



CDoS Hints and Tips 2025 No 4.

PLEASE SEE OUR HELPFUL SECURITY HINTS AND TIPS THAT ANSWER SOME OUR SUPPORT CONTRACT CLIENT'S QUESTIONS COMING UP...

16 Mere Green House, 46-48 Mere Green Road, Sutton Coldfield B75 5BT

Tel: 01213084394 Mob: 07838199007 email support@cdospcdoctor.co.uk

Here's our IT Hints and Tips & News Number 4, packed with practical tech tips for everyday users. Each item includes a helpful link so you can take action right away.

1

I must admit I have struggled to find a decent Christmas Dinner in 2025 – you know...Turkey, stuffing trimmings roasties, sprouts, Parsnips – Restaurants seem to have forgotten how to do it how shall I say - properly. Eventually I took the bull by the horn and made my own – Tasted great and I froze the rest.

Let's look at my Tech Resolutions and good security tips for 2026: Smarter, Safer, Simpler to find out what's ahead for 2026? However, first a word from me to you...

SECURITY WARNING* REPEATED every month

It doesn't matter how many times I say the words "NEVER, EVER, speak to strangers who call you on the phone asking for information, surveys, solar panels, bank information bogus security warning it seems that the "Trusting over 60's" being good decent people from an earlier perhaps simpler time KEEP on trusting what's being said by complete scam artists. Over the last few weeks over £0000's to my knowledge has been pilfered from the unsuspecting and trusting souls in Sutton Coldfield. The answer is always SHOOT FIRST AND ASK QUESTIONS LATER! This means be on your guard, never get involved in any conversion that pops up out of the blue from your bank, building society, pension provider. Very rarely will they ever approach you directly unless their algorithms suspect that you are actively involved in being scammed. Watch out for doorstep scams armed with credit card machines mysteriously refusing cash... as well from tradesmen advising they've seen a loose tile on your roof. There was an excellent program on BBC Radio 4 you and yours on the 24th November at about 11.30am check it out on BBC Sounds. We are in the middle of BBC Scam week and boy are the fraudsters out and about at present. Check out SCAM BRITAIN

Tech Resolutions for 2026: Smarter, Safer, Simpler

As we step into 2026, it's the perfect time to refresh not just our calendars but our IT habits. Whether you're a home user or power user or managing a small business or your own digital life, let's make this year smarter, safer, and more connected and best the Russian and Chinese hackers at their own game.

1. **The first resolution** Check your emails carefully and before randomly clicking attachments of friendly messages just stop and think about who how what and why this was sent and is it normal behaviour.
2. **Get an iPhone not android.** – I know I know they are more expensive BUT they are safer and less prone to hacking and you don't need all that AV software clogging it up as iPhones work differently. As for expense there is some really good deals on at present and if you take my advice I recommend buying a refurbished one they start from about £200 then all you have to buy is a sim only contract from say £17 per month and this includes all the data space you can shake a stick at! I'm not saying the iPhone hasn't had its security moments, but Apple do make efforts to protect you in many ways. Expensive – yes it can be, but I recommend to price conscious client to go for Refurbished older models on Amazon. An iPhone 17 SE is very comparable in price or older models. Say anything from iPhone 11, 12, 13, 14, 15 line up. **Consider Apple** So, if you are looking for a new phone consider the Apple. I must say that the change over does take a little getting used to but like everything it all falls into place in a few days it all becomes quite logical. I know quite a few IT people who will disagree with this view but it is my blog! In Samsung phones defence I would say that the camera and tech is very good but really the eco system I still find illogical and "Clunky"
Resistance is futile! Whatever you choose - Having a smart iPhone is not to be resisted in favour of that "Durro" they are next to useless in this security intense century. It's almost impossible to verify yourself with out a Microsoft Authenticator app. I have many clients who have benefitted from a quick 30 minute training session. We are here to help – If you are a support client apart from the £20 visit fee there is no Charge.
3. **We now supply and install the complete range of Amazon Echo devices** and most importantly will train you on getting the nest out of them. My news years resolution is to reduce the mystique that new technology brings and help our clients get the best from them.
4. **Get protected better in your home with CCTV** we now supply supportable CCTV packages where the password and control is in your hands. Not the installer. Many clients ask me "Do you know anything about CCTV systems? Often they install proprietary systems with sensitive password withheld making it impossible to manage you own security show. We install "Ring" and everything is passed over for you to manage but we stand by you to do the managing for you.
I list a top 10 set of get out of jail IT cards for you at end of this bulletin

And there's more... (Jiminy cricket if I am not mistaken)



[Grok apologizes for creating image of young girls in “sexualized attire”](#)

A Grok incident, where the chatbot acknowledged generating inappropriate images involving minors, highlights how rushed AI development can outpace safety, leading to serious guardrail failures.

3

[Keep Reading](#) →



[Disney fined \\$10m for mislabeling kids' YouTube videos and violating privacy law](#)

Disney agreed to a \$10m FTC settlement over allegations it violated US children's privacy law by improperly labeling kid-targeted YouTube content.

[Keep Reading](#) →



[Phishing campaign abuses Google Cloud services to steal Microsoft 365 logins](#)

Attackers are using highly convincing fake “Google” emails that bypass spam filters, abuse trusted Google services, and route victims to a spoofed Microsoft 365 login page to steal credentials.

[Keep Reading](#) →

One million customers on alert as extortion group claims massive Brightspeed data haul



US broadband provider Brightspeed is investigating claims by the Crimson Collective that hackers stole sensitive data on over 1 million customers, including personal, account, and billing information. Just because we are in the UK doesn't mean you are exempt as Mobile providers are often PAN-Global and "whitebox" there products to us in Europe (anyway its worth a read)

4

Blake Montgomery from the Telegraph a good read...



Hello, and welcome to TechScape. I'm your host, Blake Montgomery, US tech editor for the Guardian. Today, we discuss Elon Musk's rosy depiction of Grok's image generation controversy; the seven-figure panic among Silicon Valley billionaires over a proposed wealth tax in California, though with one notable exception; and how AI and robotics have revitalized the Consumer Electronics Showcase.

Musk's reframe

The firestorm over the Grok AI tool has been raging for more than a week now, and it shows no signs of slowing down.

Last week, I wrote about the [rising backlash against Elon Musk's Grok AI tool](#), which in recent weeks has allowed users to generate thousands of sexualized images of women. Some of the images show real women, some are fake, some are nonconsensual, and some depict children, all in "minimal clothing", as the AI tool itself described them.

X and its parent company, xAI, have taken some measures to curb the flood. The social network shut off its image generation feature for users who do not pay, which constitute the majority of X's users.

Throughout the controversy, Musk has obstinately recast the AI tool's problems as everything but what they really are. He's been promoting its popularity as if it were a piece of productivity software. He crows about its download numbers with dubious claims. On 10 January; he [celebrated](#) Grok reaching the top spot in New Zealand's version of Apple's App Store. (Rankings by the analytics firm [SimilarWeb](#) of the most-downloaded apps in New Zealand, which were updated the same day as Musk's tweet, put Grok in 14th place.) The same day, he [reposted](#) a tweet about Grok reaching the No 1 spot in Thailand's Apple App Store. (SimilarWeb's [rankings](#) do not show Grok in the top 50 most-downloaded apps in the country.) On 9 January, he retweeted a post about Google searches for Grok spiking. (I would guess the increase in searches is evidence of great interest in the AI tool's scandal more so than interest in using it.)

In response to the UK's threats to ban the AI tool, he accused the country's government of stifling free speech. After watchdogs cited instances of Grok undressing minors, he said: "Anyone using Grok to make illegal content will suffer the same consequences as if they upload illegal content," handing the responsibility to moderate his social network to law enforcement and courts. "Illegal" is in a court's hands and frees him from moderating all but the most heinous content.

So what's the strategy?

Perhaps to Musk, all press is good press? He may be right: his AI tool seems likely to accrue more users and few penalties as a result of the flood of nearly naked images.

Grok has faced some repercussions: the UK's communications regulator, Ofcom, has launched an investigation into xAI and Grok, and possible punishments could include a total ban. The Internet Watch Foundation, also based in the UK, announced it had found instances of child sexual abuse material generated by Grok in Dark Web forums. X's revenue in the UK has [plummeted by 60%](#) as concerns over content moderation and brand safety grow. Both Indonesia and Malaysia have limited access to the AI tool in response.

But missing from the chorus decrying Grok are the two de facto smartphone regulators of smartphone software, Apple and Google, operators of the world's biggest mobile app stores. Neither has indicated whether the Grok's output violates their app stores' terms of service. In the US, there's been [little backlash from regulators and lawmakers](#). As we know in the UK we are not going to let GROK get away with it as the government will insist on legal compliance.

The lesson for Musk and other tech leaders seems apparent: the fewer restrictions you place on AI, the more shocking content you allow it to generate, the greater your engagement and your profit.

Big news



Apple takes on hidden location tracking with new iOS settings

Apple quietly rolled out a new setting designed to reduce how precisely cellular networks can track your iPhone, highlighting a layer of location data most users never knew existed.

Keep Reading →



Open the wrong “PDF” and attackers gain remote access to your PC

The DEAD#VAX campaign tricks users into installing AsyncRAT by disguising a virtual hard disk as a PDF attachment.

[Keep Reading](#) →

7



Grok still generates sexualized images, despite promised safeguards

Journalists retested Grok after xAI pledged fixes and found it still produced sexualized images, even when explicitly told the subjects were vulnerable or non-consenting.

[Keep Reading](#) →



AT&T

Old AT&T breach data is back and more dangerous than before

Data from earlier AT&T breaches has resurfaced in newly merged datasets, showing how old leaks can become far more harmful when criminals add missing details.

[Keep Reading](#) →

Providing a step-by-step Security and safety guide for the over 60's

I'll keep it concise but still detailed enough to be helpful. Since we are providing the "step-by-step version," I'll focus on the top few tips for Windows 11, not all 10. I'll go through each item with numbered steps

Now—let's make this “doable without calling the kids” level clear. I'll assume **Windows 11** and focus on **practical, high-impact steps**.

1. Turn on automatic Windows updates

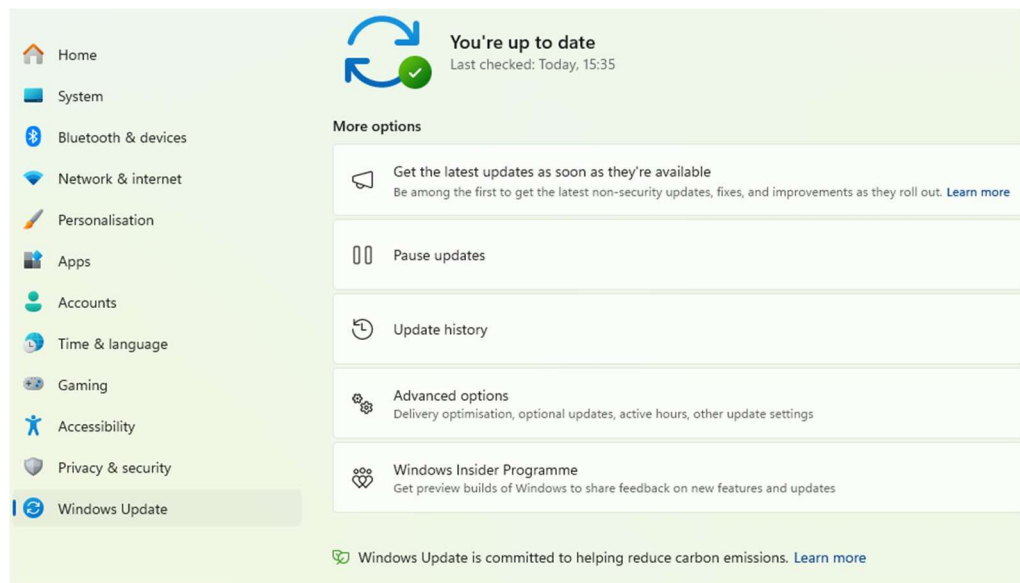
Goal: Make sure Windows keeps itself up to date.

1. Open Settings

- Click the **Start** button (Windows logo at the bottom).
- Click the **Settings** (⚙️) icon.

2. Go to Windows Update

- In the left-hand menu, click **Windows Update**.



○

Enable automatic updates

- Make sure it says “**You're up to date**” or shows updates in progress.
- Turn on “**Get the latest updates as soon as they're available**” if you see it.
- If there's a **Download** or **Install** button, click it.

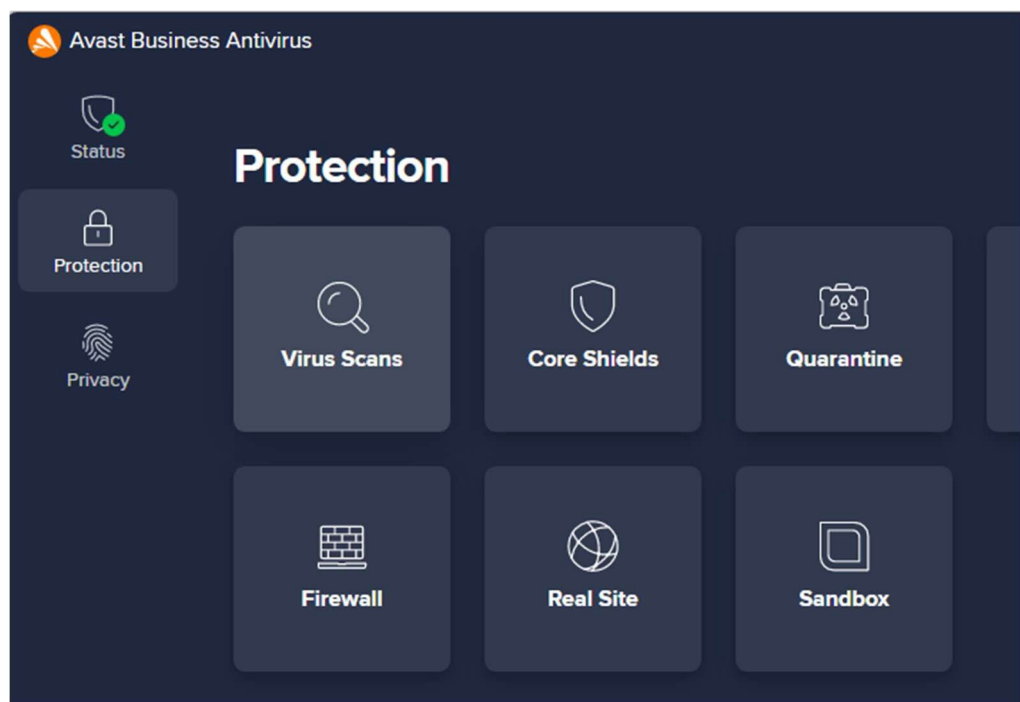
2. Check antivirus protection (Windows Security)

Goal: Make sure built-in protection is on and running.

1. Open Windows Security

- Click **Start**.
- Type **Windows Security**.
- Click the **Windows Security** app in the results. If you have a CDoS Support contract we do all the hard work for you they start at £75 per year including our Avast below.. £140 for a full remote access service inc Avast. (This is the pro version – no advertisements.

9



2. Check Virus & threat protection

- In Windows Security, click **Virus & threat protection**.
- Look for a green tick or a message like "**No current threats**".

3. Make sure real-time protection is on

- Scroll to **Virus & threat protection settings**.
- Click **Manage settings**.
- Check that **Real-time protection** is turned **On**.

3. Set a PIN to sign in

Goal: Simple, secure way to sign in.

1. Open Settings

- Click **Start** → **Settings**.

2. Go to Accounts

- In the left menu, click **Accounts**.
- Click **Sign-in options**.

3. Set up a PIN

- Under **PIN (Windows Hello)**, click **Set up** or **Add**.
- Enter your Microsoft account password if asked.
- Choose a **6-digit PIN** that isn't a birthday or simple pattern.
- Click **OK**.

4. Turn on two-step sign-in for email (example: Outlook / Microsoft account)

Goal: Add a text-message or app code to protect your email.

1. Open your browser and go to

- Type **account.microsoft.com** in the address bar and press **Enter**.
- Sign in with your email and password.

2. Go to Security settings

- At the top, click **Security**.
- Click **Advanced security options**.

3. Turn on two-step verification

- Find **Two-step verification**.
- Click **Turn on**.
- Follow the steps to add your **mobile number** or **authenticator app**.

5. Check emails safely

Goal: Avoid scams and dangerous links.

When you open an email:

1. Check who it's from

- Look at the **From** address, not just the name.
- If it looks strange (random numbers, wrong company name), be suspicious.

2. Don't click links if unsure

- If the email says things like “**urgent**”, “**your account will be closed**”, or asks for money—pause.
- Instead of clicking the link, open your browser and type the website address yourself (e.g. www.barclays.co.uk).

3. Don't open unexpected attachments

- If you weren't expecting a file, don't open it.
- If it's from a friend but feels odd, **call or message them** to check.

6. Turn on OneDrive backup for important files

Goal: Automatically back up Documents, Desktop, and Pictures.

1. Open OneDrive

- Click **Start**.
- Type **OneDrive** and open it.
- Sign in with your Microsoft account if asked.

2. Set up folder backup

- In the system tray (bottom-right), click the **OneDrive cloud icon**.
- Click the **Settings** (gear) icon → **Settings**.
- Go to the **Sync and backup** tab.
- Click **Manage backup**.

3. Choose folders to back up

- Tick **Desktop, Documents, and Pictures**.

- Click **Save** or **Start backup**.
-

7. Only install trusted software

Goal: Avoid junk and malware.

1. Use the Microsoft Store where possible

- Click **Start** → **Microsoft Store**.
- Search for the app you want (e.g. “Spotify”, “Zoom”).
- Click **Get** or **Install**.

2. Avoid pop-ups offering fixes

- If a website says “Your PC is slow, click here to fix” or “You have a virus, download this now” — **close the tab**.
- Don’t download anything from random pop-ups.

8. Use a modern browser with protection

Goal: Safer browsing with built-in warnings.

1. Open Microsoft Edge

- Click **Start** → **Microsoft Edge**.

2. Make sure SmartScreen is on

- In Edge, click the **three dots (...)** in the top-right.
- Click **Settings**.
- Go to **Privacy, search, and services**. Under **Security**, make sure **Microsoft Defender SmartScreen** is turned **On**.

9. Secure your home Wi-Fi

Goal: Make sure your Wi-Fi needs a password and isn’t using defaults.

This part can vary by router, so this is a general guide.

1. Find your router details

- Look at the **sticker on the back or bottom** of your router.
- Note the **Wi-Fi name (SSID)**, **Wi-Fi password**, and **router login address** (often something like 192.168.0.1).

2. Open router settings

- On your PC, open your browser.
- Type the router address (e.g. 192.168.0.1) into the address bar and press **Enter**.
- Log in with the **username and password** on the router label (often “admin” / printed password).

3. Change the router admin password

- Look for a section called **Administration, System, or Management**.
- Find **Change password** or similar.
- Set a new password that's not easy to guess.

4. Check Wi-Fi security

- Go to **Wireless** or **Wi-Fi** settings.
- Make sure **Security type** is **WPA2** or **WPA3** (not WEP or “Open”).
- Make sure there **is** a Wi-Fi password set.

..... and finally

If you have an Annual CDoS PCDoctor Support contract from us the setup routines includes all above. Our support services include: -

- Free Any time remote support access 7 days a week
- Free telephone support
- A safe FREE port of call if you are not sure about something
- Business class Avast AV with no adverts, daily reporting included
- Remote system setup
- 2 x free 40 minute visits per year (£20 visit fee applies but that's it)
- Reduced onsite support rates – save 10%
- CDoS Technicians with 35 years of experience behind them

All for 42p per day paid annually (consolidated to £140 over a 48 weeks period) We know you have holidays – so do we!