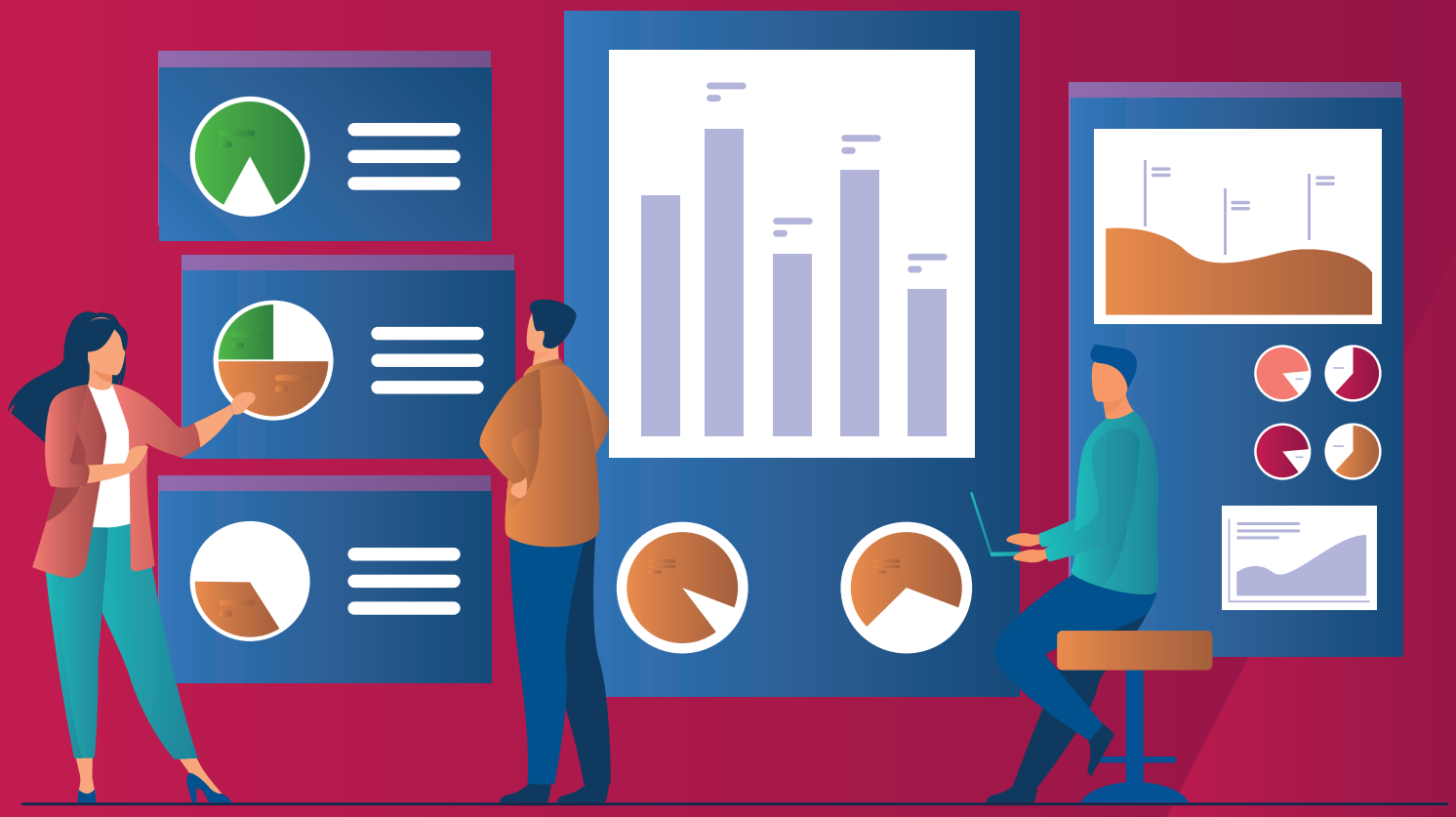
VERIFILE
Accurate data. Meaningful relationships.

5 Red Flags Your Screening Vendor Could Put You at Risk

How to tell if your background-check provider is exposing you to compliance and security risks.



Introduction

98%

of organisations have a vendor that has suffered a breach

Recent events show that even trusted background check providers can suffer serious data breaches. In June 2025, a UK vendor was compromised after attackers gained access through stolen login credentials. Personal data such as names, birth dates and national ID numbers was exposed. Unfortunately, this is not an isolated case: 98% of organisations have at least one vendor that has experienced a data breach in the past two years.

For HR, talent and compliance leaders, the warning is clear: your background screening provider's security lapses can quickly become your problem. A vendor's data leak can lead to GDPR fines of up to 4% of global turnover, legal liabilities, and lasting reputational damage.

This guide sets out five warning signs to look for in your current vendor. Written for non-technical professionals, it helps you ask the right questions without needing to be an IT expert. You'll also find a practical checklist and even a template email you can send to your vendor. Use this guide to spot red flags early and keep candidate data safe.

WARNING SIGN 1:
No Recognised Security Certifications

One of the clearest red flags is a vendor that lacks formal security certifications or compliance standards. Credible screening providers invest in **internationally recognised frameworks** to keep data safe.

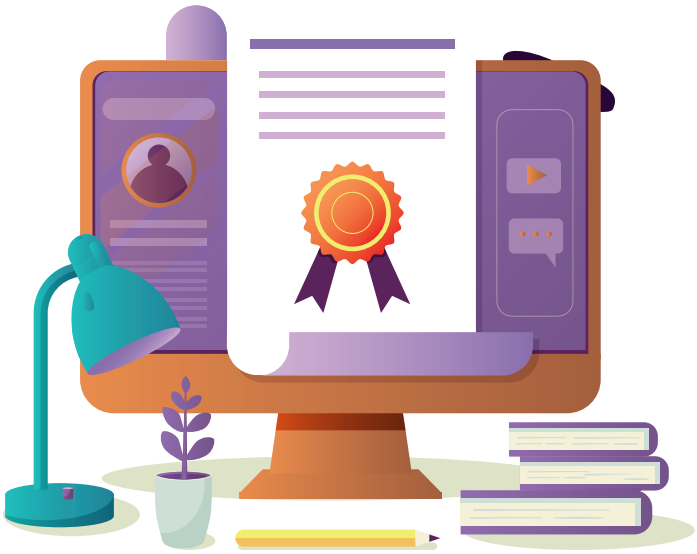
Leading providers often hold ISO 27001 for information security management, ISO 22301 for business continuity and Cyber Essentials Plus in the UK, which involves an external audit of their defences against common cyber threats. Industry accreditations like the **Professional Background Screening Association (PBSA)** are another signal that a provider has been independently assessed for data security and compliance.

If your vendor cannot demonstrate comparable credentials or regular independent audits, it suggests a relaxed approach to data protection.

This is essentially asking you to "just trust us" with sensitive candidate data.

Even then, certifications are only a baseline. A UK screening provider that suffered a serious data breach in 2025 had ISO 27001 and Cyber Essentials Plus, but weak credential security still led to compromise. This shows that certifications must be actively upheld and updated, not just held for display. A good test is to ask vendors how they maintain their controls between audits.

At Verifile, certifications are treated as a starting point rather than a badge. We hold 10 certifications, including ISO 27001, ISO 22301, PBSA accreditation, NSI Gold (BS7858 staff vetting), and Cyber Essentials Plus, and we focus on embedding the practices behind them in day-to-day operations.



Ask Yourself:

- Which certifications has our vendor achieved?
- Who audits their controls, and how often?
- How do they maintain their security controls between audits?

WARNING SIGN 2:
Poor Data Handling Practices

Another red flag is how a vendor collects, transmits, and stores the personal data you send them. If you are asked to upload documents via unencrypted links or if results are shared in spreadsheets, this is a clear warning sign. Sensitive information such as IDs, forms and criminal record results should always be transmitted and stored in an encrypted, access-controlled system. Leading providers use secure online portals, encrypt data both in transit and at rest, and restrict access so only authorised personnel can view it.

By contrast, reliance on manual processes or insecure workarounds significantly increases risk. In one recent breach, a single stolen set of admin credentials was enough to expose large volumes of data. Strong login security including multi-factor authentication (MFA), single sign-on (SSO), and monitoring for unusual access can help prevent such incidents. If your provider lacks these protections, it is a serious concern.

Reliable vendors will be able to explain their data handling protocols clearly, covering encryption, secure infrastructure, regular vulnerability testing and compliance with retention rules. If a vendor struggles to answer these questions, or if you find yourself adding ad-hoc security measures to compensate for their gaps, treat it as a red flag. Convenience should never come at the expense of security.

At Verifile, we use encrypted systems for all data transfers and storage, enforce strict access controls, and continually test our platforms against evolving threats, ensuring customer and candidate data is protected at every

Ask Yourself:

- How does our vendor ensure candidate data is encrypted in transfer and storage?
- What login security measures (MFA, SSO, monitoring) do they provide?
- Do they rely on manual processes that could expose data?

WARNING SIGN 3:
Lack of Transparency and Accountability

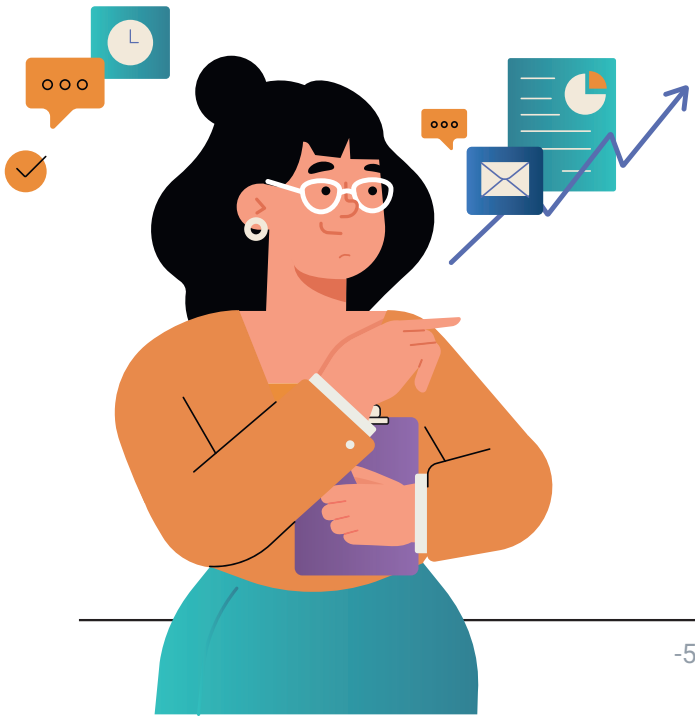
A trustworthy screening provider should be open about their security and privacy practices. If a vendor avoids questions, provides vague answers, or resists sharing documentation, it is a red flag. Transparency is closely tied to accountability: reliable providers make their practices visible and verifiable.

Accreditations such as the PBSA require rigorous independent audits across data security, compliance, and quality. Leading providers also commission external penetration tests or publish their security commitment to demonstrate confidence in their safeguards. These steps show a willingness to be scrutinised and a culture of accountability.

By contrast, if a vendor cannot provide evidence of third-party assessments or shows no plans to pursue them, it suggests security is not a priority at leadership level. Consider also their behaviour in practice: would they inform you promptly of a breach, or attempt to keep it quiet? How they respond under pressure reveals their true stance on accountability.

Another subtle warning sign is a vendor that signs complex data protection terms without question. Reputable providers will review and, if needed, negotiate obligations to ensure they can meet them. A company that agrees immediately to everything may not have carefully considered the requirements, which could create problems later.

At Verifile, we view transparency as a core part of partnership. We welcome due diligence, are open about our security posture, and proactively undergo audits and accreditations to validate our practices.



Ask Yourself:

- Has our vendor ever disclosed a data breach or incident, and how was it handled?
- Can they share independent security assessments or accreditations?
- Do they meaningfully review contractual security and compliance obligations?

WARNING SIGN 4:
Poor Data Handling Practices

A trustworthy screening provider should be open about their security and privacy practices. If a vendor avoids questions, provides vague answers, or resists sharing documentation, it is a red flag. Transparency is closely tied to accountability: reliable providers make their practices visible and verifiable.

Accreditations such as the PBSA require rigorous independent audits across data security, compliance, and quality. Leading providers also commission external penetration tests or publish their security commitment to demonstrate confidence in their safeguards. These steps show a willingness to be scrutinised and a culture of accountability.

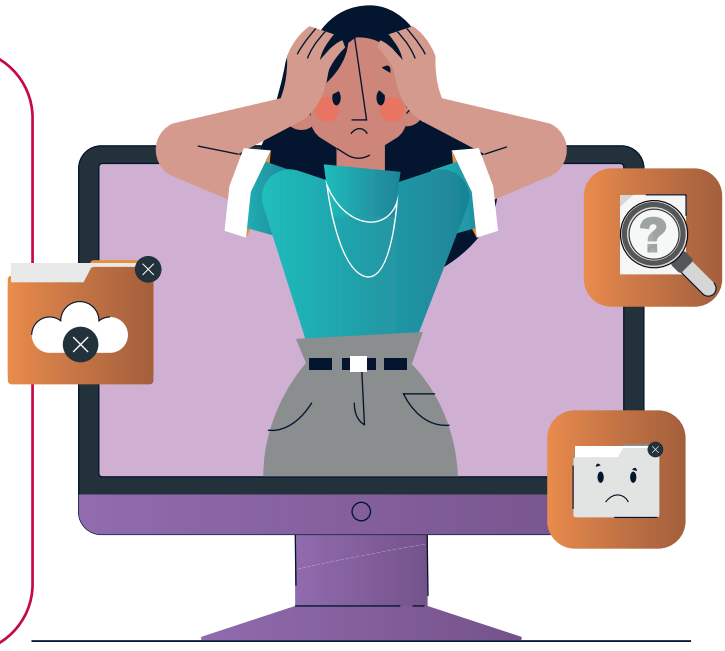
By contrast, if a vendor cannot provide evidence of third-party assessments or shows no plans to pursue them, it suggests security is not a priority at leadership level. Consider also their behaviour in practice: would they inform you promptly of a breach, or attempt to keep it quiet? How they respond under pressure reveals their true stance on accountability.

Another subtle warning sign is a vendor that signs complex data protection terms without question. Reputable providers will review and, if needed, negotiate obligations to ensure they can meet them. A company that agrees immediately to everything may not have carefully considered the requirements, which could create problems later.

At Verifile, we view transparency as a core part of partnership. We welcome due diligence, are open about our security posture, and proactively undergo audits and accreditations to validate our practices.

Ask Yourself:

- Does our vendor support SSO, MFA, and up-to-date encryption?
- How frequently is their system updated or penetration-tested?
- Are they a tier-one provider with direct integrations, or do they resell another company's services?



WARNING SIGN 5:
Neglect of Data Protection Compliance

A screening vendor that does not proactively comply with data protection laws is a serious liability. HR and recruitment functions handle highly sensitive personal information, and under GDPR and the UK Data Protection Act this brings strict obligations. Your vendor should act as a compliance partner, helping you meet legal requirements rather than creating new risks.

Red flags include vendors who cannot align with your organisation's data retention and deletion requirements, leaving candidate data stored for longer than is lawful or appropriate. Others may neglect to obtain proper consent from candidates, or be unable to support you in responding to data subject requests. Any of these gaps could expose your organisation to fines and reputational damage.

Jurisdiction is another critical factor. You should know exactly where your data is stored and processed, and whether it ever leaves the UK or EU. If a vendor cannot explain this clearly, or relies on transfers to jurisdictions without equivalent protections, you risk breaching GDPR transfer rules. Similarly, vendors must be prepared to notify you of a breach within the 72-hour window required by law. A partner who cannot commit to this is a clear risk.

Culture also matters. Do they train staff on confidentiality? Do they vet employees who handle sensitive data? A vendor indifferent to these basics may be exposing you to regulatory and reputational harm.

At Verifile, compliance is embedded in our culture. We sign robust Data Processing Agreements, align with client-specific data retention and deletion schedules, and vet all employees to BS7858 standards, achieving NSI Gold accreditation. This ensures that client and candidate data is handled securely, lawfully, and with the highest standards of care.

Ask Yourself:

- Has our vendor ever disclosed a data breach or incident, and how was it handled?
- Can they share independent security assessments or accreditations?
- Do they meaningfully review contractual security and compliance obligations?

SELF-CHECK:
Do You Know How Secure Your Vendor Really Is?

Beyond questioning your vendor, it is important to test your own knowledge of their security posture. Use this quick self-check to see where the risks lie:

- Do I know which security certifications my vendor holds and how often they are audited?
- Am I confident candidate data is encrypted in transfer and storage, and not exposed in insecure systems?
- Does the platform support SSO or MFA, and is it kept up to date with patches and tests?
- Has the vendor openly shared policies, incident history and compliance measures with us?
- Do I know their data retention and deletion approach, and are they aligned with our requirements?
- Am I sure checks are performed directly by them, not through resellers?

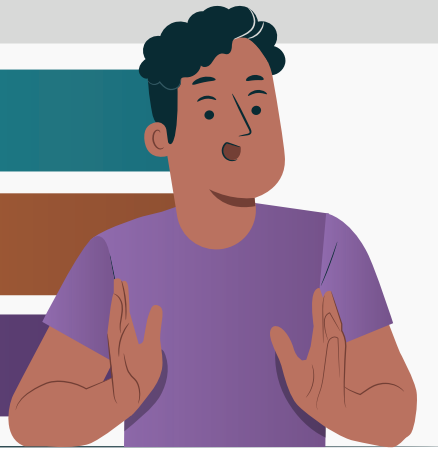
YES	MAYBE	NO
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐

Scoring:

Mostly Yes = **Low risk**

Some No/Maybe = **Medium risk; areas need clarification.**

Many No = **High risk; vendor may be exposing you to serious security or compliance issues.**



TAKING ACTION:
Vendor Security & Compliance Checklist

When evaluating your current or prospective screening provider, use this checklist to test their security and compliance posture. Each question highlights a potential red flag if the answer is weak or unclear.

Ask		Red Flag
Which certifications or audits do you currently hold (e.g. ISO 27001, ISO 22301, Cyber Essentials Plus)?	**Certifications**	No external certifications, or reluctance to share details.
How do you ensure candidate data is encrypted in transfer and at rest? Who can access it?	**Data Security**	Reliance on unencrypted email, shared drives, or weak access controls.
Does your platform support MFA or SSO? How do you monitor for unauthorised access?	**Authentication**	Password-only logins, no recent security testing, or lack of monitoring tools.
Have you experienced a data breach? What is your notification process?	**Incident Response**	No clear answer, or a history of poor disclosure.
Will you sign a GDPR-compliant Data Processing Agreement and support our retention, deletion and data subject rights?	**Compliance**	Unfamiliar with GDPR obligations or unwilling to align with your compliance needs.
Do you perform checks in-house using your own systems, or do you resell another provider's services?	**Service Delivery**	Data passing through unknown third parties, with no direct oversight.
How do you vet and train your staff who handle sensitive data?	**Internal Culture**	No internal vetting, weak training, or lack of security culture.

VENDOR DUE DILIGENCE
Email Template

To get clarity from your vendor, here is a ready-to-use template:

Subject: Security and Compliance Inquiry – [Your Company Name]

Dear [Vendor Name] Team,

As part of our due diligence, we are reviewing the data security and compliance measures of our screening providers. Please share details on the following:

- Certifications & Audits: Which certifications do you hold (e.g. ISO 27001, ISO 22301, Cyber Essentials Plus)? When was your last independent audit, and by whom?
- Data Protection: How is sensitive candidate data protected in your systems? Is it encrypted in transit and at rest? What access controls are in place?
- Authentication & Access: Does your platform support SSO? What authentication methods are in use? Do you provide audit logs and role-based access?
- Incident History & Response: Have you experienced any breaches or incidents? If so, how were they handled? What is your breach notification process?
- Compliance: Will you sign a GDPR-compliant Data Processing Agreement and align with our retention and deletion requirements? How do you support data subject requests?
- Service Delivery: Do you conduct all checks in-house using your own platform, or do you outsource to other providers? If third parties are involved, how are they vetted?

Internal Security Practices: How do you vet your staff who handle client data, and what training do they receive?

We appreciate your transparency in providing this information to help us ensure strong security and compliance.

Sincerely,

[Your Name]
[Your Title]
[Your Company]

CONCLUSION
& Next Steps

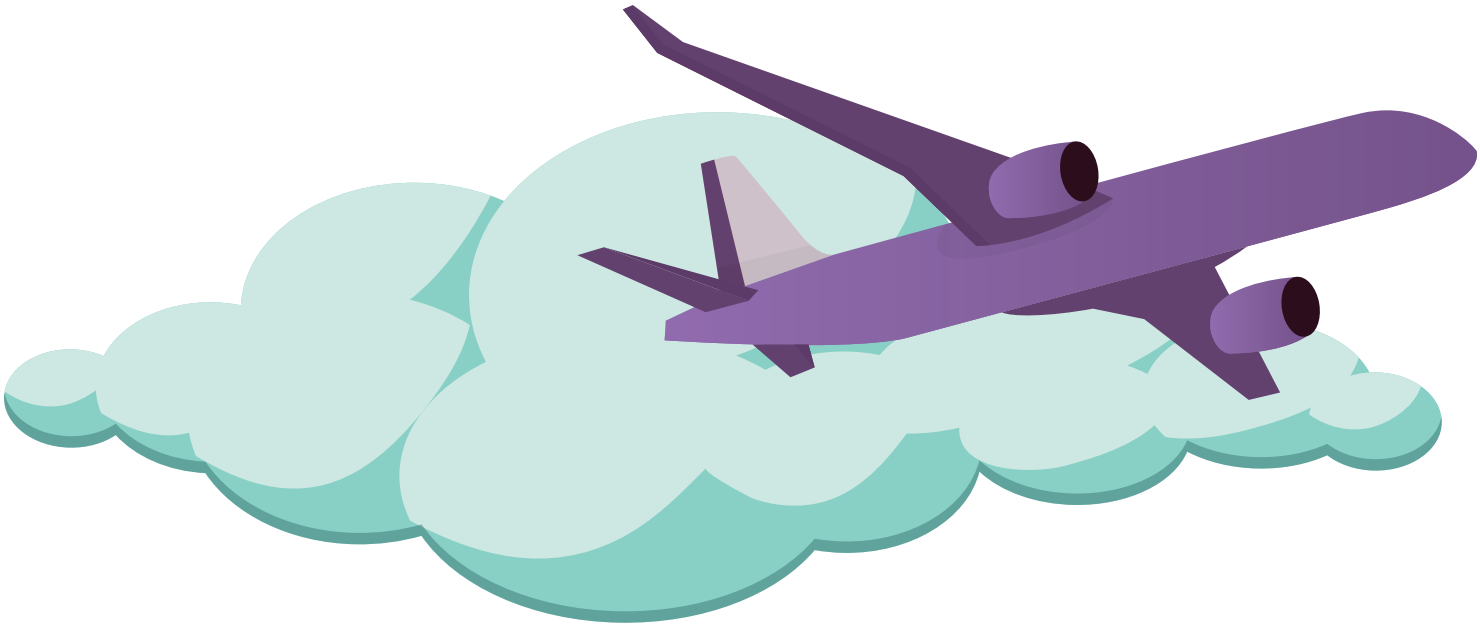
In an era of escalating cyber threats and strict data protection laws, HR and compliance leaders cannot afford to ignore red flags in their background screening providers. Your vendor should be a security asset, not a liability.

The good news is that raising your standards does not have to mean paying more. For example, Verifile offers a price-match guarantee for like-for-like services, so upgrading your security posture does not have to increase your budget. More importantly, the cost of complacency is far higher: a single breach could mean regulatory fines, lawsuits, and reputational damage.

By using the red flags and tools in this guide, you've taken the first step toward stronger data security in hiring. If you spot gaps with your current provider, don't ignore them — raise the issues, demand improvements, or consider switching to a vendor that treats security and compliance with the seriousness it deserves.

Next Steps:

1. Review your current provider against the five red flags.
2. Use the self-check and due diligence email to identify gaps.
3. Take action now before a breach forces your hand.



VERIFILE

Accurate data. Meaningful relationships.

READY TO STREAMLINE YOUR SCREENING PROCESS?

Let us help you transform your HR operations.

Verifile HQ

5 Franklin Court Stannard Way Priory Business Park Bedford MK44 3JZ

Sales

+44 (0) 1234 60 80 90

sales@verifile.co.uk

Candidate Support

+44 (0) 1234 339 300

hello@verifile.co.uk

Client Services

+44 (0) 1234 339 350

service@verifile.co.uk

General Enquiries

+44 (0) 1234 339 339

info@verifile.co.uk

www.verifile.co.uk