Your guide to online safety

Edition 1 - February 2026

By Joshua Russell

clearcommunityweb

MOPAC | MAYOR OF LONDON

NEIGHBOURHOOD WATCH

Welcome

Welcome to the first edition of Community Cyber-Shield, a newsletter crammed full of practical advice, reviews and resources to help our community feel safer online and be more awareness to look out for the people we are close to.

For many people this can feel like an overwhelming subject with no end in sight. It also feels like a world for those who can rather than those who can't yet, as our world increasingly is online.

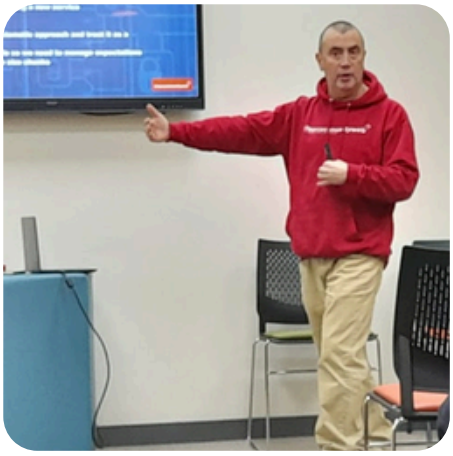
We must find ways in which we can participate safely, and importantly, be mindful of those needing a little more support.

This is where you come in. Our belief at ClearCommunityWeb is that a community focussed approach is what will keep us safer, by understanding what to so in a crisis and being there for people to help answer fundamental questions and to be open to learn something along the way.

What you see compiled here is a combination of subjects discussed through community events as well as the diligent research and insight from our Digital Ambassador, Joshua Russell, who has curated this for you.

Read, learn, share

Joshua Russell
Researcher and Writer



Caspar Kennerdale
Editor

clearcommunityweb

MOPAC | MAYOR OF LONDON

Cyber-News

Elon Musk's AI Grok under fire after being used to create fake sexualised images of children

January 2026

Elon Musk's Grok, an AI assistant that can be accessed via his social media platform, X (formerly known as Twitter), has faced a variety of controversy, including being rigged by Elon to have a right leaning mindset, praising Naziism, as well as several completely plain incorrect statements such as that second hand smoke exposure "isn't real" and former First Lady Michelle Obama is a man. Its latest controversy is that it is being used to generate deepfake (realistic, AI-generated media) sexualised images of real people. Users send real images of people and tell Grok remove their clothes and replace them with lingerie or bikinis. Grok is restricted from making people outright naked, but users can request that the clothes are replaced with strings or dental floss.

A large proportion of the people being targeted are young women including the Stranger Things star, Millie Bobby Brown and Ashley St. Clair, a conservative influencer and one of Musk's 4 baby mothers. When the latter posted online to complain about the images, a flood of people she called "Elon acolytes" responded that if she didn't like being undressed by Grok, she should simply log off. Various female victims have described feeling violated and dehumanised. Women's rights campaigners, including Refuge, Women's Aid and Womankind Worldwide, have said they are "deeply concerned" by the reports and that there are "dangerous" consequences for women and girls, including to their safety and mental health.

Elon and X's response to this have been mostly two-faced. He's stated on X that "Anyone using Grok to make illegal content will suffer the same consequences as if they upload illegal content", but simultaneously re-shared generated images, mostly of young, thin women in revealing outfits. X has said it acts against illegal content, including child sexual abuse material, "by removing it, permanently suspending accounts, and working with local governments and law enforcement as necessary" but still many women report their photos are still on the site.

The UK Government and Ofcom have called on Musk and X to deal with the situation. Ofcom said it had made "urgent contact" with Elon Musk's company xAI and said it was investigating concerns Grok has been producing "undressed images" of people. Liz Kendall, the Technology Secretary, has endorsed the regulator's actions, saying "It is absolutely right that Ofcom is looking into this as a matter of urgency and it has my full backing to take any enforcement action it deems necessary."

Sources:

BBC News - Elon Musk's Grok AI image editing limited to paid users after deepfakes

BBC News - Government demands Musk's X deals with 'appalling' Grok AI

Washington Post - X users tell Grok to undress women and girls in photos. It's saying yes.

Cyber-News

New cyber security law proposed to Parliament

January 2026

Hospitals, energy and water supplies and transport networks would be better protected from the threat of cyber-attacks under new laws that were introduced in Parliament on 12th November. The law, put forward by Science Secretary, Liz Kendall, comes after independent research revealed that shows the average cost of a significant cyber-attack in the UK is now over £190,000. This amounts to around £14.7 billion a year across the economy - equivalent to 0.5% of the UK's GDP.

Additionally, The Office for Budget Responsibility has warned that a cyber attack on critical national infrastructure could temporarily increase borrowing by over £30bn – the equivalent of 1.1 per cent of the UK's GDP. Therefore, it's a no brainer that the security problem needs solving.

The proposed bill, named "**The Cyber Security and Resilience Bill**" would extend cyber security regulation to key digital and essential services such as healthcare, transport, energy, and water, including medium and large IT and cyber security suppliers for the first time. These organisations would be required to meet clear security standards, report serious cyber incidents quickly, and have strong plans in place to manage attacks.

Regulators would gain new powers to designate critical suppliers and enforce minimum security requirements across supply chains, backed by tougher, turnover-based penalties for serious breaches. The Technology Secretary would also be able to direct regulators and essential service providers to take proportionate action to prevent cyber threats that could affect UK national security.

The bill has received backing from many senior officials including National Cyber Security Centre CEO Dr Richard Horne, National Chief Information Security Officer for Health and Care at Department of Health & Social Care, Phil Huggins and Simon Sheeran, Head of Cyber Security Oversight at the UK Civil Aviation Authority, who've praised it as "a crucial step in better protecting our most critical services", "(provide the ability to) help keep services available, protect data, and maintain trust in our systems in the face of an evolving threat landscape" and "This Bill will help improve cyber defences essential for maintaining the already very high safety standards in aviation".

Sources:
Gov.uk - Press release Tough new laws to strengthen the UK's defences against cyber attacks on NHS, transport and energy
Gov.uk - https://www.gov.uk/government/publications/government-cyber-action-plan
The Independent - New laws to bolster UK's defences against cyber attacks on NHS, transport and energy
Data Protection Network - UK Cyber Security Bill introduced to Parliament

Cyber-News

1 in 3 adults in the UK are using AI as a digital friend and therapist

January 2026

According to a report by the AI Safety Institute, an organisation part of the Department for Science, Innovation and Technology aiming to evaluate and ensure the safety of users using AI, a third of adults AI for for emotional support or social interaction. Additionally, one in 25 people turned to the tech for support or conversation. The report is based on two years of testing the abilities of more than 30 unnamed advanced AIs - covering areas critical to security, including cyber skills, chemistry and biology.

A survey by AISI of over 2,000 UK adults found people were primarily using chatbots like ChatGPT for emotional support or social interaction, as well as by voice assistants like Amazon's Alexa. They also found that in a subreddit (an online forum on a website called Reddit) dedicated to discussing AI companions, people reported that when their chatbots went down, they described symptoms of withdrawal", such as feeling anxious or depressed, disrupted sleep and neglecting their responsibilities.

The report discussed various issues with such a mindset including the ability to sway people's political opinions, with the most persuasive AI models delivering "substantial" amounts of inaccurate information in the process.

Additionally, over-reliance on AI might reduce opportunities for real human connection, leading to increased feelings of loneliness and social isolation. Studies have also found that a quarter of teenagers in the UK have turned to AI chatbots for mental health support in the last year.

Relying on chatbots as a primary, significant or only source of communication is bad for several reasons, including a reduction in human contact, which is bad for mental health and the occasional inaccuracies of what a chatbot says, which is followed on, could have serious consequences.

A chatbot isn't designed to pick up on social cues and emotions-it's just there to answer questions. So, relying on it for human interaction isn't going to work because it isn't programmed to understand how to do it in a way that is truly helpful. If you are having trouble related to interacting with others, it's better to reach out to real individuals, ideally in real life or sometimes online although be careful, especially with the latter.

Sources:
BBC News - One in three using AI for emotional support and conversation, UK says
The Guardian - Third of UK citizens have used AI for emotional support, research reveals
The Independent - Experts issue warning over people forming 'emotional bonds' with AI chatbots

Cyber-News

UK Teens Charged in £85m TfL and US Cybercrime

December 2025

2 teenagers were charged by US Department of Justice and the Crown Prosecution Service in England in connection to attacks on TfL in August 2024, which resulted in a data breach potentially affecting thousands of customers whose names, contact information and bank details was accessed. Thalha Jubair, a 19-year-old from East London, was also charged with computer fraud, wire fraud and money laundering in relation to more than 120 network intrusions and extortion involving 47 US entities. He's believed to have extracted $115mil (around £85mil) in ransom from his victims. His accomplice, Owen Flowers, an 18-year-old from Walsall, has been accused of conspiring with others to infiltrate and damage the networks of SSM Health Care and attempting to target Sutter Health's networks. Both are alleged to be part of Scattered Spider, a US and UK based hacking group whose previous high-profile targets include the casino, Caesars Entertainment and UK shops M&S, Co-op and Harrods. If convicted, they could spend a minimum of 14 behind bars.

Sources: The Telegraph: Teenagers charged over multi-million pound tfl cyber-attack/;
BBC News: Teenagers charged over Transport for London cyber attack;
Financial Times: Briton charged in US and UK over major cyber attacks

Tech Review: YubiKey

The YubiKey is a hardware authentication device developed by Yubico. It works as a method of **2 factor authentication**, where a login requires the user to confirm their attempt to login on 2 different devices. In this instance, the user would go to the settings of an app they have a login to, then add the YubiKey as a "security key". From that point on, the user will login using their username and password like before but also need the YubiKey to be plugged into the device at the same time.

The latest edition of the YubiKey costs £50.16 direct from the website and £56 on Amazon. It has been designed to support USB-A, USB-C and NFC, Lightning ports.

Reviews for the product praise it for the physical durability of the device as well as its versatility across multiple platforms and its strength against phishing-attacks.

However, customers also note that the small size of the product can lead it being lost or stolen, the initial cost to purchase is high, and the setup can be a bit confusing for those not so technically minded.

https://www.yubico.com/
https://amzn.eu/d/eFqoSuK

A to Z of Cyber-Crime

Cyberstalking/Harassment

This involves using digital communication technologies (such as emails, messaging apps, or social media) to harass, monitor, or stalk someone. It's not a one-off incident but repeated behaviour intended to frighten, intimidate, or distress the victim. Examples include sending threatening messages, spreading rumours online, tracking someone's online presence, or trying to gain access to private accounts. In severe cases, cyberstalking can escalate to offline harassment.

Denial-of-Service (DoS) Attacks

A DoS attack tries to overload a system, website, or server with too many requests so that it becomes too slow or completely unavailable to legitimate users. A more powerful version is called a Distributed Denial-of-Service (DDoS) attack, where multiple computers (often hijacked by malware) flood the target at the same time. These attacks can cause major disruptions for businesses, governments, and online services.

Hacking

This is when someone gains unauthorised access to a computer, system, or network. Hackers often do this by exploiting software vulnerabilities, using stolen passwords, or tricking people into giving them access. Once inside, they might steal data (like bank details), install malware, deface websites, or use the system to launch other attacks. Not all hackers are criminals — some are "ethical hackers" who test security systems but in everyday use, the term usually refers to malicious activity.

Identity Theft

This happens when a criminal steals someone's personal information — such as names, addresses, National Insurance (NI) numbers, bank account details, or credit card numbers — and uses it to commit fraud. This could mean opening new credit accounts in the victim's name, making unauthorised purchases, or even applying for loans. Victims often don't know until they see unusual bank charges or are denied credit due to debts they didn't create.

Ransomware

This is a type of malware that blocks or encrypts files on a victim's computer so they can't access their own data. The attacker then demands payment (often in cryptocurrency) to "unlock" it. Ransomware can spread through infected email attachments, malicious downloads, or compromised websites. High-profile cases have affected hospitals, schools, and even national infrastructure. Paying the ransom doesn't guarantee recovery, and in many cases, victims remain locked out.

Sim Cloning/ Sim Swap Fraud

Sim cloning is when an attacker gains physical access to the target's SIM card and then copies the number onto another sim card. The attacker can use this to access the victim's texts, phone calls, and location data. From that point, they can read your text messages to get information about you, scam your contacts by posing as you, or receive 2-Factor Authentication (i.e. you login via username and password onto a site, then they text you a code your phone to make it more secure-logging in on 2 devices).

Social Engineering

Instead of hacking computers, attackers manipulate people directly into handing over sensitive information. They create convincing scenarios — for example, pretending to be a bank official, a delivery company, or even a colleague — and ask for details like login credentials, bank numbers, or personal data. Phishing emails, phone scams, and fake websites are all examples. Social engineering works because it exploits human trust rather than technical weaknesses.

clearcommunityweb

MOPAC MAYOR OF LONDON OFFICE FOR POLICING AND CRIME

NEIGHBOURHOOD WATCH 1982 - TODAY

FOCUS ON: Sim Swap Fraud

SIM swap fraud is when scammers take control of a phone number by switching the service from the customer's SIM to another SIM in their possession. Its then possible to access your online accounts and personal data.

What are the signs?

- You are no longer receiving calls or texts
- Your bill/call logs show calls and texts to numbers you don't recognize
- Your location appears elsewhere
- You've been locked out of accounts you previously had access to.

Protecting yourself

- Avoid sharing your mobile number online unnecessarily
- Use app-based authentication (e.g., Google Authenticator) instead of SMS codes
- Set up a SIM PIN or passcode through your mobile provider

What to do in a crisis:

Contact your mobile provider immediately: They can confirm if a swap occurred, deactivate the fraudulent SIM card, and help you regain control of your phone number.

Notify your banks and financial institutions (e.g., credit card companies): Request that they freeze your accounts to block any unauthorized transactions and monitor for suspicious activity. You may be able to do this from within an app!

Secure your online accounts: Change your passwords to new, strong, and unique ones and disable SMS-based two-factor authentication (2FA) temporarily and switch to more secure methods like app-based authenticators (e.g., Google Authenticator) or physical security keys.

Report the fraud: Report the crime to Action Fraud online or by calling 0300 123 2040. Ensure you keep a record in case of future disputes.

Monitor your accounts: Keep a close watch on your bank statements and online accounts for any transactions you don't recognize. If you find any, report them immediately as unauthorized charges.

DID YOU KNOW?

SIM-swapping fraud doubled nationally in both 2023 and 2024, with nearly 3,000 incidents reported last year, according to Report Fraud.

Report Fraud

clearcommunityweb

MOPAC | MAYOR OF LONDON

NEIGHBOURHOOD WATCH

Online Safety 101

Password Safety rules

To create the best passwords, make them long (12+ characters), complex (mix of uppercase/lowercase letters, numbers, and symbols), and unique for each site. Avoid personal information, common words, and simple patterns like "12345".

Consider using a strong passphrase or a password manager to help you generate and store these strong, unique passwords securely.

Key Characteristics of a Strong Password

Length: Aim for at least 12 characters, but 14 or more is even better.
Complexity: Use a mix of:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special symbols (!, @, #, $, etc.)

Uniqueness: Use a different password for every online account.
Randomness: Avoid dictionary words, personal information, and predictable sequences.

Tips for Creating and Managing Passwords

- **Create a passphrase:** A string of random, unrelated words is often easier to remember than a complex jumble of characters.
- **Use a password manager:** These tools can generate strong, unique passwords and securely store them for you.
- **Enable Two-Factor Authentication (2FA):** For added security, enable 2FA on your accounts whenever possible.
- **Avoid Personal Information:** Never use your name, birthday, address, pet's name, or any other information that could be easily guessed or found online.
- **Don't Reuse Passwords:** If one account is compromised, using the same password for other accounts creates a massive security risk.

Little Guide to Passwords (MET)

How secure is my password?

clearcommunityweb

MOPAC | MAYOR OF LONDON

NEIGHBOURHOOD WATCH

Online Safety Glossary

Antivirus – A program that protects your computer from harmful software (called viruses) by spotting and removing them.

App – Short for "application." A small program you use on your phone, tablet, or computer, like WhatsApp or online banking.

Browser – The tool you use to look at websites, such as Google Chrome, Safari, or Microsoft Edge.

Cookie – A small file websites save to remember your preferences, such as your login or shopping basket. Usually harmless.

Encryption – A way of scrambling information so only the right person can read it – like sending a message in code.

Firewall – A shield that blocks unwanted visitors or threats from entering your device through the internet.

Hacker – Someone who tries to get into computers or accounts without permission. Some are criminals, but not all.

Malware – Short for "malicious software." Harmful programs such as viruses or spyware that can damage or spy on your device.

Password – A secret word or phrase you use to protect y our accounts. The best ones are long and hard to guess.

Pop-up – A small window that suddenly appears on your screen, often showing adverts or scams.

Scam – A trick to steal your money or information, often by pretending to be someone you trust.

Spam – Unwanted or junk emails, usually adverts or scams, that clutter your inbox.

Two-Factor Authentication (2FA) – An extra layer of security that asks for two things to log in, like your password and a code sent to your phone.

Update – A fix or improvement for your apps or computer. Updates keep you safer and make things run better.

Username – The name you use to log in to a website or service – often your email address or a nickname.

Virus – A type of malware that spreads and damages your computer or files, like a cold for your device.

VPN (Virtual Private Network) – A tool that hides your location and makes your internet use more private, especially on public Wi-Fi.

Wi-Fi – A way to connect to the internet without wires. It's safest when password-protected.

Website address (URL) – The link you type in to visit a site, such as www.bbc.co.uk. Always check spelling to avoid fake sites.

clearcommunityweb

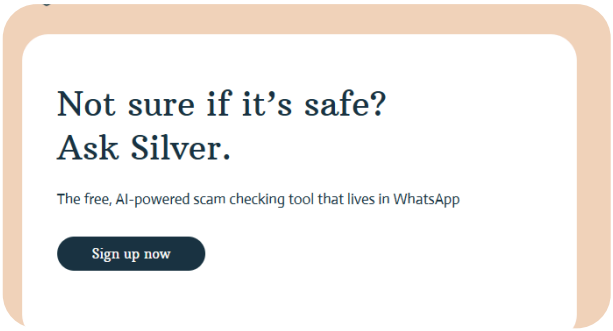
MOPAC | MAYOR OF LONDON

NEIGHBOURHOOD WATCH

Useful software & services

AskSilver

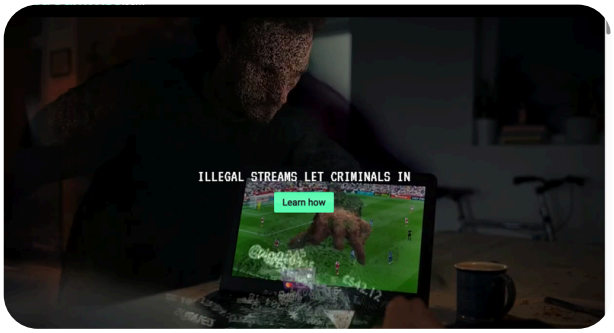
Launched in 2023, this is a scam checking tool which operates as part of WhatsApp. It was created by Alex Somervell and Jonny Pryn after Alex's dad was scammed 3 times in 2019, losing a total of £150,000. The tool works in a similar way to a typical text thread on WhatsApp, where you send a photo a text message or email address to the chatbot, then it will scan for any signs of a potential scam, such as the sender's email address not matching the domain name of the company they supposedly work for, any added links not going to a legitimate site or a lack of personalization(i.e. "Dear Customer" rather than "Dear Ms May Parker") and based on the results, it responds with a list of any suspicious things it finds and gives the user the opportunity to report it.



Based on testing, it's quite an effective tool but the app itself notes that it is to be used alongside the user's own research and best judgement. It's completely free and all that's needed to use it is a phone and a WhatsApp account.
https://www.ask-silver.com/

BeStreamWise

BeStreamWise is an ongoing campaign about banning illegal streams. It was started in 2023 and is backed by several companies and organisations including the government's Intellectual Property Office, Crimestoppers, the Federation Against Copyright Theft (Fact), ITV, Sky and the Premier League. a website dedicated to informing visitors about the dangers of using illegal streaming websites. It discusses the risks of accessing illegal websites, such as accidently downloading viruses, some facts about the dangers of illegal streams, news articles about people running illegal streaming services getting arrested and convicted.



It also provides the user with more info about identifying dodgy websites and where to report them to. It also links to websites such as JustWatch which provides info on publicly and legally accessible TV shows and movies and the digital platforms that you can view them on such as Netflix, Prime Video, BBC iPlayer and even the cinema with prices.
https://www.bestreamwise.com

Focus On: Report Fraud

Report Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud in England, Wales and Northern Ireland. Between April 2018 and March 2019, 741,123 crimes were reported to Report Fraud, with a total of £2.2bn lost by victims.

They pass on reports on fraud to the necessary authorities, provide guidance and resources to prevent fraud and gather news articles which provide advice about how to avoid scams and scams that are currently being used.

They also give information about different forms of cybercrime and how to prevent yourself from getting hit by cyberattacks.

Reports are passed onto the the National Fraud Intelligence Bureau (NFIB) who assess and analyse the reports then send them to the appropriate police forces for investigation.

The Home Office funds Report Fraud and the NFIB and the City of London police, which is the national lead police force on fraud, runs the 2 organsisations.

The charity, **Victim Support** provides free and confidential support to victims, witnesses of crime, their friends & family and anyone affected across England and Wales.
When reporting fraud, users can request support from Victim Support.

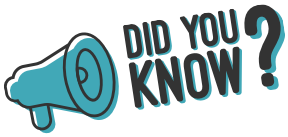
If you wish to contact Report Fraud, you can call them at **0300 123 2040 Monday to Friday 8am - 8pm** or register online for their online reporting tool.

https://www.reportfraud.police.uk/

#NoBlameNoShame

19 Million Lose Money To Scams But Fewer Than A Third Report

Coercive Control in fraud and Scams
National Trading Standards calls on Government to improve support for victims



73% of UK adults or 40 million people have been targeted by scams, with 35% - or 19 million losing money because of this criminal offence.

The average amount lost by victims is £1,730, but fewer than a third (32%) report the crime to the authorities, according to new research, released today by National Trading Standards (NTS).

clearcommunityweb

MOPAC MAYOR OF LONDON

Most common types of scams

Romance scams (long-term catfishing, sharing of personal info, makes it easy to manipulate victim)

These usually happen online (dating sites, social media, games). The scammer pretends to be romantically interested and spends weeks or months building trust. They often share fake stories, pictures, and emotions to make the victim feel a deep connection. Once the victim is emotionally invested, the scammer asks for money, gifts, or personal details (like bank info) and uses guilt or love as pressure.

Banking/Investment scams (they ask for money and claim they can double it, one way or another)

These scams promise huge returns with little or no risk, often through fake investment platforms, cryptocurrency schemes, or “get rich quick” opportunities. Victims are told to deposit money. Eventually, the scammer either disappears or pressures the victim to “invest more” before they can withdraw anything.

Impersonation scams (pretending to be a loved one, typically requesting financial support due to an emergency)

Here, the scammer contacts the victim claiming to be a friend, relative, or partner in trouble. They might say they’ve been in an accident, arrested abroad, or stuck with unexpected expenses. They usually demand urgent money transfers and rely on panic and concern, so the victim doesn’t stop to verify the situation.

Blackmail scams (claiming to have private data they will leak)

The scammer says they’ve hacked into the victim’s accounts or devices and claim to have compromising photos, videos, or sensitive information. They threaten to share this with family, friends, or employers unless the victim pays (often in cryptocurrency). In most cases, they actually have no real data — they just rely on fear and embarrassment.

Technical support scams (claim that you have a virus and need to download an app or visit a website—which is usually the real virus—to get rid of it)

The scammer poses as a tech support agent from companies like Microsoft, Apple, or your internet provider. They warn you about a fake virus or security breach, then tell you to install software or visit a website. The software is actually malware that lets them steal data, lock your files (ransomware), or demand payment for fake fixes.

Friends Against Scams

Join over 1 million people in helping the fight against fraud.

Friends Against Scams is a **National Trading Standards** initiative in the UK that educates people to recognize scams, protect themselves and others, and support victims by providing awareness training and encouraging community conversations about scams.

https://www.friendsagainstscams.org.uk/

clearcommunityweb

MOPAC | MAYOR OF LONDON

NEIGHBOURHOOD WATCH

Email Scams to watch out for

Temu free prizes

Temu is a Chinese company which offers heavily discounted consumer goods, typically shipped directly from China where most things are manufactured. The general catch is risks to user privacy due to extensive data collection, concerns about unethical labour practices and forced labour in its supply chain and poor or inconsistent product quality.

There is an ongoing widespread scam in which the scammer posing as Temu sends an email which claims that the victim could receive a prize such as a free or heavily discounted e-bike in exchange for answering a few questions about their shopping experience with the brand. The victim will then click on a dodgy website and give their personal data.

Cloud Service Full

Cloud storage is a method of storing digital data on remote servers, accessible over the internet, rather than on local devices like hard drives. Multiple companies offer a form of cloud service, including Google (Drive), Microsoft (OneDrive) and Apple (iCloud).

Scammers sometimes send messages claiming to be the cloud provider and they inform you that your cloud storage is full and you must pay to upgrade. They can sometimes even claim that you will no longer be able to send messages or that your account will be locked or even deleted if you don't respond to the message urgently.

If the user was at or over the limit for their storage, the worst-case scenario would be that you may not be able to edit your files or upload new ones, depending on the provider's methods, but your account would not be locked or deleted.

Winter fuel payments

Criminals will message you claiming to be from the government and ask you to update your details or complete an application to receive your Winter Fuel Payment. They'll direct you to a fake government or energy website that looks just like the real thing.

The website will ask for your personal information and card details, which the criminals will use to make fraudulent payments. If you're eligible for the Winter Fuel Payment, the government won't text or email you. Most people that are eligible will get their payment automatically and receive a letter to confirm the amount. You can use the real government website to check if you are eligible.

clearcommunityweb

MOPAC MAYOR OF LONDON

NEIGHBOURHOOD WATCH

Warning! - Making a fake website is easier than you think

What I want you to do is go onto a website, like YouTube, BBC News or Amazon. Then either press "Ctrl" and "U" at the same time or click "Inspect" on Edge or "View Page Source" on Chrome or something similar. What comes up is the source code. This is written by developers to make the website function and look nice.

Cyber-criminals can use this to their advantage. If you clicked on a link that claimed it was from your bank and you found a site that look messy and nothing like it usually does, you'd probably not go ahead with using the website.

To bypass that, criminals will take the source code, keep the outside formatting but change both some of the text and the behind-the-scenes parts of the website to carry out their crimes.

For example, display an urgent warning message, and instead of the login button giving you access to your bank account, your email address, card number and password are just sent to the attacker's computer. Therefore, it is important to be wary when clicking on links. If the email doesn't match the usual format, the sender's address looks suspicious or the web address doesn't match, those could be all signs of something wrong.

Ultimately, if you're not sure, use Google to access the website directly or contact the company via established contact details for confirmation of the email's claims. If you already clicked on the link and entered any details, close the page, call the real company so that they can lock your account if needed or change your password.

Below is 2 pictures with examples of such modifications. Which is the real one and which is fake?

6 years is an amazing deal, but I was unaware that David Beckham and Bruce Springsteen were BBC journalists!

You can check if a website is genuine or not here https://www.getsafeonline.org/checkawebsite/

Partners

The Cyber Helpline

The Cyber Helpline is a charity founded in 2018 by Rory Innes, supporting victims of cybercrime, digital fraud, and online harm. Its main service is a chatbot that asks users a few anonymous questions to identify potential threats, then provides guides and resources on issues like account hacking, online harassment, and identity theft. Users can also request to speak to an advisor, who will respond within three days via phone or email to address immediate threats, gather evidence, and teach online security. The chatbot is available worldwide, while advisors operate in the UK and USA.

The service is free, funded by donations, fundraisers, and sponsors. Since its founding, it has supported over 1.5 million users, with 80,000 receiving self-help guidance.

https://www.thecyberhelpline.com/

National Cyber Security Centre

The NCSC provides advice to individuals, small, medium & large organisations, the self-employed and those in the public sector on how to protect their data and devices through articles and recommendations for organisations and websites to report crime, secure data and learn about
cyber security.

The NCSC also works with educational institutes to design practical resources for school staff, help create standards for cyber security degrees across many different universities including Greenwich, Bradford and Gloucestershire and provide training opportunities for people to gain certifications to become qualified cyber security professionals.

https://www.ncsc.gov.uk/

Neighbourhood Watch

Neighbourhood Watch are the largest volunteer-led crime prevention charity in the country, working in communities to support them in being safer, more resilient places to live. They provide resources, projects and networks that support volunteers and communities to work together to prevent crime, raise awareness around safety initiatives and community resilience, and connect neighbourhoods.

Resources

Advice & Information

National Cyber Security Centre (NCSC)
The National Cyber Security Centre, a part of GCHQ, helps businesses, the public sector and individuals protect the online services and devices that we all depend on.

MET - Little Guides
A series of leaflets and books design by the MET to explain some of the most common scams and give advice on how to avoid falling victim to them

The Cyber Helpline Guides
A series if guides and how-to's developed by The Cyber Helpline

Get Safe Online
The UK's leading internet safety website. We provide unbiased, factual and easy-to-understand information on online safety.

Internet Matters
Offers expert guides, practical advice, and interactive resources for parents, carers, and professionals to navigate the digital world and its various risks.

ChildNet
A UK-based charity who empower children, young people, and those who support them in their online lives, and its mission is to work with others to make the internet a great and safe place for children and young people.

Take Five
Useful resources to help people be more resilient against scams and financial fraud

Reporting

Reporting Fraud
Formally known as Action Fraud, is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cyber crime.

CrimeStoppers
Independent charity enabling the anonymous reporting

Victim Support
Support services to help people manage after crime and to empower them to ensure their voices are heard.

Useful Tools

How Secure is My Password
Check how quickly and easily your password is to guess and improve it. Great tool to help people make their passwords more secure

Have I Been Pwned
Check to see if your email address has been caught in a data beach

The Cyber Helpline
A chatbot which takes you through the steps to understand if you have been compromises, signpost to relevant resources or connect you with a trained volunteer

F-Secure Online Virus checker

Cyber Action Plan
Online tool for both individuals and business created by the NCSC.

Videos

MET Little Guides

A series of short videos including safety passwords, securing your identity and phishing

Data to go

A case study on how personal information can be taken and used in a public space

Don't be a victim

A series of case studies deconstructing common scams

Scam Safe

A collection of videos from the BBC

Downloads

Little book of Cyber Scams 2.0

Little book of Big Scams

clearcommunityweb

Training

Cyber Awareness Training
Free training from ESET covering the fundamental for employees

Introduction to Cyber Security
Free online training from Open University and NCSC

Cyber Security Course
Subsidized Level 3 Training

Cybrary
Free industry focused training

Learn My Way
Free learning for you to gain digital skills to stay safe and connected

Do you know someone who needs help? Make a referal!

The threat of any form of cyber crime or harassment can lead to extreme anxiety and affect all aspects of life and health.

Speak to us now for clear advice and guidance on whether you have been compromised and what you can do about it.

We can help you to

- **Find the right support**
- **Work with you to create a recovery plan**
- **Build resilience for the future**

To make a referral please complete the form:
https://clearcommunityweb.co.uk/referral

Contact

info@clearcommunityweb.co.uk
07523 646 277
www.clearcommunityweb.co.uk
@clearcommunityweb

clearcommunityweb

MOPAC | MAYOR OF LONDON

NEIGHBOURHOOD WATCH

About ClearCommunityWeb

ClearCommunityWeb help people feel more confident and comfortable with technology through classes, workshops and individual support. We guide and support people to become more independent, more confident and to reduce anxiety. In 2025 we worked with over 1500 across South London.

We understand, that for many people, technology can be overwhelming. Making information as simple as possible can go a long way in giving people the confidence to overcome their fears and anxieties.

We have become a place where no question is too basic and we can work together to overcome the challenges you face.

We look foreward to meeting you

Newsletter

Schedule

Contact

info@clearcommunityweb.co.uk
07523 646 277
www.clearcommunityweb.co.uk
@clearcommunityweb

clearcommunityweb

MOPAC MAYOR OF LONDON

NEIGHBOURHOOD WATCH