



Cyber news that bites back

Issue 8 • August 2026

WHAT THE HACK?

NEWS

**THE REAL
COST OF
DATA THEFT:**
IMPACTS ON
INDIVIDUALS
AND
BUSINESSES

**TfL CYBER
ATTACKERS
JAILED FOR
FIVE AND A
HALF YEARS
EACH AFTER
£39M BREACH**

**CYBER
OPERATIONS
(HACKING!)
IN MODERN
MILITARY
STRATEGY**



TfL Cyber Attackers Jailed for Five and a Half Years Each After £39m Breach

Two young hackers have been sentenced to five years and six months in prison each for carrying out a sophisticated cyber attack on Transport for London (TfL) that caused months of disruption and cost the organisation an estimated £39 million.

Thalha Jubair, 20, from east London, and Owen Flowers, 18, were sentenced on 16 July 2026 at Woolwich Crown Court. Flowers also received the sentence for additional offences relating to attacks on two US healthcare providers.

The attack took place between 31 August and 3 September 2024. The pair gained access to TfL's systems, escalated their privileges to the highest levels, downloaded large volumes of data, created backdoors, and attempted to cover their tracks. They communicated via Telegram and Flowers live-streamed parts of Jubair accessing the systems. The intrusion only ended when TfL detected the activity and removed them from the network.

The consequences were significant. TfL's online services were disrupted for three months, affecting customer information boards, refund systems, and Oyster photocard applications. All 28,000 employees had to reset their passwords in person. Around 10 million customers were notified of potential data exposure. Prosecutors described the attack as one of the most serious cyber incidents targeting UK critical infrastructure in recent years, noting the potential for catastrophic damage had the central systems been locked or destroyed.

Both men, linked to the Scattered Spider cybercrime group, pleaded guilty on the first day of their trial in June 2026. Jubair had previous convictions for hacking offences. The National Crime Agency described the case as the largest cyber crime prosecution brought before the UK courts under the Computer Misuse Act.

During sentencing, the court heard that the hackers were "highly skilled" but "utterly reckless," showing complete disregard for the impact on the public and essential services.

The case has been highlighted by law enforcement as a clear example of the real-world harm caused by cyber attacks on critical national infrastructure.

The Real Cost of Data Theft: Impacts on Individuals and Businesses

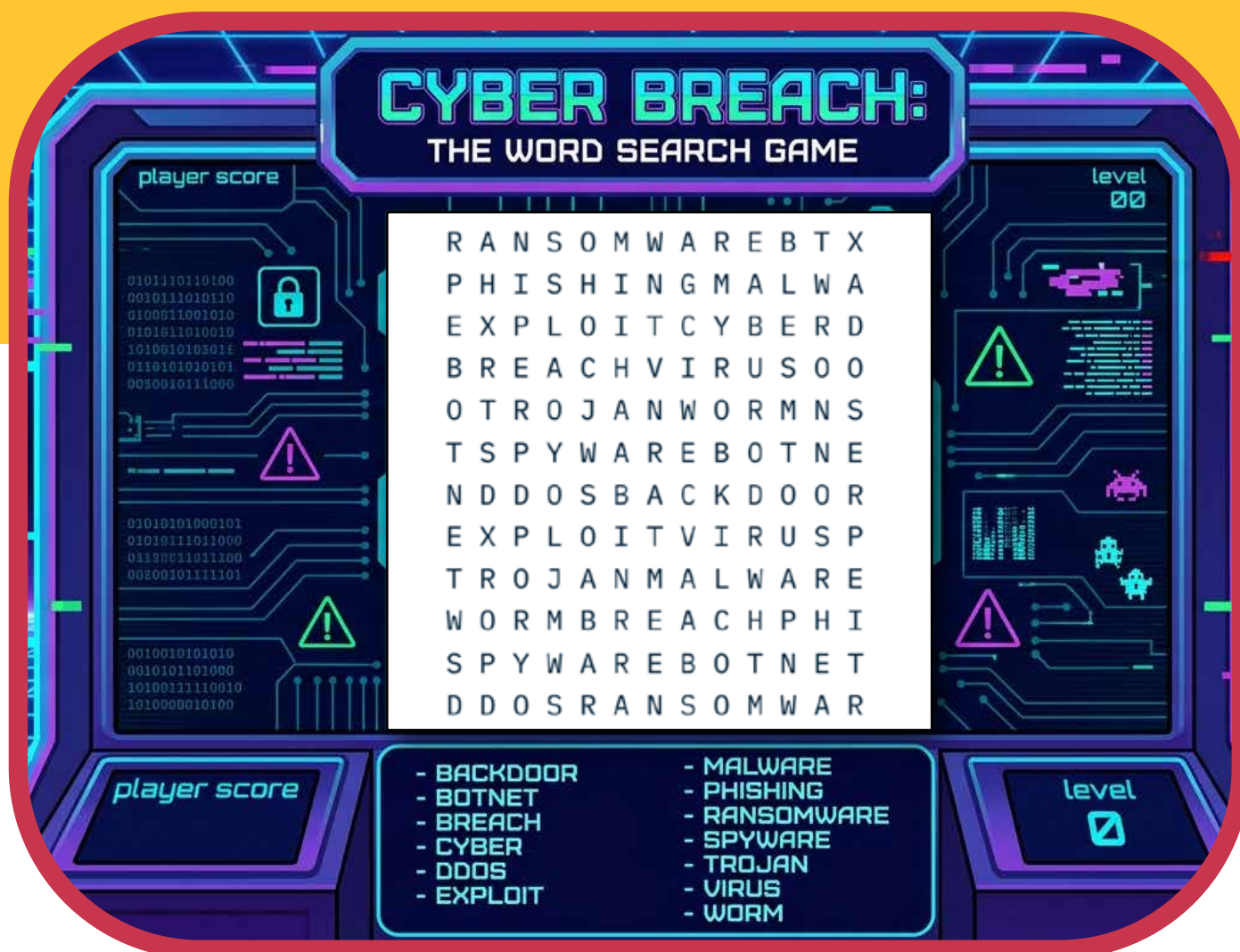
Data theft rarely stays confined to servers and databases. When personal information is stolen, the consequences ripple outward, affecting real people and the organisations entrusted with their data. Few incidents illustrate this more clearly than the 2017 Equifax breach, one of the largest in history.

In that case, sensitive details belonging to approximately 147 million Americans - including Social Security numbers, birth dates, addresses, and credit histories - were exposed. For individuals, the fallout was immediate and often long-lasting. Many became victims of identity theft and fraud. Fraudulent tax returns were filed in their names, unauthorised credit accounts were opened, and some faced years of financial disruption. Victims spent countless hours placing credit freezes, monitoring accounts, and disputing fraudulent activity. Beyond the monetary cost, many reported significant stress, anxiety, and a lasting loss of trust in institutions that hold personal data. For those with fewer resources or complex financial situations, recovery proved especially difficult and time-consuming.

The impact on Equifax itself was equally severe. The company incurred more than \$1.4 billion in costs related to victim compensation, legal settlements, security improvements, and regulatory penalties. Its chief executive resigned under pressure, and the breach triggered intense public and congressional scrutiny. Consumer confidence in the credit reporting agency dropped sharply, damaging its reputation and business relationships. The incident also accelerated regulatory attention across the financial sector and prompted broader industry discussions about data protection responsibilities.

Data theft of this scale reveals a fundamental truth: organisations that collect and store personal information carry significant liability. A single breach can trigger regulatory fines, class-action lawsuits, loss of customers, and long-term brand damage. At the same time, individuals often bear the heaviest practical burden - time, money, and emotional strain - with limited ability to prevent or fully recover from the misuse of their data.

The Equifax case remains a powerful reminder that data theft is not an abstract technical problem. It produces tangible harm to people's financial security and peace of mind, while imposing serious strategic and financial consequences on the businesses responsible for protecting that information. In today's data-driven economy, safeguarding personal information is both a technical challenge and a core business and ethical obligation.





Cyber Operations (Hacking!) in Modern Military Strategy

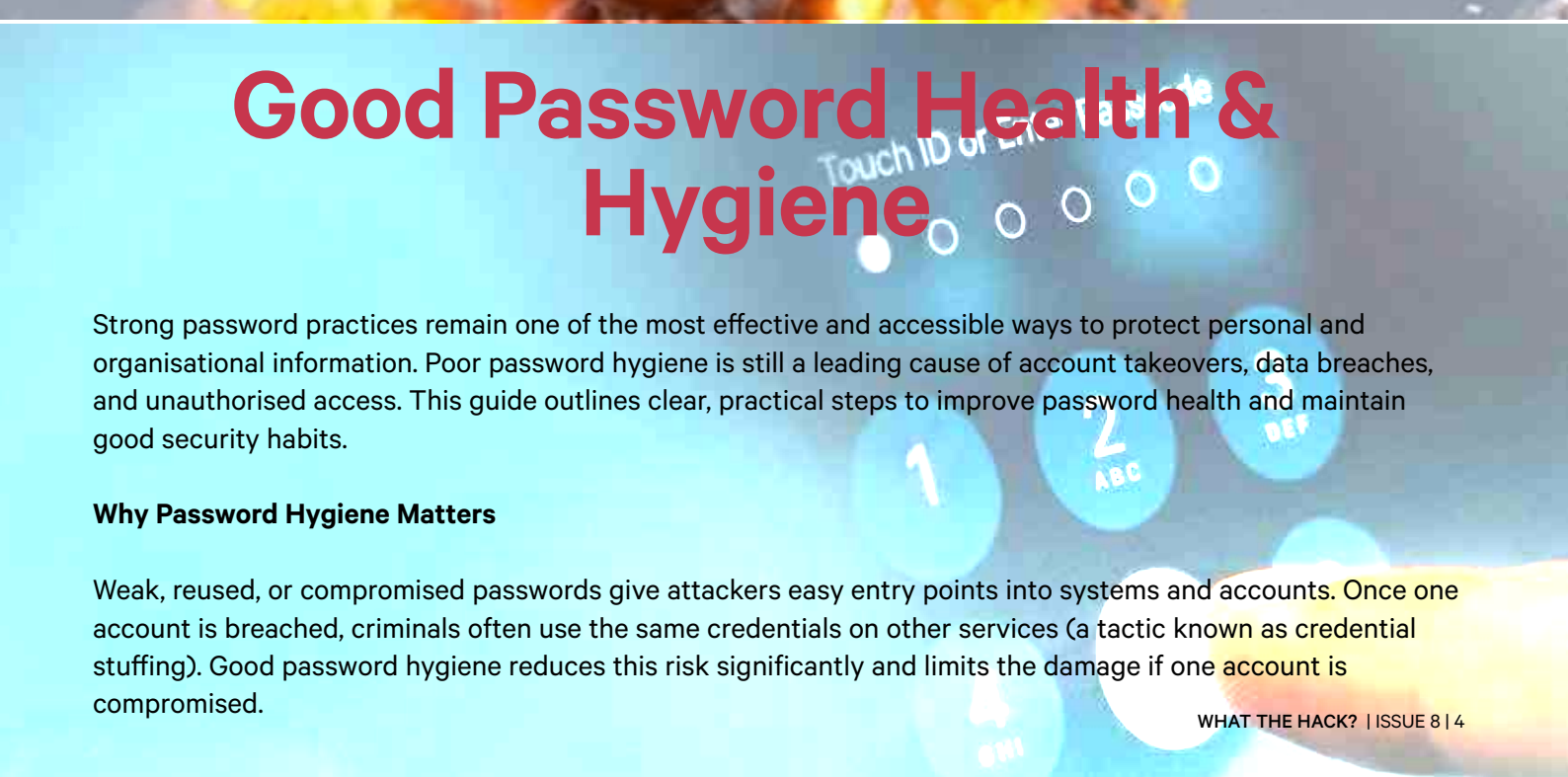
Cyberspace is now a recognised domain of warfare. States integrate cyber capabilities into military strategy to achieve effects previously requiring kinetic strikes or extended intelligence campaigns. These tools support espionage at scale, degrade command-and-control and logistics systems, pre-position access for future use, and generate ambiguity below the threshold of open conflict.

Major powers view cyber operations as persistent instruments. They enable intelligence collection and can disrupt critical infrastructure or communications. Pre-positioned access allows rapid activation in crises, while “defend forward” postures impose costs on adversaries without immediate escalation.

The 2010 Stuxnet operation against Iran’s nuclear program showed cyber power as a precise alternative to airstrikes, reportedly destroying centrifuges and delaying enrichment. In Ukraine, Russian-linked actors have paired disruptive attacks on energy grids and government systems with conventional operations since 2014 to undermine coordination and morale. The 2017 NotPetya malware, initially targeting Ukraine, spread globally and caused billions in damage, illustrating both strategic reach and risks of uncontrolled effects.

China prioritises long-term advantage through intellectual property theft and infrastructure pre-positioning to bolster military modernisation and wartime options. Other actors, including North Korea and Iran, employ cyber tools for revenue generation and asymmetric retaliation.

Despite their utility, cyber operations face clear limits. Attribution remains difficult, effects are often temporary, and unintended spillover is common. International norms are underdeveloped, sustaining a grey zone of activity. As artificial intelligence accelerates these capabilities, military planners must integrate them carefully with clear political objectives and awareness of escalation risks. Cyber has become a core element of multi-domain strategy, but its unpredictable nature requires disciplined application alongside traditional forces.



Good Password Health & Hygiene

Strong password practices remain one of the most effective and accessible ways to protect personal and organisational information. Poor password hygiene is still a leading cause of account takeovers, data breaches, and unauthorised access. This guide outlines clear, practical steps to improve password health and maintain good security habits.

Why Password Hygiene Matters

Weak, reused, or compromised passwords give attackers easy entry points into systems and accounts. Once one account is breached, criminals often use the same credentials on other services (a tactic known as credential stuffing). Good password hygiene reduces this risk significantly and limits the damage if one account is compromised.

1. Create Strong, Unique Passwords

- Use long passwords - aim for at least 12–16 characters. Longer passwords are generally stronger than complex short ones.
- Make passwords unique for every important account. Never reuse passwords across different services.
- Avoid predictable patterns such as names, birthdays, common words, or simple substitutions (e.g. “P@ssw0rd”).
- Consider using passphrases - a sequence of unrelated words or a memorable sentence (e.g. `Correct-Horse-Battery-Staple-47`). These are easier to remember and very strong when sufficiently long.

2. Use a Password Manager

A reputable password manager is the single most important tool for good password hygiene.

Benefits:

- Generates and stores strong, unique passwords for every account.
- Reduces the need to remember multiple passwords.
- Alerts you to reused or weak passwords.
- Makes it easier to update passwords regularly.

Choose a well-regarded password manager with strong encryption and a good security track record. Enable its own strong master password and multi-factor authentication.

3. Enable Multi-Factor Authentication (MFA) Everywhere

Passwords alone are no longer enough. Multi-factor authentication adds a critical second layer of protection.

Best practices:

- Enable MFA on all important accounts (email, banking, work systems, password manager, cloud services).
- Prefer authenticator apps or hardware security keys over SMS-based codes, as SMS can be intercepted.
- Where available, use passkeys (passwordless authentication using device biometrics or security keys). Passkeys are generally more secure and convenient than traditional passwords.

4. Avoid Common Mistakes

- Never share passwords via email, messaging apps, or documents.
- Do not write passwords down in easily accessible places (unless stored securely in a locked physical location).
- Avoid using the same password for work and personal accounts.
- Do not use passwords that appear in data breaches. Tools like “Have I Been Pwned” can help check if your email or passwords have been exposed. See <https://haveibeenpwned.com/>.
- Be cautious of password reset processes. Attackers often target these to gain access.

Good Password Health & Hygiene

5. Regular Maintenance

Good password hygiene is not a one-time task. Build these habits:

- Review and update important passwords periodically (especially after any suspected breach or when a service announces a security incident).
- Regularly check your password manager's security dashboard for weak, reused, or old passwords.
- Monitor accounts for suspicious activity and enable login alerts where available.
- When leaving a job or ending a service relationship, change relevant passwords promptly.

6. Additional Protections for Work and High-Value Accounts

- Use separate passwords for work-related accounts and never reuse them on personal services.
- Follow your organisation's password and access policies.
- For privileged or administrative accounts, use stronger controls such as hardware security keys and just-in-time access.
- Be especially careful with email accounts - these are often the gateway to resetting passwords on other services.

7. Educate and Support Others

If you manage teams or support family members:

- Encourage the use of password managers.
- Promote MFA adoption.
- Run short awareness sessions on recognising phishing attempts that try to steal credentials.
- Lead by example - visibly using good password practices makes others more likely to follow.

CHECKLIST



Quick Checklist for Good Password Health

- ☐ Use a password manager
- ☐ Create long, unique passwords (or passphrases) for every account
- ☐ Enable MFA (preferably app-based or hardware keys) on important accounts
- ☐ Avoid password reuse
- ☐ Check for compromised passwords regularly
- ☐ Update passwords after known breaches
- ☐ Use passkeys where available

Final Thought

Good password hygiene is about reducing risk through consistent, practical habits rather than aiming for perfection. By using a password manager, enabling multi-factor authentication, and avoiding reuse, you dramatically lower the chances of falling victim to credential-based attacks.

Treating passwords with the same care as other aspects of personal and organisational security helps protect both individual accounts and the wider systems they connect to.

At ICTS Legal Services, we continue supporting pension funds, their providers, and trustees with compliance, assessments, risk management plans, training (ICTS Academy), and resilience strategies.

Questions or contributions? Contact us at ICTS Legal Services.

Breaking out of the box on risk management

Contact
Leon Greyling
082 464 5786
greylingl@icts.co.za



Hacking Poem of the Month:

There once was a young hacker so bold,
Who thought every system would fold.
He cracked them with ease,
Stole data like a breeze...
Now he counts the years till he's old.

No hoodie can hide what he's done,
No script can make the guilt run.
The screen's gone dark,
His cell is the new mark.
And the only code left is "none."

Stay vigilant, stay resilient.

The ICTS Legal Services Team



What The Hack is published monthly or when required. Past editions available on request.
This newsletter is for information purposes only and does not constitute legal advice.