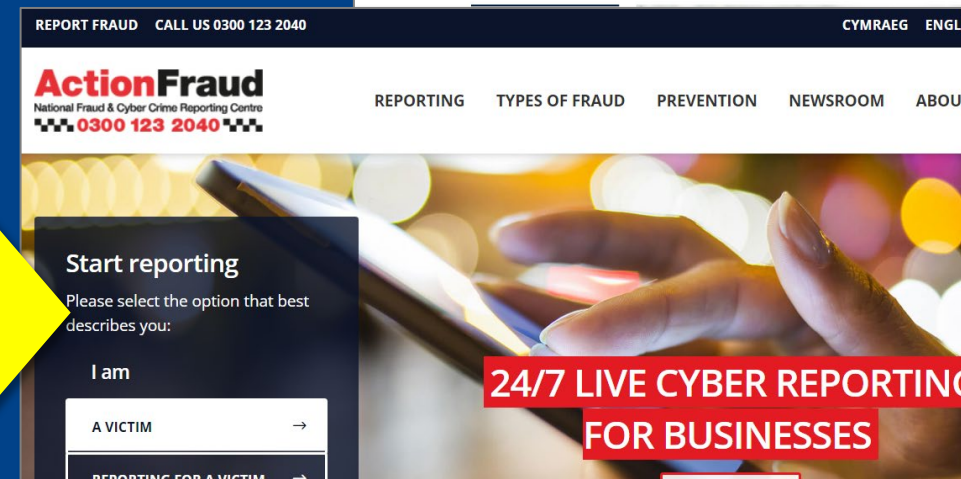
**VERSION**

# Always report scam emails, texts, websites, adverts & phone calls

Visit: [www.ncsc.gov.uk/report-scam-website](http://www.ncsc.gov.uk/report-scam-website) or [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

- Forward suspicious emails to [report@phishing.gov.uk](mailto:report@phishing.gov.uk)
- Forward scam texts to **7726**  
(handy tip: 7726 spells out SPAM on a phone keypad)
- Report suspicious phone calls: **text 7726** with the word 'Call', followed by the scam caller's number
- Report fake/scam websites, and adverts:  
<http://ncsc.gov.uk/report-scam-website>

If you have lost money or responded to a suspicious email, phone call, message, social media advert or website, please report to Action Fraud by calling 0300 123 2040 or report the fraud online: [www.actionfraud.police.uk](http://www.actionfraud.police.uk)





# Report attempted & actual fraud and cybercrime

- Report to **Action Fraud** and the **Charity Commission**.
- Action Fraud is the only national reporting centre for fraud and cybercrime in the UK.
- Keep copies of / photos when reporting:
  - Logs (server / access / email)
  - Email headers
  - Any related documents
  - Keep forwarding rules
- **Action Fraud does not investigate.**
- **NFIB assesses every report for lines of enquiry and tasks out to relevant Police force.**

**Action Fraud**  
National Fraud & Cyber Crime Reporting Centre  
0300 1 2040

National Fraud  
Intelligence Bureau



HERTFORDSHIRE  
CONSTABULARY

**Prevention** First



# Reporting a live cyber attack

**If you are a business, charity or other organisation which is currently suffering a live cyber attack (in progress)**

- **Call Action Fraud immediately on 0300 123 2040**
- **Consider reporting to the Information Commissioner's office (ICO)**

**(Under GDPR rules it is mandatory that you report data breaches to the ICO within 72 hours)**



# Cyber crime & fraud prevention events at libraries

**Everyone is welcome!**

- **Borehamwood** - Wednesday 12th March 2025
- **Bishop's Stortford** – Wednesday 23rd April 2025
- **Stevenage** – Monday 12th May 2025
- **Watford** - Wednesday 4th June 2025
- **Ware** – Monday 14th July 2025

**More dates and venues (libraries) to be announced in the summer.**



HERTFORDSHIRE

CONSTABULARY

**Prevention** First

**Cyber & Fraud Aware?**

**Stay safe & secure online**

**All day drop-in** with cyber & fraud crime prevention experts to answer your questions.

- Password & 2-step verification
- Phishing and social engineering
- Phone, email, text scams and other top tips

**Our Cybercrime & Fraud Prevention events are coming to a library near you. Search 'cybercrime' on [www.hertfordshire.gov.uk/libraries](http://www.hertfordshire.gov.uk/libraries)**

**FREE event**  
No tickets or booking required

**Cyber Aware** **Action Fraud** **Prevention First** **beacon**

[www.hertfordshire.gov.uk/libraries](http://www.hertfordshire.gov.uk/libraries) Further details 0300 123 4049

**Hertfordshire**