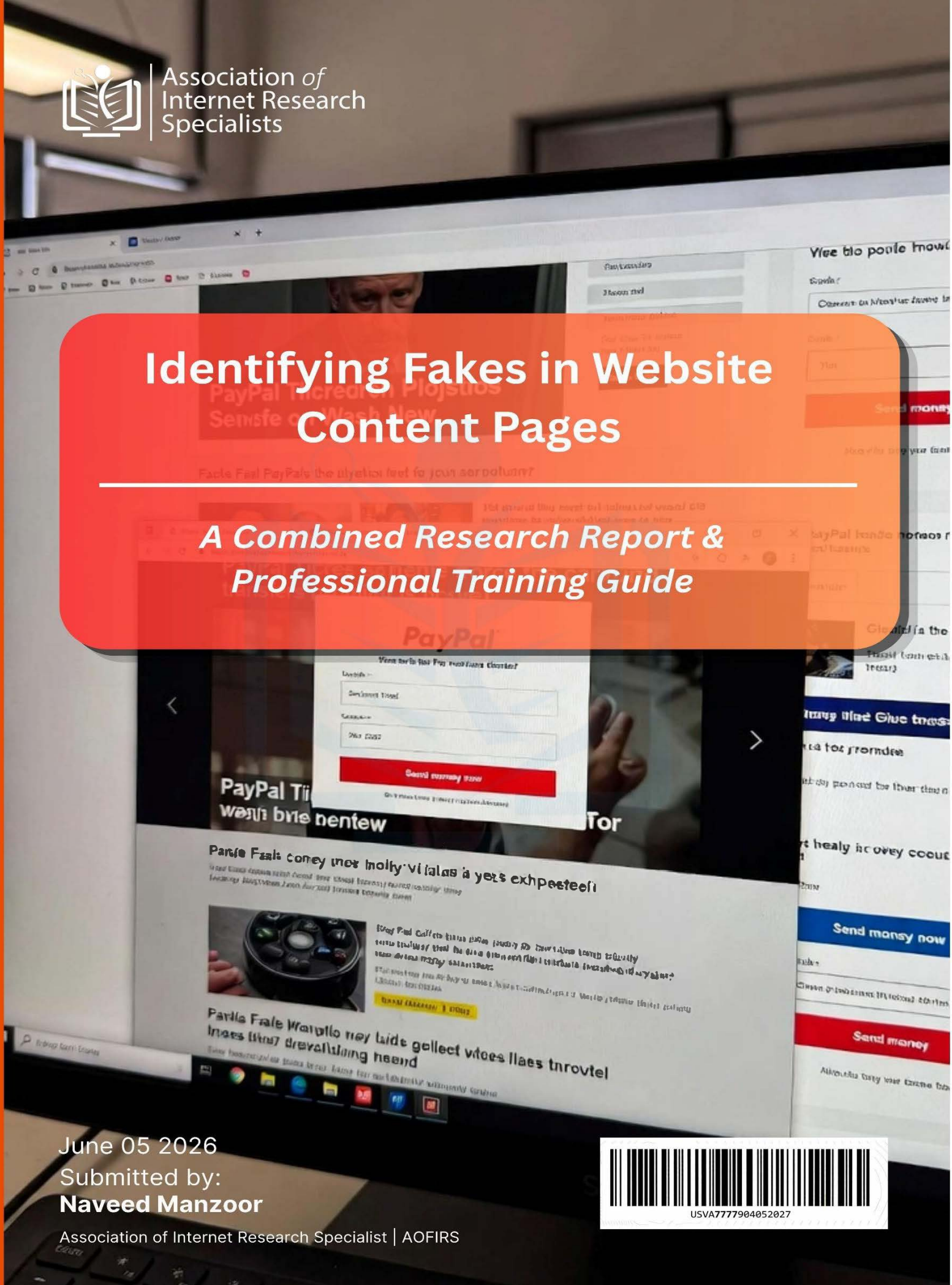
Association *of* Internet Research Specialists

Identifying Fakes in Website Content Pages

A Combined Research Report & Professional Training Guide



June 05 2026

Submitted by:
Naveed Manzoor
Association of Internet Research Specialist | AOFIRS

USVA7777904052027

© 2026 Association of Internet Research Specialists (AOFIRS) | aofirs.org | All Rights Reserved

© 2026 Association of Internet Research Specialists (AOFIRS) | aofirs.org | All Rights Reserved

ASSOCIATION OF INTERNET RESEARCH SPECIALISTS

Certified Internet Research Specialist (CIRS™) Program

TRAINING MODULE 9 • UNIT 23

Identifying Fakes in Website Content Pages

A Combined Research Report & Professional Training Guide

Research Coverage: AI-Era Fake Website Detection • Digital Forensics • OSINT Verification

Updated with 2025–2026 Findings & Current Detection Tools

© 2026 Association of Internet Research Specialists (AOFIRS). All Rights Reserved.
aofirs.org • Mississauga, Ontario, Canada

TABLE OF CONTENTS

Executive Summary 4
Introduction: The Evolving Landscape of Fake Websites 5
Section I: Website Homepage Analysis 6
1.1 Logo Verification 6
1.2 Homepage Layout and Navigation 7
Section II: Policy and Legal Pages 8
2.1 Plagiarism in Privacy Policies and Terms of Use 8
Section III: About Us Page Analysis 9
3.1 Plagiarism and Content Authenticity 9
3.2 Completeness and Information Verification 9
3.3 Language Quality and Grammar 10
3.4 Over-Abundance of Advertisements 10
3.5 Digital Footprint Verification 10
3.6 Authentic Images and Profile Photo Checks 11
Section IV: Products and Services Verification 14
4.1 E-Commerce Fraud Overview 14
4.2 Consumer Complaint Patterns 14
4.3 How to Spot Fake or Counterfeit Products Online 15
Section V: Checkout and Payment Verification 17
5.1 Invoice and Transaction Security 17
5.2 HTTPS, SSL/TLS and Digital Certificates 17
5.3 Trust Seals and Payment Gateway Verification 18
Section VI: Website Content Analysis 19
6.1 Text, Spelling and Plagiarism 19
6.2 Video Content and Deepfakes 19
6.3 Contact Information Verification 20
6.4 Copyright Status Verification 22
Section VII: Profile Photos and Image Verification 23
7.1 Reverse Image Search and Stock Photo Identification 23
7.2 Digital Image Tampering Detection 25
Section VIII: Social Media and Background Checks 26
Section IX: Third-Party Verification and Trust Marks 27
9.1 Affiliates, Partners and Authorized Re-Sellers 27
9.2 Trust Mark Logos and Accreditation Bodies 28
9.3 Accreditation vs. Licensing vs. Certification 29
Section X: Customer Reviews and Testimonials 30
Section XI: AI-Era Threats and Advanced Detection (2025–2026) 33

11.1 Generative AI and Instant Website Cloning 33
11.2 AI Cloaking: Serving Different Content to Crawlers 34
11.3 Deepfake Fraud: Statistics and Impact 34
11.4 New Detection Tools and Techniques for Researchers 35
11.5 Browser-Based Security Indicators in 2025–2026 36
Section XII: Researcher Training Quick-Reference Checklist 37
References (APA) 39
Index 41

Executive Summary

This combined Research Report and Training Guide constitutes Unit 23 of the Certified Internet Research Specialist (CIRS™) Program developed by the Association of Internet Research Specialists (AOFIRS). It addresses one of the most critical competencies for professional online researchers: the systematic identification of fake, fraudulent, or deceptive websites.

Fake websites represent a sophisticated and growing threat to consumers, businesses, researchers, and institutions worldwide. The Anti-Phishing Working Group (APWG) identified nearly 1.8 million new phishing and fake websites in the latter half of 2024 alone. By 2026, generative AI tools have dramatically lowered the barrier to creating convincing fake sites—enabling the rapid cloning of entire websites, including layouts, SSL certificates, trust seals, and policy pages, within minutes.

This report provides a comprehensive, structured methodology for evaluating every major component of a website—from homepage logos and navigation to checkout processes, contact information, and third-party trust marks. Each section integrates foundational techniques developed through AOFIRS research methodologies with new 2025–2026 findings on AI-assisted fraud, deepfake proliferation, and browser-based detection tools.

Metric	Value	Source	Year
New phishing sites per half-year	~1.8 million	APWG	2024
Deepfakes shared online	8 million projected	European Parliament Research Service	2025
Deepfake fraud increase	+2,137% over 3 years	Keepnet Labs	2026
AI-built phishing sites	6–7% of all phishing infrastructure	Panda Security	2026
Human deepfake detection accuracy	55.54% (near chance)	iProov Study	2025
US deepfake-related financial losses	$1.1 billion	Keepnet Labs	2025

Table 1. Key 2025–2026 Statistics on Fake Website and Deepfake Threats

Professional internet researchers who complete this unit will be equipped to conduct structured website audits across all major content categories, apply both manual and tool-assisted verification techniques, and produce evidenced assessments of website legitimacy—skills essential to investigative research, due diligence, competitive intelligence, and fraud prevention.

Introduction: The Evolving Landscape of Fake Websites

The proliferation of fake websites is not a new phenomenon—fraudsters have exploited the anonymity and accessibility of the World Wide Web since its earliest days. However, the technological arms race between legitimate web operators and malicious actors has reached a new inflection point with the mass adoption of generative artificial intelligence (AI) tools.

Historically, creating a convincing fake website required programming knowledge, graphic design skills, and at least a modest time investment. Today, tools such as Vercel's v0 and other large language model-powered website generators allow anyone—regardless of technical ability—to clone a site by typing a simple natural-language prompt. The AI replicates design, layout, search engine optimization (SEO) structure, and even trust signals such as cookie banners and return policy pages. As Panda Security (2026) reports, one analysis found AI-built sites now accounting for 6–7% of all phishing infrastructure (pandasecurity.com, 2026).

Beyond cloning, adversaries exploit a new technique called "AI cloaking," wherein a website serves entirely different content to AI-driven web crawlers (used by search engines and fact-checking tools) than to human visitors. Research by SPLX demonstrated this convincingly against tools including Atlas and ChatGPT (Dark Reading, 2025). This means that automated trust-verification tools can be systematically deceived.

Against this backdrop, the methodology detailed in this training module becomes even more indispensable. A trained researcher who applies the structured, multi-layered verification approach described in the following sections is significantly harder to deceive than any automated scanner or casual web user. This unit covers the following major areas of website evaluation:

- Homepage design, logos, and navigation integrity
- Policy and legal page authenticity and plagiarism detection
- About Us and management team verification
- Products, services, and e-commerce fraud indicators
- Payment and checkout security validation
- Content quality, video deepfakes, and contact information
- Image verification, stock photo detection, and digital tampering
- Social media footprint and background checks
- Third-party affiliations, trust marks, and accreditation verification
- Customer review and testimonial authenticity
- AI-era detection methods for 2025–2026

Section I: Website Homepage Analysis

1.1 Logo Verification

The homepage of any website is the digital equivalent of a storefront window—it creates the first and often most lasting impression. For fake website operators, speed and low cost are paramount; logos are therefore among the first elements where fraudulent intent becomes visible to the trained eye.

Logos on fake websites are commonly copied directly from the internet and altered minimally—typically only the business or domain name is changed. Images downloaded from the web without purchasing the original high-resolution asset invariably suffer from degraded pixel quality. When magnified, these low-resolution copies exhibit visible blurring, pixelation at edges, and inconsistent anti-aliasing. Only logos produced from scratch in professional applications (such as Adobe Photoshop, Adobe Illustrator, or CorelDraw) or purchased from stock image libraries at high resolution will render crisply at all zoom levels.

A practical verification technique is to conduct a reverse image search on the logo using Google Images, TinEye, or Bing Visual Search. If the logo returns results pointing to stock image repositories (such as Shutterstock, Getty Images, or Adobe Stock) or to a different company than the one being investigated, this constitutes a significant red flag.

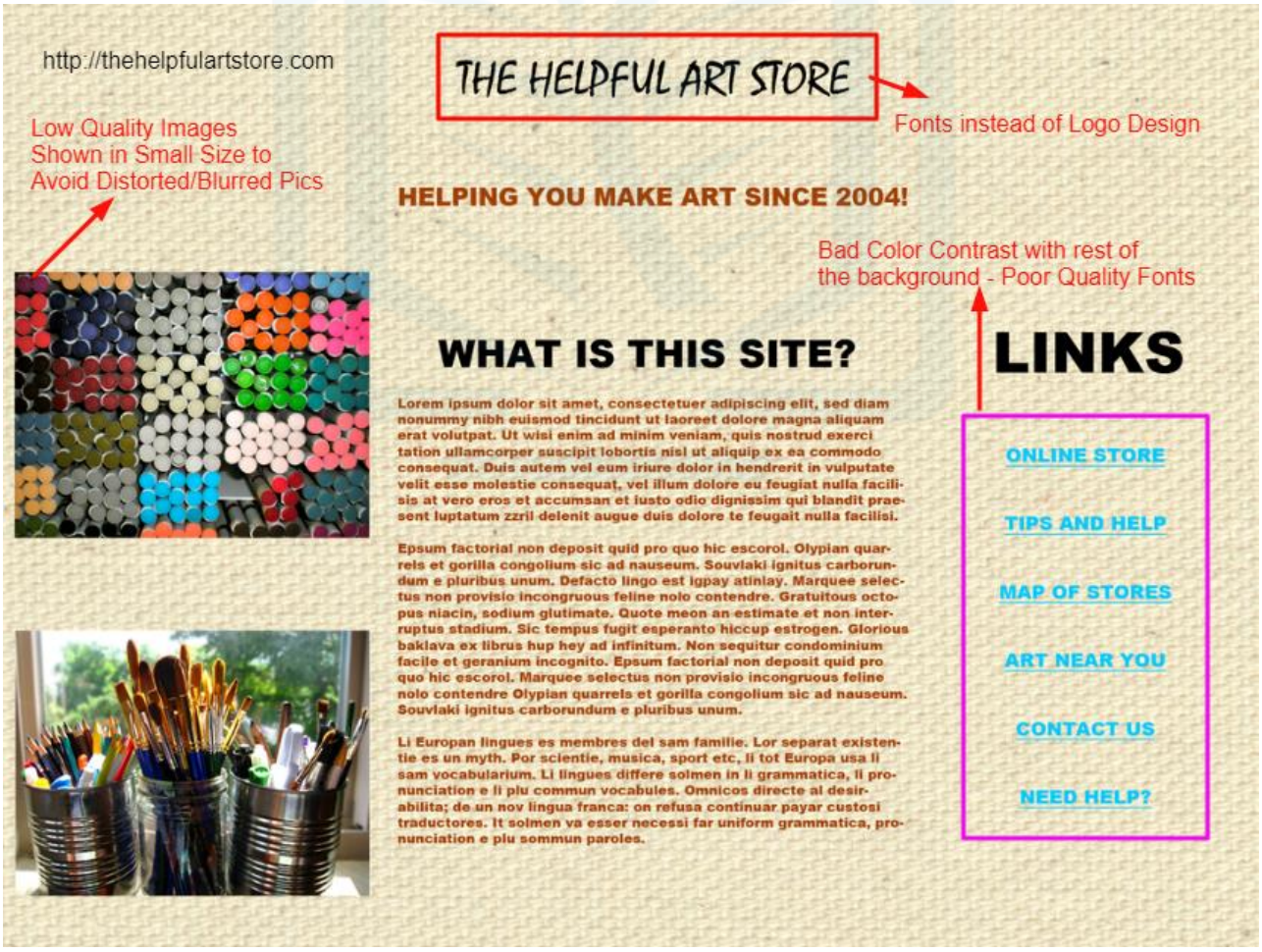


Figure 8. Example of Image Search Results: Original logo in high-quality resolution (left) versus low-quality copy (right). The high-quality version was sourced from Shutterstock, indicating the fake website operator did not license the original artwork.

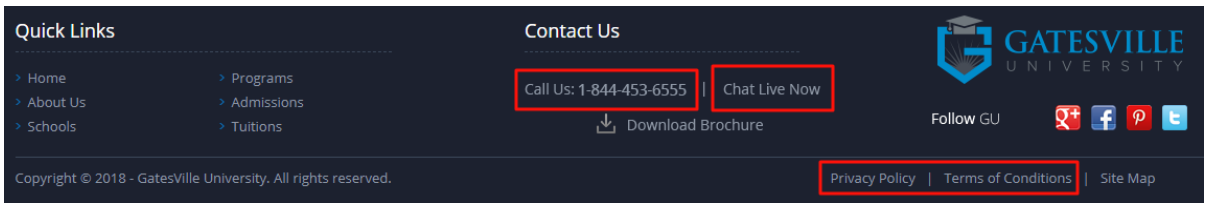


Figure 9. Example of a Fake Logo in Low Resolution. Zooming in reveals blurred and disparate pixel quality characteristic of an improperly downloaded or copied image.

CIRS™ RESEARCHER TIP — Logo Verification Quick Steps

1. Right-click the logo on the suspect website and select “Open image in new tab” to view the raw URL and file name. 2. Upload or drag the logo image into Google Images, Bing Visual Search, or TinEye. 3. Review results for stock image library matches or appearances on unrelated websites. 4. Note whether the returned high-resolution version matches the claimed brand identity. 5. Check if the same image file name reappears across multiple unrelated domains—a common sign of mass-deployed fake sites.

1.2 Homepage Layout and Navigation

A legitimate website reflects sustained investment in its digital presence. Its design is intentional: layout, typography, color palette, and navigation are coherent and aligned with the brand’s identity. Fake websites, by contrast, often reveal their origins through a number of structural and aesthetic anomalies.

Key Indicators of Fraudulent Homepage Design

Dead links and broken navigation: Fake sites constructed in haste frequently contain navigation elements that do not function, or link to placeholder pages. Test every navigation menu item methodically.

Static images replacing HTML elements: Some fraudulent websites substitute entire navigation bars or interactive elements with single flat image files. These cannot be selected as text and may not function as links. Right-clicking a suspicious menu element and selecting “Inspect” reveals whether it is a genuine HTML element or an image.

Homepage-as-image construction: Particularly low-effort fake sites build the entire homepage as one large image file rather than structured HTML. This prevents text selection, copy-paste testing, and accurate spell-checking by browsers.

Aggressive monetization design: Fake sites that prioritize revenue extraction funnel visitors directly to payment pages. Excessive pop-ups, unsolicited discount offers, and countdown timers creating artificial urgency are red flags documented by the FTC (2025).

Mismatched branding: Check that the logo colors match the site’s color theme. Legitimate businesses maintain strict brand guidelines; cloned sites often apply logos to poorly matched backgrounds.

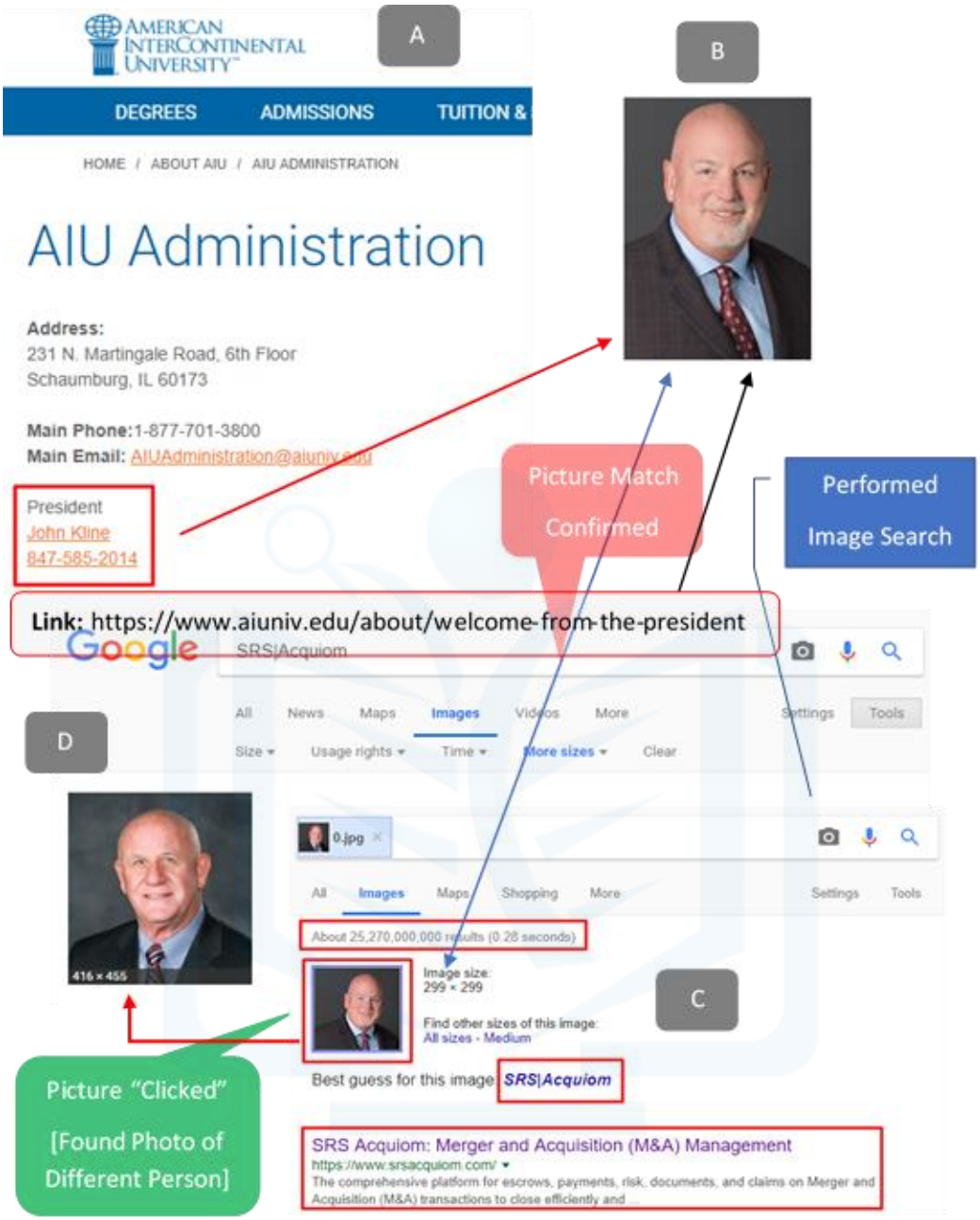


Figure 10. Example of a Fake Website Homepage Constructed Largely from a Single Image. Note the absence of interactive HTML elements, functional navigation, and structural HTML coding. The homepage serves as a visual trap rather than a navigable experience.

2025–2026 UPDATE — AI-Cloned Homepages

Generative AI website cloning tools (e.g., Vercel v0, various LLM-based site builders) can now replicate a legitimate homepage's complete visual design, CSS layout, meta tags, and even simulated testimonials within seconds. These AI clones are increasingly indistinguishable from originals to casual users. Researchers should use tool-assisted verification (outlined in Section XI) in addition to visual inspection.

Section II: Policy and Legal Pages

2.1 Plagiarism in Privacy Policies and Terms of Use

Legal and policy pages—including Privacy Policies, Terms and Conditions, Terms of Use, and Disclaimers—are compulsory components of legitimate websites operating in most jurisdictions. Their presence signals accountability; their absence or plagiarized content signals the opposite.

Fake website operators frequently plagiarize these documents for two reasons: (1) they lack the legal expertise to draft original policies, and (2) speed of deployment takes priority over authenticity. A variety of free policy generator tools (such as freeprivacypolicy.com) are routinely exploited by fraudulent sites because they produce template language that is immediately identifiable when cross-checked against other sites.

To detect plagiarized policies: copy a distinctive phrase of 8–15 words from the suspect site's privacy policy and perform an exact-phrase Google search by enclosing the phrase in quotation marks. If the identical text appears verbatim on multiple unrelated websites, the content is plagiarized.

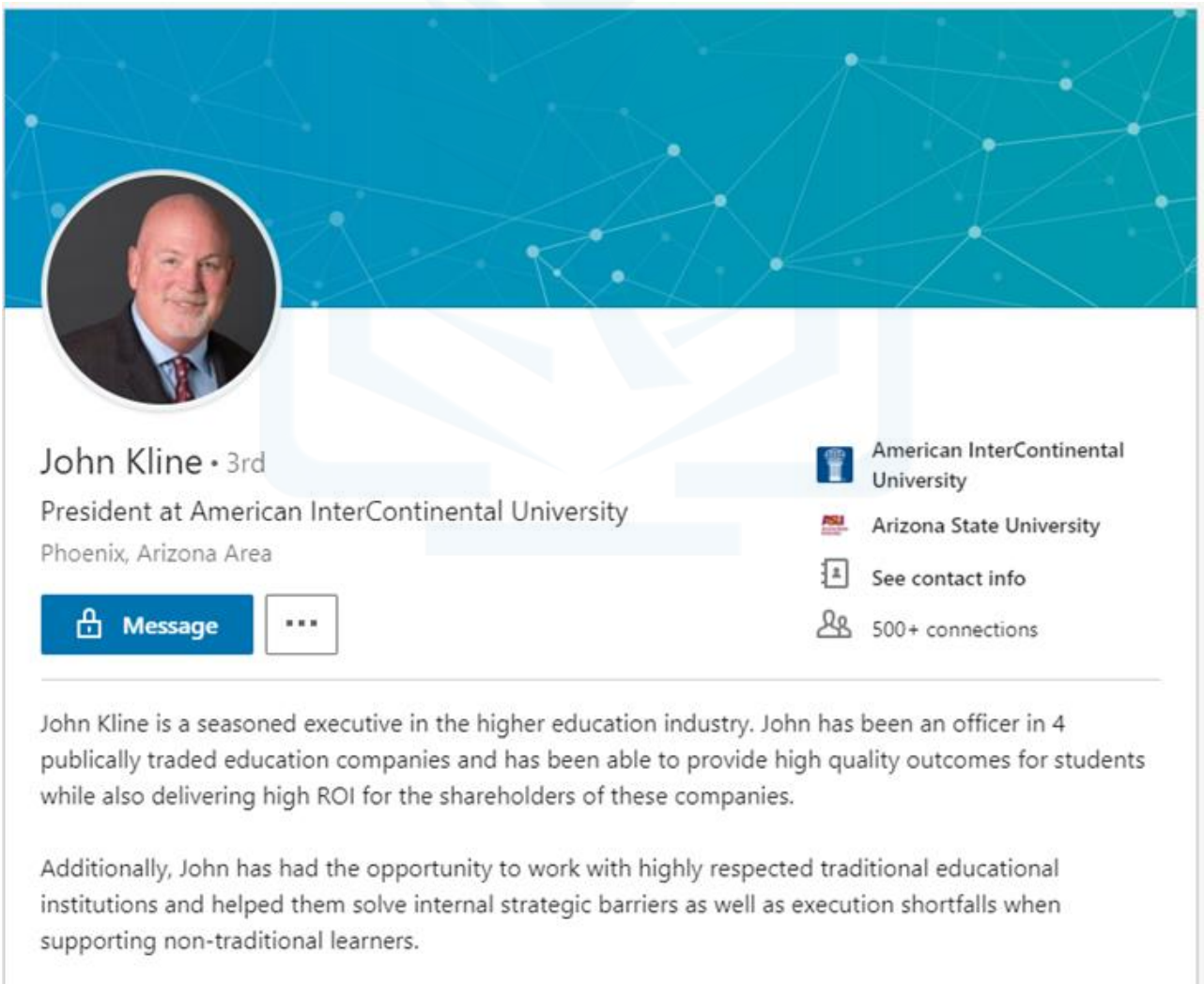


Figure 11. Plagiarism Detection Result. A line of text from the Privacy Policy of "Gatesville University" was searched in Google with exact phrasing. The identical wording was found verbatim in the Privacy Policy of another, unrelated educational institution—a strong indicator of plagiarized content and lack of original policy authorship.

Beyond simple copy-paste plagiarism, researchers should examine whether the policy content is internally consistent. For example, a site claiming to be a Canadian-based educational institution should not reference "FERPA" (a US federal education law) without acknowledging the jurisdictional distinction. Similarly, a policy referencing regulations such as GDPR (EU) or PIPEDA (Canada) should reflect operational practices consistent with those regulatory frameworks.

The 2024 Digital Services Act (EU) and evolving US state privacy laws (CCPA, Virginia CDPA) have increased the specificity required in legitimate privacy policies. Sites that post generic 2019-era boilerplate unchanged in 2025–2026 may be operating illegally or fraudulently regardless of their geographic claims.

Section III: About Us Page Analysis

The “About Us” page is the public face of an organization’s identity online. It answers fundamental questions about who operates the website, what their credentials are, and what value the organization provides. For a professional researcher, this page is a primary intelligence source—and one of the most revealing when a site is fraudulent.

3.1 Plagiarism and Content Authenticity

The “About Us” page of a fake website is often populated in one of two ways: (1) through direct plagiarism from similar organizations, or (2) through generic, templated content that lacks specificity. While plagiarism of policy pages is a technical red flag, plagiarism of the “About Us” page is a more serious indicator because it directly misrepresents the organizational identity.

Researchers should extract 2–3 distinctive phrases from the “About Us” content and run quoted searches in Google. Large language model tools can now generate grammatically correct, superficially convincing “About Us” copy on demand; detection therefore requires cross-referencing claimed facts (founding dates, awards, leadership names) with independent authoritative sources.

3.2 Completeness and Information Verification

A legitimate “About Us” page contains substantive, verifiable information. Researchers should evaluate the page against the following five criteria, with a score of 3/5 or greater suggesting authenticity and fewer than 3/5 warranting further investigation:

1. Mission, objectives and expressed organizational philosophy
2. Business structure details (formation date, corporate type: corporation, LLC, affiliate, subsidiary, etc.)
3. Photos of directors and management team with verifiable credentials
4. Verified email addresses with company domain names (not generic Gmail/Yahoo)
5. Logos of business partners, awards with verifiable provenance and accreditation bodies

3.3 Language Quality and Grammar

Grammar, spelling, and language consistency are reliable proxies for the quality of operational investment a website represents. A legitimate business—particularly in education, finance, healthcare, or professional services—would not publish content with repeated grammatical errors, inconsistent tenses, or non-idiomatic English. Systemic errors concentrated on “About Us” and policy pages are especially significant because these are the pages that receive the most editorial attention on legitimate sites.

With AI content generation now pervasive, researchers should be alert to a new variant: content that is grammatically perfect but semantically hollow—plausible-sounding but devoid of verifiable specifics. Well-structured LLM-generated copy that makes no falsifiable claims is increasingly characteristic of sophisticated fake sites.

3.4 Over-Abundance of Advertisements

Advertisements are a normal component of many legitimate websites, particularly content-driven platforms that monetize through ad revenue. However, when a website’s primary function is

commercial (selling products or professional services) and yet the “About Us” and content pages are dominated by third-party ads, pop-ups, and misdirecting click-bait links, this represents a fundamental mismatch between stated purpose and actual operation. Legitimate professional service sites do not typically monetize their mission statements with interstitial ads.

3.5 Digital Footprint Verification

An established, legitimate business leaves multiple corroborating traces across the digital landscape: business directories, news mentions, regulatory filings, academic citations, professional association listings, and social media history. A research protocol for verifying digital footprint should include:

- Google the business name plus the term “reviews”, “scam”, and “complaint”
- Search the business in the Better Business Bureau (BBB) directory at bbb.org
- Check business registration in the relevant jurisdiction (e.g., Corporations Canada, US Secretary of State database, Companies House UK)
- Search for SEC filings (for US publicly traded entities) at sec.gov/edgar
- Verify any claimed awards, rankings, or recognitions directly with the issuing organization
- Cross-reference physical address against Google Maps Street View and commercial real estate databases

3.6 Authentic Images and Profile Photo Checks

Profile photographs of executives, directors, and team members are among the most commonly manipulated elements on fake websites. Scammers have developed increasingly sophisticated approaches to this deception, ranging from simple stock photo deployment to animated avatar generation and AI-synthesized portraits.

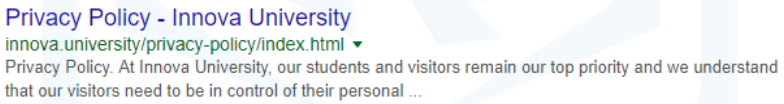


Figure 12. Original Company Logo and Business Building Signage. Physical location signage that can be independently verified using Google Maps Street View.

The following case study, drawn from AOFIRS research into a post-secondary institution (“American International University”), illustrates a complete image verification workflow for an executive profile photo.

Case Study: Verifying an Executive Profile Photo

Figure 13. Basic Information Checked: Image, Name, Phone, and Email verification for Mr. John Kline, listed as University President. The initial profile photograph retrieved from the university website was then subjected to reverse image search.

Figure 14. Reverse Image Search result showing the original profile image alongside image search matches. Note the discrepancy between the photo retrieved from the university page and the match returned by Google's image search.

Figure 15. Network Connections Observation. Analysis of the subject's professional network revealed a disproportionate number of 3rd-degree connections from unrelated industries, which is atypical for a senior executive of a 105,000-student institution.

Figure 16. Experience Verification on LinkedIn. The executive's stated employment history, academic credentials, and professional connections were cross-referenced against LinkedIn data for consistency and corroboration.

The LinkedIn analysis revealed further anomalies consistent with a constructed rather than authentic professional identity. The subject's skill endorsements were predominantly from 3rd-degree connections in unrelated industries, a pattern inconsistent with the genuine endorsement behavior observed for senior university presidents. Specific endorsers included a car dealer, a

Monsanto Company technician, and an Eagle Scout co-investor—connections unlikely to endorse the professional skills of a leading academic administrator.

Figure 17. Education Section Verification

Figure 18. Skill Endorsements Observation (3rd degree connection anomaly)

Corporate Background Verification

Corporate identity verification requires cross-referencing business claims against multiple public record databases. Key databases for North American researchers include:

Figure 19. ZoomInfo Corporate Background Check for Mr. John Kline. Cross-referencing the subject's claimed professional history against the ZoomInfo database revealed additional data points for verification.

Figure 20. SEC Edgar Filing Reference. U.S. Securities and Exchange Commission EDGAR database filings provide independently verified corporate information for publicly traded entities and certain registered investment vehicles.

Researchers verifying institutional claims should additionally check the U.S. Department of Education's database of accredited postsecondary institutions (ope.ed.gov/accreditation), the Council for Higher Education Accreditation (CHEA) registry, and jurisdiction-specific corporate registration databases. For the specific case analyzed, the institutional rankings claims were independently verified at U.S. News & World Report's published rankings and confirmed, while the profile photo discrepancy remained unresolved—illustrating that a single verified fact does not validate the totality of a website's claims.

Section IV: Products and Services Verification

4.1 E-Commerce Fraud Overview

E-commerce fraud is one of the most financially damaging manifestations of fake websites. While there are many legitimate companies conducting business online, fraudulent sellers exploit the anonymity of internet commerce to cheat consumers, steal personal data, and spread malware. These sites may lack safeguards for consumer privacy, security, and safety. Some reportedly install malware surreptitiously, commit advertisement fraud, and enable phishing scams that steal personal information to increase unlawful profits.

It is estimated that one in three content theft sites expose consumers to malware and other risks. Remote Access Trojans (RATs) reportedly use content theft sites as tools to spread malware. According to data published by the U.S. Trade Representative (USTR), between 227,000 and 1.3 million new malware files are released every day. A 2025 survey found that 36% of Americans who purchased from a fraudulent online store received no refund (Panda Security, 2026). Deloitte estimates AI-assisted scams could drive global losses to $40 billion by 2027.

4.2 Consumer Complaint Patterns

Common consumer complaints documented across major consumer protection databases and the AOFIRS research corpus include:

- Counterfeit brand-name products delivered instead of genuine merchandise
- Goods delivered significantly late, or not at all
- Products received that do not match website descriptions, dimensions, or quality representations
- Sellers refusing to accept returns or process refunds
- No direct telephone contact available; seller unreachable
- Physical business address differs from shipment origin address, or goods ship from undisclosed overseas locations
- Failure to disclose material information about the product or the terms of the sale
- Fake or fraudulent discount coupons, future purchase credits, and credit card enrollment discounts

Typical Categories of Counterfeit Products

- Prescription medicines, supplements, and online pharmacies
- Quick remedies for common health conditions and “miracle cure” products
- Diet pills, body enhancement products, and energy supplements
- Personal care products (cosmetics, perfumes, creams, and lotions)
- Consumer electronics (memory cards, hard drives, laptops, smartphones)
- Software, games, and digital downloads
- Major brand-name luxury goods (clothing, footwear, bags, jewellery, watches)

Primary Venues for Fake Goods

- Online auction platforms (eBay)

- Large inventory marketplaces (Amazon Marketplace, Walmart.com third-party sellers, Alibaba, Flipkart, Groupon)
- Social media commercial storefronts (Facebook Shops, Instagram Shopping, TikTok Shop)
- Peer-to-peer marketplace apps (Craigslist, Kijiji, Poshmark, Facebook Marketplace)
- Individual websites and independent e-commerce portals operating under obscure domains

4.3 How to Spot Fake or Counterfeit Products Online

Image and Listing Analysis

The visual presentation of products on fake e-commerce sites provides multiple diagnostic signals. A rigorous product image analysis should assess:

Exhibit 1. Color and Shade Comparison: Original (top) vs. Counterfeit (bottom). The counterfeit product displays noticeably different color tones, inconsistent shading, and variations in font weight on product labelling. These discrepancies are invisible at thumbnail resolution but become clear under close examination.

Beyond color analysis, product listing indicators of fraud include:

Font variations on packaging: Counterfeit products frequently display incorrect font weights, typefaces, or character spacing on labels and packaging photographs when compared against official brand style guides.

Single image vs. multiple views: Legitimate sellers typically provide multiple high-resolution images showing the product from multiple angles, with close-ups of serial numbers, certifications, and labels. Fake listings commonly feature only one or two images.

Inconsistent background and staging: Photographs taken in inconsistent lighting conditions, against informal backgrounds, or with visible staging errors (fingerprints on lens, poor focus) may indicate the product is not from an authorized distributor.

Missing or altered certification marks: For regulated product categories (electronics, children's products, safety equipment), verify that certification marks (CE, FCC, UL, CSA) are present and correctly rendered.

Exhibit 2. Font Variation Comparison. Product packaging showing an original versus a counterfeit version. Font weight, kerning, and character spacing differ measurably, visible even without specialized tools.

Section V: Checkout and Payment Verification

The checkout and payment process is the ultimate point of vulnerability for online consumers. Fake e-commerce sites are specifically engineered to extract financial and personal data at this stage. A structured verification protocol, applied before any financial transaction, significantly reduces exposure to fraud.

5.1 Invoice and Transaction Security

Check Invoice Amount Total: Before completing a purchase, verify that the order summary correctly reflects the product quantity, unit price, shipping cost, applicable taxes, and any additional fees. The total displayed should match the charge initiated at payment.

Review Refund Policy: If the refund policy is confusing, highly restrictive, or explicitly non-refundable, this is a significant risk indicator. Reputable e-commerce operators provide clear, accessible refund processes in compliance with consumer protection regulations in their jurisdiction.

Return Merchandise Policy: Complex, costly, or deliberately unclear return procedures are characteristic of scam sites that do not expect to fulfill return requests honestly.

Secure Transaction Verification: Ensure that your payment transaction is processed through a recognized, secure payment gateway. A reliable transaction should generate at minimum two confirmation communications: one from the vendor and one from the merchant bank. Single-confirmation transactions or those that do not generate any email confirmation are suspect.

Read Legal Contracts: Read through the Payment Terms, Policies, Agreements, and Disclaimers carefully. Where subscriptions, long-term contracts, licensing agreements, or auto-renewal provisions are present, these must be explicitly acknowledged before authorization.

Auto-Renewal Pre-checked Boxes: Many fake e-commerce sites default to auto-renewal with consent checkboxes pre-ticked. Always uncheck these unless intentionally subscribing to a recurring service.

5.2 HTTPS, SSL/TLS and Digital Certificates

The evolution from HTTP to HTTPS represents a foundational shift in web security. HTTPS (HTTP + TLS/SSL—Transport Layer Security/Secure Sockets Layer) encrypts all communication between a user's browser and the website server, preventing interception, manipulation, or theft of transmitted data in transit.

However, the presence of HTTPS alone is no longer a reliable indicator of a legitimate website. By 2025, the ACME protocol and providers such as Let's Encrypt offer TLS certificates at no cost and with minimal verification. Scam sites routinely obtain basic SSL certificates, which means the padlock icon—while necessary—is not sufficient evidence of legitimacy. Researchers should:

- Confirm the padlock icon is present and the URL begins with "https://"—not just the domain name portion
- Click the padlock to view certificate details: verify the issuing Certificate Authority (CA), the certificate validity period, and the Common Name (CN) or Subject Alternative Name (SAN) to ensure they match the website being visited
- Use browser security indicators: Chrome now shows a "Not Secure" warning for HTTP sites; an "info" icon (ⓘ) may indicate mixed content (HTTPS page loading non-secure resources)

- For high-stakes transactions, verify the certificate against the CA's public Certificate Transparency log (crt.sh)

2025–2026 SECURITY UPDATE — SSL Certificate Misuse

The KnowBe4 2025 Phishing Threat Trends Report found that 82.6% of phishing emails analyzed between September 2024 and February 2025 contained AI-generated content, and a significant proportion of corresponding phishing sites carried valid TLS certificates. Researchers should treat HTTPS as a baseline hygiene requirement rather than a trust signal. Extended Validation (EV) certificates, which display the organization name in the browser address bar, provide a higher level of assurance but have become less common as browsers have simplified their trust UI.

5.3 Trust Seals and Payment Gateway Verification

Trust seals are visual indicators that a website has undergone some form of third-party security verification. Common legitimate trust seals include those issued by DigiCert, Sectigo (formerly Comodo), McAfee Secure, Norton Secured, PayPal Verified, and BBB Accredited Business. Importantly, trust seals on legitimate sites are interactive—clicking them should redirect to the issuing authority's verification page, confirming the seal is current and valid.

Fake sites commonly display copied or fabricated trust seal images that are not hyperlinked to any verification page, or that link to a non-functional placeholder. Verification protocol: click every trust seal on the checkout page. A non-functional seal image is a clear red flag.

Section VI: Website Content Analysis

6.1 Text, Spelling, and Plagiarism

Every computer and web browser incorporates spell-check functionality, and professional content management systems include built-in editorial review tools. There is, in practical terms, no excuse for systemic spelling and grammatical errors on a professionally operated website. Accordingly, any website with numerous spelling errors or persistent grammatical mistakes should be treated with heightened scrutiny, particularly where those errors appear on principal content pages.

Content authority should be evaluated against four criteria: accuracy (do claims correspond to verifiable facts?), authority (are sources cited, and are authors credentialed?), clarity (is the content specific and coherent?), and non-bias (does the content present multiple perspectives or only self-serving information?). In the current environment of AI-generated content, a fifth criterion is increasingly relevant: verifiability (do specific claims cite independently accessible sources that can be confirmed?).

6.2 Video Content and Deepfakes

Video content on fake websites ranges from unsophisticated borrowed clips to AI-generated deepfakes. The most difficult to verify are deepfakes—ultrarealistic synthetic videos created with AI—which require specialized forensic tools for definitive authentication. The European Parliamentary Research Service (2025) projected that 8 million deepfakes would be shared in 2025, up from 500,000 in 2023—a 1,500% increase in under two years. Human detection accuracy for deepfakes sits at approximately 55.54%, barely above random chance (iProov, 2025). For high-quality video deepfakes, human detection rates drop to 24.5%.

Standard Video Verification Checklist

- Check the video source URL (right-click > “Inspect” or view page source)
- Verify if the video is hosted on the site or merely embedded from YouTube, Vimeo, or social media
- Check video upload date and original share date—context manipulation often involves re-dating legitimate footage
- Evaluate video quality for visual anomalies: blurring around moving objects, edge artifacts at face boundaries, unnatural blinking patterns or facial microexpressions
- Match environmental details (building signs, vehicle plates, signage language) against claimed geographic location
- Check for light and shadow inconsistencies between subject and background
- Search for the video on social media and other platforms using reverse video search (InVID/WeVerify plugin)
- Assess whether scenes appear staged, camera movement seems unnatural, or framing seems deliberately limited

2025–2026 UPDATE — AI Deepfake Proliferation

The Keepnet Labs 2026 analysis found that deepfake fraud incidents increased tenfold between 2022 and 2023, with 179 deepfake incidents reported in Q1 2025 alone—surpassing the total for all of 2024 by 19%. U.S. deepfake-related financial losses reached $1.1 billion in 2025, tripling

from $360 million in 2024. CloudSEK's 2026 report identifies the best enterprise deepfake detection platforms as combining machine learning with forensic signal analysis. For CIRS™ researchers, the WeVerify/InVID browser plugin and Microsoft Video Authenticator remain accessible first-line tools.

6.3 Contact Information Verification

Address Verification

- Verify the physical address using Google Maps Street View—confirm whether the location corresponds to a commercial property, a residential address, or a virtual office
- Ensure the address is complete: unit number, building name, street address, city, province/state, and country
- Cross-reference the postal/ZIP code against the stated city and province/state—mismatches are common in fake site address fields
- For businesses claiming to operate in regulated industries (financial services, healthcare, education), confirm the address against the relevant regulatory authority's registry

Telephone Number Verification

Legitimate businesses typically maintain published telephone numbers, most often associated with landlines or traceable VoIP systems. While VoIP telephony is entirely legitimate and widely used by genuine businesses, scam operators disproportionately rely on unregistered VoIP numbers because they are inexpensive, immediately available, and easily abandoned.

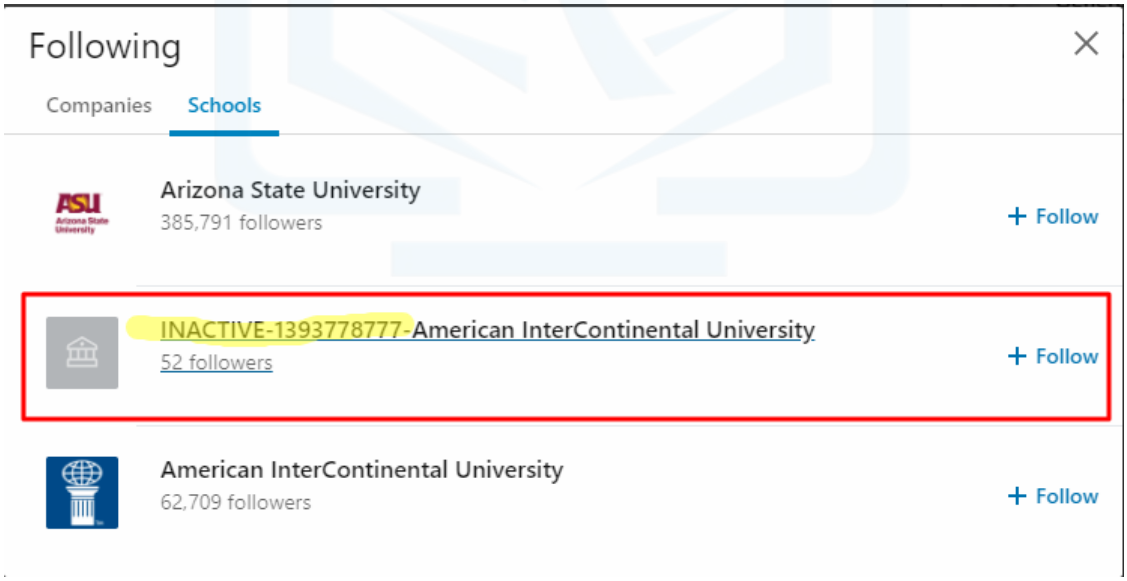


Figure 27. Social Media Phone Number Search Query. Constructing a targeted search query embedding a phone number in social media search operators reveals whether the number is associated with profiles or messages that corroborate or contradict the website's stated identity.

Phone verification tools available to researchers include:

CNAM Lookups (Caller ID Name): Database services that query the CNAM record associated with a telephone number, revealing the registered name and any spam history

Reverse phone lookup services: Services such as Free Cell Phone Lookups, NumLookup, or ZLOOKUP allow identification of the registered owner of a number

Trapcall: A service that reveals blocked or private caller ID information from incoming calls

Social media operator queries: Phone numbers embedded in social media search operators (site:linkedin.com "+1-800-XXX-XXXX") can surface associated profiles

Email Verification

Email addresses on a business website should use the organization's own registered domain name. Generic personal email addresses (Gmail, Yahoo, Hotmail) on a business contact page are a red flag; sub-domain manipulation (e.g., support@paypal-helpdesk.com rather than support@paypal.com) is a classic phishing technique.

Email Address Example	Researcher Assessment
david.caprillo@airsassociation.com	Correct format: domain matches organization
david.caprillo@airsassociation.membership.com	Incorrect: domain is a subdomain of a different organization
david.caprillo@amazoncustomerservice.com	Incorrect: deceptive domain designed to impersonate Amazon
david.11901@airsassociation.com	Suspicious: numeric suffix typical of bulk/temporary email generation
david.caprillo@gmail.com	Inappropriate: personal address on a business contact page

Table 2. Email Address Verification Examples. Format analysis of email addresses found on website contact pages.

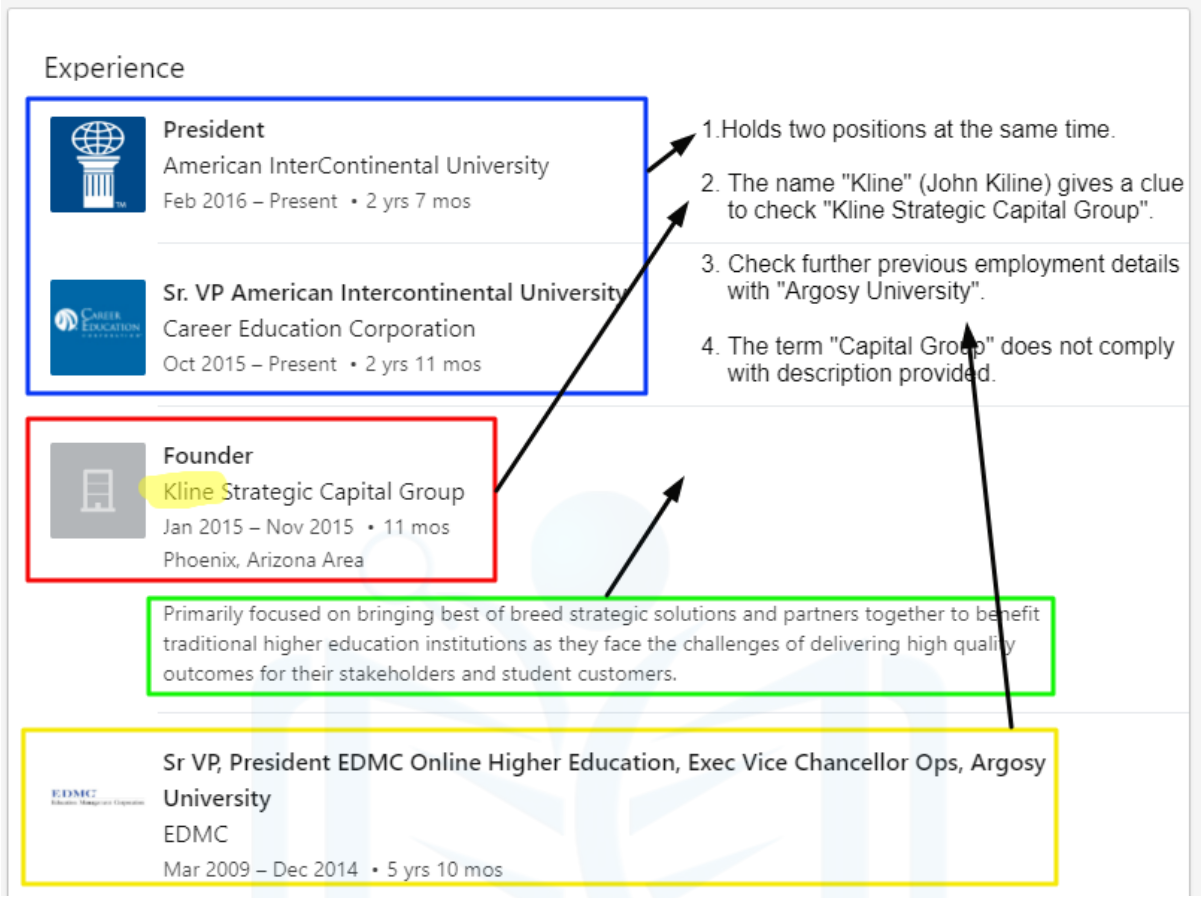


Figure 28. Email Server Verification Tool Result. The email verification service connects directly to the mail server via SMTP and performs a DNS MX record lookup to confirm whether the mailbox exists and the domain is properly configured. Note the MX record details and server response code in the results panel.

6.4 Copyright Status Verification

A legitimate commercial website maintains current copyright notices on all pages, typically rendered in the footer as: © [Year] [Entity Name]. All Rights Reserved. The copyright year should reflect the current year or the most recent content update. Sites with outdated copyright years (often by several years) frequently indicate either an abandoned website, a fraudulently repurposed domain, or a site whose operators are not actively maintaining its content.

Researchers should understand the distinction between copyright (©), trademark (™ and ®), and trade dress protection. Logos are generally considered artistic works and are protected as trademarks; website content is protected by copyright. Fake sites frequently either omit copyright notices entirely, apply incorrect symbols (using ® for unregistered works), or use copyright dates that are inconsistent with the domain registration date.

Section VII: Profile Photos and Image Verification

7.1 Reverse Image Search and Stock Photo Identification

Image verification is among the most technically accessible yet frequently neglected components of fake website analysis. While advanced digital forensics requires specialized tools, the initial triage—reverse image search—requires only a browser and internet access, yet eliminates the majority of unsophisticated fake image deployments.

The primary reverse image search platforms available to researchers are Google Images (images.google.com), Bing Visual Search (bing.com/visualsearch), TinEye (tineye.com), and Yandex Images (yandex.com/images). Each uses different indexing algorithms and covers different image corpora; running a suspicious image through all four significantly increases detection probability.

Identifying Stock Photos: Diagnostic Criteria

Stock photography libraries (Shutterstock, Getty Images, Adobe Stock, iStock, Unsplash) contain millions of images that are routinely misused on fake websites to simulate a team, physical premises, or product range that does not exist. The following characteristics are highly diagnostic of stock photo usage:

Immaculate lighting with no natural shadows: Professional studio lighting produces evenly illuminated subjects with controlled, symmetrical shadows. Natural workplace and office environments invariably have ambient light variation, reflections, and partial shadows.

Clean, distraction-free backgrounds: Stock shoots use controlled studio backdrops or purpose-set environments. Genuine office and working environment photos contain natural clutter: personal items, cables, asymmetric furniture arrangements.

Absent brand identifiers: Stock images deliberately avoid logos, brand names, product marks, and identifiable faces (unless licensed as such). A “team meeting” photo with no company branding, generic whiteboards, and ethnically diverse models in non-specific attire is characteristic of stock photography.

Uniform aesthetic quality: Stock photography collections exhibit consistent professional quality across all images. A website where some images have very high professional quality while others are clearly smartphone or amateur photos suggests selective deployment of stock images for deceptive purposes.

Emotionally exaggerated facial expressions: Stock portrait photography favors clearly expressed, universally recognizable emotions (enthusiastic smiling, serious concentration) over the more subtle expressions that characterize candid workplace photography.

Multiple-variation shot: A reverse image search on a stock photo will typically return numerous variations: the same subjects from different angles, with different props, or against different backgrounds—all from the same stock shoot.

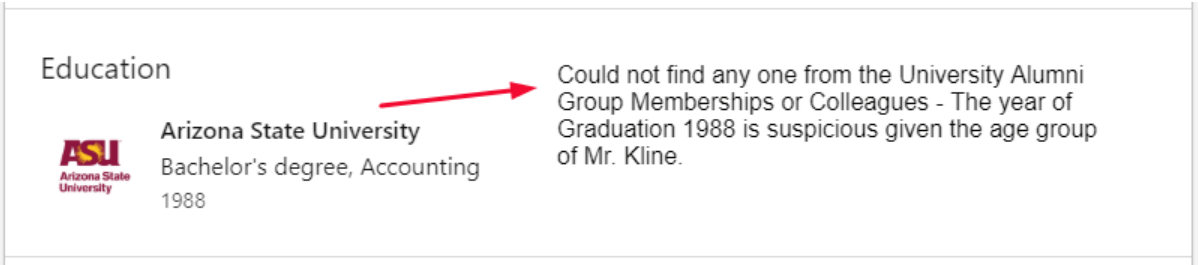


Figure 29. AOFIRS Research Images Set: Supporting material for stock photo identification methodology.

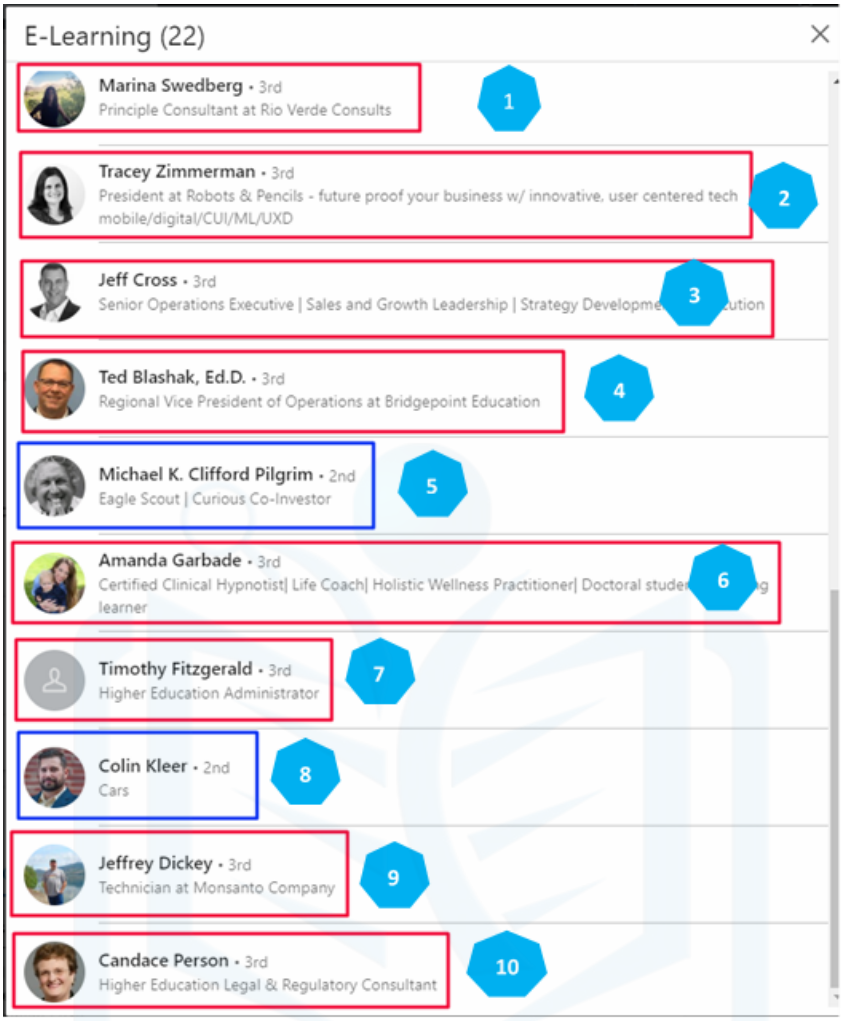


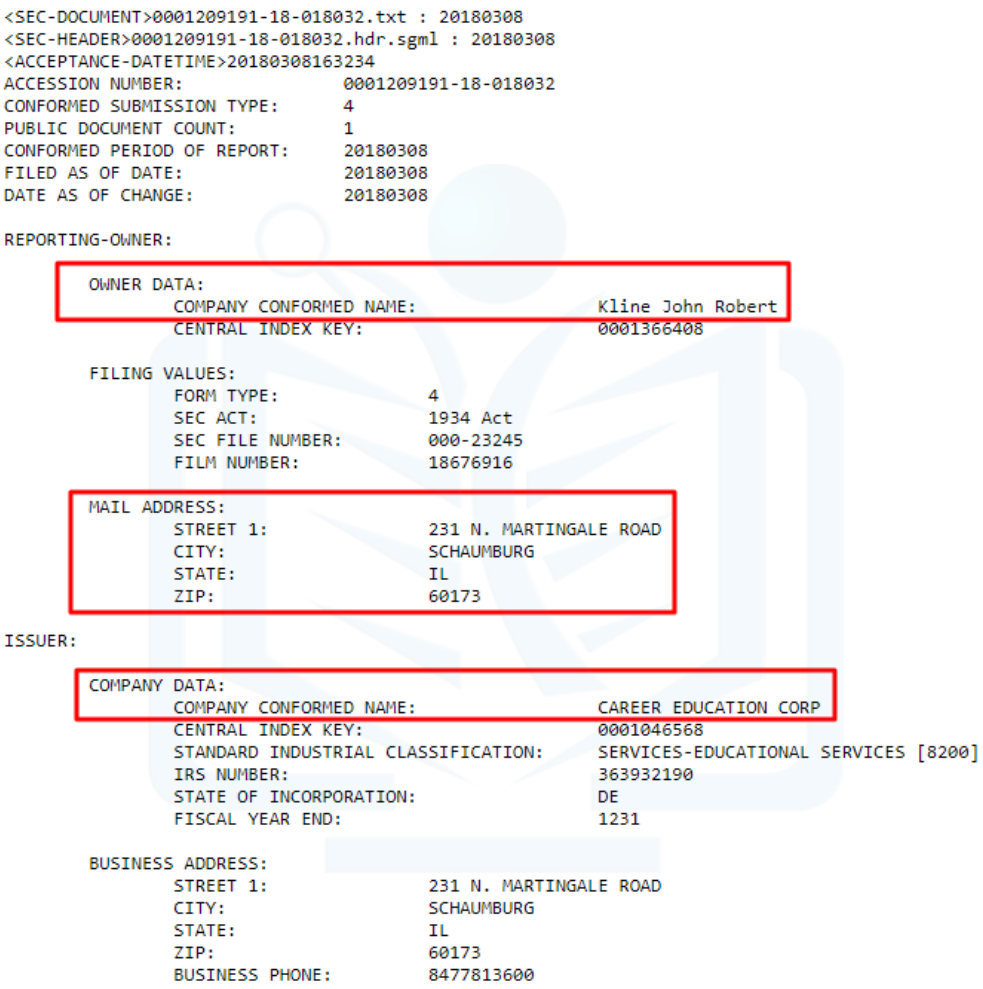
Figure 30. Stock Photo of a Working Office vs. Authentic Office Environment. Stock images (right) show immaculate staging, absent brand materials, and professional lighting absent in genuine working environments (left). Note the absence of cables, personal items, and brand materials in the stock version.

Figure 31. Stock Call Center vs. Authentic Call Center Environment. Professional stock photography (right) shows uniform, unrealistically organized work environments. Real operational call centers (left) display natural variation in personal workstation setup and informal organization.

7.2 Digital Image Tampering Detection

Digital image tamper detection has become an important research specialization in its own right. The challenge for general researchers is that professional-quality image manipulation has become accessible to non-specialists through AI-assisted editing tools (Adobe Firefly, Midjourney inpainting, Stable Diffusion) that can seamlessly alter photographs without the artifacts that previously characterized Photoshop manipulation.

While forensic-grade tools remain the authoritative standard, researchers can perform first-line tamper analysis using accessible methods:



```
<SEC-DOCUMENT>0001209191-18-018032.txt : 20180308
<SEC-HEADER>0001209191-18-018032.hdr.sgml : 20180308
<ACCEPTANCE-DATETIME>20180308163234
ACCESSION NUMBER:               0001209191-18-018032
CONFORMED SUBMISSION TYPE:      4
PUBLIC DOCUMENT COUNT:          1
CONFORMED PERIOD OF REPORT:     20180308
FILED AS OF DATE:               20180308
DATE AS OF CHANGE:              20180308

REPORTING-OWNER:

        OWNER DATA:
                COMPANY CONFORMED NAME:                 Kline John Robert
                CENTRAL INDEX KEY:                      0001366408

        FILING VALUES:
                FORM TYPE:              4
                SEC ACT:                1934 Act
                SEC FILE NUMBER:        000-23245
                FILM NUMBER:            18676916

        MAIL ADDRESS:
                STREET 1:               231 N. MARTINGALE ROAD
                CITY:                   SCHAUMBURG
                STATE:                  IL
                ZIP:                    60173

ISSUER:

        COMPANY DATA:
                COMPANY CONFORMED NAME:                 CAREER EDUCATION CORP
                CENTRAL INDEX KEY:                      0001046568
                STANDARD INDUSTRIAL CLASSIFICATION:     SERVICES-EDUCATIONAL SERVICES [8200]
                IRS NUMBER:                             363932190
                STATE OF INCORPORATION:                 DE
                FISCAL YEAR END:                        1231

        BUSINESS ADDRESS:
                STREET 1:               231 N. MARTINGALE ROAD
                CITY:                   SCHAUMBURG
                STATE:                  IL
                ZIP:                    60173
                BUSINESS PHONE:         8477813600
```

Figure 32. Examples of Image Tampering Techniques. The five panels (A–E) illustrate the principal categories of digital image manipulation: (A) face substitution, (B) body part alteration, (C) artificial shadow insertion, (D) selective lighting enhancement, and (E) object transposition. Each category has specific detection signatures detectable through metadata and edge analysis.

EXIF metadata analysis: Download the image and examine its embedded EXIF metadata using a tool such as Jeffrey's Exif Viewer or ExifTool. Authentic photographs contain camera make/model, GPS coordinates, timestamp, and lens data. Images stripped of metadata (all fields blank) or with metadata that contradicts the claimed context (e.g., GPS coordinates inconsistent with stated location) are suspect.

Error Level Analysis (ELA): FotoForensics.com provides free ELA analysis. Areas of an image that have been digitally modified show different JPEG compression artifacts than unmodified areas, appearing as bright patches in the ELA output.

Clone detection: Izitru and ImageEdited.com check images for signs of cloning (duplicated pixel regions), which is characteristic of object removal or background fill operations.

AI face detection indicators: AI-generated or AI-modified faces exhibit specific artifacts: unnatural symmetry, reflections in both eyes that do not match, hair at the edge of the frame that blends into the background, and ears that are partially rendered or asymmetric. The Hive Moderation and Illuminarty tools detect AI-generated imagery with high accuracy.

Section VIII: Social Media and Background Checks

An established, legitimate business maintains a consistent and active social media presence across relevant platforms, typically including Facebook, Instagram, LinkedIn, and (depending on industry) X (formerly Twitter), YouTube, or TikTok. Social media profiles for legitimate businesses typically demonstrate: (1) a history of posts predating the current date by at least several months, (2) genuine customer engagement (comments, responses, shared content), (3) follower counts consistent with stated age and size, and (4) content that corroborates the website's stated products or services.

Fake website operators frequently create social media accounts concurrent with or shortly after launching the fraudulent site. These accounts exhibit characteristic patterns: very recent account creation date, low organic follower counts, content that is generic or replicated from other accounts, absence of authentic customer interaction, and no content history prior to the recent fraud campaign.

Social Media Verification Protocol

- Note the date of account creation (visible under "About" on Facebook, "Joined" on X/Twitter, and accessible via LinkedIn)—accounts less than 6 months old warrant heightened scrutiny
- Review the posting history for continuity, topic consistency, and evidence of genuine community engagement
- Examine follower/connection quality: profiles that follow the account should be identifiable real people with established histories, not recently created shell accounts
- Cross-reference the account's profile images against the website's team photos and against reverse image search results
- Look for discrepancies between claimed location in the social profile and website address
- Search for mention of the business in third-party posts, reviews, and news articles independent of the business's own content

BACKGROUND CHECKS — Individual Identity Verification

When a website lists named executives, board members, or management team with contact information, structured background verification can be performed: (1) Search full name + business name in LinkedIn, XING, and business directories such as ZoomInfo and Yelp. (2) Verify stated educational credentials against institutional alumni directories. (3) Search professional licensing databases (e.g., state bar associations, medical boards, financial regulator registries) for claimed professional qualifications. (4) Cross-reference any published biographical details against public records databases. Comprehensive individual background check methodology is detailed in Module 10, Units 25–26 of the CIRS™ curriculum.

Section IX: Third-Party Verification and Trust Marks

9.1 Affiliates, Partners, and Authorized Re-Sellers

Fake websites commonly display logos and branding of well-known companies to imply an authorized affiliation, partnership, or reseller relationship that does not exist. Understanding the operational distinctions between these relationship types equips the researcher to ask the right verification questions.

Relationship Type	Definition and Verification Approach
Affiliate	An internet-based marketer who promotes a parent company's products/services online in exchange for commission. Affiliates do not hold inventory and are not authorized dealers. Their relationship is primarily promotional.
Authorized Reseller	An entity that purchases products from a manufacturer or distributor and resells them, typically with added value (support, customization, service). Authorized resellers are formally listed in the parent company's partner directory.
Channel Partner	An entity enrolled in a formal partner program to expand the parent company's reach. Channel partners earn commissions and are bound by partner program agreements governing use of brand assets.

Table 3. Business Relationship Types and Verification Approach

Verification of claimed affiliations and partnerships should be conducted through the following methods:

- Direct inquiry to the claimed parent company through contact channels listed on the parent's verified official website (not through contact information on the suspect site)
- Search the parent company's official website for a "Partner Finder", "Authorized Reseller Locator", or "Find a Dealer" directory
- Check public business registration databases for the claimed legal entity
- Search SEC EDGAR (for US companies), Corporations Canada, or equivalent for formal corporate filings that corroborate the relationship

9.2 Trust Mark Logos and Accreditation Bodies

Figure 33. Animated and AI-Synthesized Profile Images. Fake website operators increasingly deploy AI-generated or animated avatar images of team members to avoid detection by reverse image search. These images do not exist in any stock photography database and produce no matches in standard reverse image search.

Figure 34. Image Search Anomaly: Same Person with Two Different LinkedIn Profiles. The same individual's photograph (with minor alterations—here, the presence versus absence of glasses) was found associated with two separate LinkedIn profiles, a strong indicator of fraudulent identity construction.

Research by ANEC (the European consumer organisation) found that seven in ten people report greater likelihood of using a website displaying a trust-mark label or logo. This statistic explains why fake websites invest in unauthorized or fabricated trust mark displays. The primary categories of trust marks include:

- Non-profit charitable organizations with global recognition (International Red Cross, Doctors Without Borders, Habitat for Humanity)
- Professional association memberships (American Marketing Association, American Psychological Association, American Academy of Forensic Science)
- Standardization and accreditation bodies (ISO, ANSI, BSI, NIST)

- Educational accreditation agencies recognized by the U.S. Department of Education and CHEA
- Industry licensing bodies (AICPA/NASBA for CPAs; CFA Institute; state medical and legal boards)
- Consumer protection verification bureaus (Better Business Bureau)
- Payment security certifications (PCI DSS compliance marks, PayPal Verified)
- Website security seals (DigiCert, Norton Secured, McAfee Secure)

9.3 Accreditation vs. Licensing vs. Certification

These three credential categories are frequently conflated but have distinct legal and practical meanings. Researchers verifying institutional claims must apply the correct verification standard for each:

Accreditation	Licensing	Certification
Voluntary process applicable only to organizations, agencies, or programs	Required for public safety; applies to individuals, facilities, organizations, or agencies	Demonstrates specialized capability; applies to individuals, facilities, or organizations
Awarded by recognized accreditation bodies following external review	Issued by government authorities; operating without license is illegal	Issued by professional bodies; sometimes mandated by regulators
Verify directly with accrediting body's public registry	Verify with relevant government licensing authority	Verify with credentialing organization's public verification portal

Table 4. Distinctions Between Accreditation, Licensing, and Certification

Section X: Customer Reviews and Testimonials

Online consumer reviews are among the most powerful signals available to prospective customers, and therefore among the most lucrative targets for manipulation by fake website operators. The critical distinction for researchers is between third-party reviews (collected independently of the business) and testimonials (curated and published by the business itself).

Third-party review platforms (Google Reviews, Yelp, Trustpilot, BBB) operate independently and cannot be controlled by the reviewed business, although astroturfing (coordinated fake positive reviews) and review bombing (coordinated fake negative reviews against competitors) are documented practices. Testimonials published on the website are selected, edited, and controlled by the site operator; they may be entirely fabricated.

Indicators of Fake Reviews

Fake negative reviews used as endorsements: An unusual tactic where negative reviews are framed as positive outcomes. Example: “This pill does NOT work as advertised—I lost 30kg instead of 20!” This technique provides fake positive social proof while technically posting a “negative” review.

Duplicate reviews with slight variations: Reviews that are structurally similar to other reviews on the same page or elsewhere online, differing only in minor word substitutions—a characteristic of AI-generated bulk review campaigns.

Grammar and language anomalies: Systemic grammatical patterns consistent with non-native English writing, particularly when multiple consecutive reviews exhibit the same errors, suggest outsourced review generation.

Hyperspecific product praise: Reviews that emphasize specific model numbers, dimensions, and technical details with unnatural precision, combined with price-value emphasis, are characteristic of paid review patterns documented in FTC enforcement actions.

Buzzword saturation: Repeated use of the same promotional phrases across multiple reviews (“courteous service, excellent support, great price”) suggests a templated generation process rather than independent customer expression.

Anonymous or pseudonymous reviewer accounts: Check reviewer account creation dates and posting history. Accounts created immediately prior to a cluster of positive reviews, accounts with only one review, and accounts using pseudo-names with numeric suffixes are red flags.

Reviews predating product availability: Cross-reference review dates against the product launch or service commencement date. Reviews published before the product existed are definitively fraudulent.

Generic short-form reviews: One-line reviews that express enthusiasm without describing a specific experience (“Fantastic service!”, “Great product, highly recommend”) provide no verifiable information and are readily generated in bulk.

Plagiarism in review text: Paste two to four distinctive phrases from a review into a quoted Google search. Identical text appearing across multiple review platforms is a clear indicator of manufactured content.

Verification Best Practices

Researchers and consumers should apply the following practices when evaluating the authenticity of review ecosystems:

- Compare reviews across multiple independent platforms (Google, Yelp, Amazon, Trustpilot, Quora) for consistency and corroboration
- Read full review text rather than relying on aggregate star ratings—rating manipulation is common, but detailed fraudulent reviews are more labor-intensive to produce and more often reveal inconsistencies
- Assess reviewer profiles: follow links to profiles of reviewers whose feedback is most influential to your assessment; credible reviewers have diverse review histories unrelated to the business under scrutiny
- For Facebook Business page reviews, the public nature of reviewer accounts allows direct verification and outreach
- Consult the FTC's guidance on endorsements and testimonials (ftc.gov) for authoritative criteria on what constitutes authentic vs. deceptive review content

Section XI: AI-Era Threats and Advanced Detection (2025–2026)

This section presents the most current findings on the evolving intersection of artificial intelligence and fake website fraud, drawing on research and threat intelligence published through mid-2026. The findings document a qualitative shift in the fake website landscape that every practicing CIRS™ researcher must understand.

11.1 Generative AI and Instant Website Cloning

The introduction of large language model-powered website generators represents the most significant capability escalation for fake website operators since the commercialization of the web. Tools including Vercel's v0, Loveable.dev, and comparable LLM-driven application builders allow users to replicate the complete visual and functional design of any website by submitting a natural-language prompt or a screenshot. The generated clone includes:

- Visual layout, typography, and color scheme matching the original
- Functional navigation and JavaScript interactive elements
- Plausible meta titles, meta descriptions, and SEO keyword structure
- Auto-generated legal pages (Privacy Policy, Terms of Use, Returns Policy) calibrated to match the apparent jurisdiction and industry
- Cookie consent banners and GDPR/CCPA compliance popups
- Fake trust seals and award logos copied from the original

Panda Security (2026) reports that AI-built sites now account for 6–7% of all phishing infrastructure, with the proportion growing rapidly. A 2025 survey found that 36% of Americans who purchased from a fraudulent online store received no refund (Panda Security, 2026). Deloitte (2025) projects AI-assisted scam losses could reach $40 billion globally by 2027.

11.2 AI Cloaking: Serving Different Content to Crawlers

A sophisticated evasion technique documented by SPLX researchers and reported in Dark Reading (2025) allows fake websites to serve entirely different content depending on the type of visitor. When a web crawler (AI search agent, fact-checking bot, or safety scanner) visits, the site presents safe, legitimate-appearing content. When a human browser visits, it presents fraudulent, harmful, or phishing content.

This technique, demonstrated against AI crawlers including Perplexity's Atlas and ChatGPT's browsing agent, has profound implications for automated trust verification: no tool-based website scanner should be treated as definitive on its own. The CIRS™ methodology's emphasis on multi-source, multi-method manual verification is specifically resistant to this evasion technique.

11.3 Deepfake Fraud: Statistics and Impact

The following quantitative benchmarks from 2025–2026 define the current operating environment for researchers assessing video and audio content on suspect websites:

Finding	Value	Source/Year
Deepfakes shared online (2025)	8 million projected	EU Parliamentary Research Service / 2025
Growth from 2023 baseline	+1,500%	Keepnet Labs / 2026
Q1 2025 deepfake incidents vs. full year 2024	+19% in one quarter	Keepnet Labs / 2025
US deepfake financial losses (2025)	$1.1 billion (3× increase)	Keepnet Labs / 2025
Average human detection accuracy (all deepfakes)	55.54%	iProov / 2025
Human accuracy for high-quality video deepfakes	24.5%	iProov / 2025
AI-generated phishing emails (Sept 2024–Feb 2025)	82.6% of analyzed sample	KnowBe4 / 2025
AI content farm websites tracked globally	3,006 in 16 languages	NewsGuard / March 2026

Table 5. Key 2025–2026 Statistics: AI Deepfake and Fake Website Threat Landscape

11.4 New Detection Tools and Techniques for Researchers

The following tools have emerged or achieved significant adoption in the 2024–2026 period as effective components of a researcher's website verification toolkit:

Tool	Category	Function / Use Case
ScamAdviser	Website Trust Scoring	Uses 40+ data sources and law enforcement reports; trust score generation within seconds
Fraud-Detector.eu	Automated Website Check	ML-trained model checks domain age, SSL, traffic patterns, and technology stack
URLVoid	URL/Domain Reputation	Multi-engine blocklist check against known scam and malware databases
Google Safe Browsing	Browser Safety Status	Daily scan of billions of URLs; integrated into Chrome, Firefox, Safari
PhishTank	Phishing Database	Community-driven phishing URL verification; widely integrated in browser tools
ICANN Lookup / Whois.com	Domain Registration	Registration date, registrar, registrant country; identifies recent registrations
Norton Safe Web	Website Reputation	Community-sourced threat intelligence; real-time site reputation reports
WeVerify / InVID Plugin	Video Verification	Reverse video search, keyframe analysis, metadata extraction for video authentication
CloudSEK Deepfake Platform	Deepfake Detection	Enterprise-level synthetic media detection including video, audio, and image modalities
FotoForensics.com	Image Tamper Analysis	Free ELA (Error Level Analysis) for JPEG compression artifact detection

Tool	Category	Function / Use Case
Hive Moderation / Illuminarty	AI Image Detection	Detects AI-generated (GAN, diffusion model) images with high accuracy
crt.sh (Certificate Transparency)	SSL Certificate Audit	Public ledger of all issued TLS certificates; audits issuing CA and certificate age

Table 6. Current Website Verification Tool Inventory for CIRS™ Researchers (2025–2026)

11.5 Browser-Based Security Indicators in 2025–2026

Modern web browsers have evolved significantly in how they communicate security information to users. Chrome's transition to a simplified lock icon UI (completed in 2023–2024) removed the Extended Validation (EV) green address bar, meaning that Chrome no longer visually distinguishes between a basic DV (Domain Validated) certificate—obtainable in seconds for free—and an OV (Organization Validated) or EV certificate that requires documented identity verification.

Padlock icon: Indicates HTTPS is active. In Chrome, Firefox, Edge, and Safari, a padlock indicates an active TLS connection. Click the padlock to see issuing CA, certificate details, and connection security status.

“Not Secure” warning: Displayed for HTTP pages. Any checkout or login page displaying “Not Secure” should be abandoned immediately.

Info icon (ⓘ): In Chrome, the info icon indicates a site that uses HTTPS but has mixed content issues (loading non-encrypted resources). This creates a man-in-the-middle vulnerability for the non-encrypted elements.

Certificate Authority check: Click the padlock > “Certificate is valid” to view the full certificate. Verify: Issued To (organization name), Issued By (CA name), Valid From/To (current dates). A certificate issued by an unrecognized CA or one expiring within days is suspect.

Browser security settings: Chrome, Firefox, Edge, and Safari all offer configurable Safe Browsing protection levels. Chrome’s “Enhanced Protection” mode provides real-time URL checking against Google’s threat database, offering substantially more protection than the default “Standard Protection.”

Section XII: Researcher Training Quick-Reference Checklist

The following structured checklist consolidates the complete fake website verification methodology into an actionable research instrument. CIRS™ candidates should be able to complete a full website audit using this checklist systematically, documenting evidence for each assessed element.

A. HOMEPAGE & INITIAL IMPRESSION

- ☐ Logo quality: Zoom in to check for pixel degradation; conduct reverse image search
- ☐ Color consistency: Logo colors match site color palette
- ☐ Navigation functionality: All navigation links lead to functional pages
- ☐ No dead links or placeholder “Lorem ipsum” content
- ☐ Homepage construction: HTML-based, not a single image file
- ☐ Pop-up / ad density: Not disproportionate for stated purpose

B. POLICY AND LEGAL PAGES

- ☐ Privacy Policy present and year-current
- ☐ Terms of Use/Service present and legally coherent
- ☐ Policy text passes quoted-phrase plagiarism test in Google
- ☐ Policy references correct jurisdiction(s) for stated operating territory
- ☐ Copyright notice present, correctly formatted (©), current year

C. ABOUT US / ORGANIZATION IDENTITY

- ☐ At least 3 of 5 completeness criteria met (mission, structure, team, email, awards)
- ☐ No plagiarized text detected in “About Us” content
- ☐ Named individuals verified via LinkedIn, professional directories
- ☐ Executive profile images pass reverse image search (not stock photos)
- ☐ Business registration confirmed in relevant public corporate registry
- ☐ Physical address verified via Google Maps Street View
- ☐ No AI-generated or animated profile images detected

D. PRODUCTS & SERVICES

- ☐ Multiple product images from different angles provided
- ☐ Product color, font, and label details consistent with brand originals
- ☐ Certification marks (CE, FCC, UL) present and correctly rendered
- ☐ No listings of medicine, supplements, or regulated goods without licensing disclosure
- ☐ Third-party marketplace listing cross-referenced against brand’s authorized seller list

E. CHECKOUT & PAYMENT

- ☐ HTTPS confirmed throughout checkout process
- ☐ TLS certificate details verified (issuing CA, validity, CN match)
- ☐ All trust seal logos are interactive (click confirms validity)
- ☐ Refund and returns policy clear and accessible
- ☐ Auto-renewal / subscription terms clearly disclosed and pre-checked boxes absent
- ☐ Two independent confirmation emails received (vendor + payment processor)
- ☐ Billing address requirement checked against credit card holder name

F. CONTENT QUALITY

- ☐ No systemic spelling or grammar errors on principal pages
- ☐ All factual claims cite verifiable, accessible sources
- ☐ Content passes quoted-phrase plagiarism test in Google
- ☐ Video content: source verified, not deepfake characteristics identified
- ☐ Image reverse search completed on all profile/team photos
- ☐ Copyright notice correct and current

G. CONTACT INFORMATION

- ☐ Physical address complete and verified on Google Maps
- ☐ Phone number: area code matches stated location; not a call center front
- ☐ Phone number: CNAM lookup completed
- ☐ Email addresses use company domain name (not generic)
- ☐ Email server MX record verified using email verification tool
- ☐ Domain WHOIS registration details cross-referenced with stated founding date

H. SOCIAL MEDIA & DIGITAL FOOTPRINT

- ☐ Social media accounts present on major platforms
- ☐ Account creation dates predate recent fraud window (6+ months)
- ☐ Organic engagement evident (genuine comments, shares, diversity of followers)
- ☐ Profile images consistent across website and social media
- ☐ Business mentioned in third-party news, directories, or regulatory records
- ☐ BBB check completed (for North American businesses)

I. THIRD-PARTY CLAIMS & TRUST MARKS

- ☐ All trust seal logos are clickable and verify correctly
- ☐ Claimed affiliations verified directly with parent company
- ☐ Accreditation claims verified with accrediting body registry
- ☐ Professional licensing verified with relevant authority
- ☐ Award and ranking claims verified at primary source

J. REVIEWS & TESTIMONIALS

- ☐ Third-party reviews checked on Google, Yelp, and Trustpilot
- ☐ No evidence of duplicate reviews, buzzword saturation, or review clusters
- ☐ Review dates do not predate product availability
- ☐ Reviewer profiles assessed for account age and posting history
- ☐ Selected review text subjected to quoted-phrase plagiarism test

K. AI-ERA CHECKS (2025–2026)

- ☐ Domain registration date checked via ICANN Lookup / Whois
- ☐ URL scanned in ScamAdviser, URLVoid, or Google Safe Browsing
- ☐ Website checked against PhishTank database
- ☐ Selected images analyzed via FotoForensics ELA or Hive Moderation AI detector
- ☐ Any video content checked via InVID/WeVerify plugin
- ☐ Manual site inspection performed in incognito mode (bypasses AI cloaking filters)
- ☐ URL manually typed (not accessed via email link or search ad)

References (APA)

Anti-Phishing Working Group. (2025). Phishing activity trends report, Q4 2024. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf

Association of Internet Research Specialists. (2026). CIRS™ program training modules 1–23. AOFIRS. https://aofirs.org

CloudSEK. (2026). Best AI deepfake detection platforms in 2026: Accuracy, coverage and enterprise integration. CloudSEK. https://www.cloudsek.com/knowledge-base/best-ai-deepfake-detection-tools

Dark Reading. (2025, October 29). AI search tools easily fooled by fake content. Dark Reading. https://www.darkreading.com/cyber-risk/ai-search-tools-easily-fooled-by-fake-content

Deloitte. (2025). The future of fraud: AI-assisted scam risk projections 2025–2027. Deloitte Global.

European Parliamentary Research Service. (2025, July). Deepfakes and synthetic media: The escalating challenge for information integrity. European Parliament. https://www.europarl.europa.eu/thinktank

Federal Trade Commission. (2025). Online shopping and e-commerce fraud: Consumer guidance. FTC. https://consumer.ftc.gov/articles/shopping-avoiding-frauds-scams

Get Safe Online & ScamAdviser. (2026). Check a website: Free scam and fraud detection tool. Get Safe Online. https://www.getsafeonline.org/checkawebsite/

highervisibility.com. (n.d.). How to identify fake customer reviews and testimonials. HigherVisibility. https://www.highervisibility.com

iProov. (2025). The iProov biometric threat intelligence report 2025: Human vs. machine detection accuracy for synthetic media. iProov. https://www.iproov.com

Jenova AI. (2026, May). AI fake news detector: Spot misinformation before it spreads. Jenova AI. https://www.jenova.ai/en/resources/ai-fake-news-detector-202605

Keepnet Labs. (2026). Deepfake statistics 2025–2026: Financial losses, incident trends, and detection challenges. Keepnet Labs. https://keepnetlabs.com

KnowBe4. (2025). 2025 phishing threat trends report (September 2024–February 2025). KnowBe4. https://www.knowbe4.com

lifewire.com. (n.d.). How to determine if a website is legitimate. Lifewire. https://www.lifewire.com

info.legalzoom.com. (n.d.). Website copyright: What you need to know. LegalZoom. https://www.legalzoom.com

Norton / LifeLock. (2026, January 22). How to identify fake websites: 13 clues. Norton LifeLock. https://lifelock.norton.com/learn/fraud/how-to-identify-fake-websites

Panda Security. (2026, April 10). Scammers use AI to build fake websites: Spot the scams. Panda Security. https://www.pandasecurity.com/en/mediacenter/scammers-use-ai-build-fake-websites/

Packetlabs. (2025, July 1). How to identify fake websites: 10 warning signs. Packetlabs. https://www.packetlabs.net/posts/how-to-identify-fake-websites-10-warning-signs/

Safety Detectives. (2026, March 14). How to identify fake websites: Complete 2026 guide. Safety Detectives. https://www.safetydetectives.com/blog/how-to-identify-fake-websites/

U.S. Trade Representative. (n.d.). Annual report on notorious markets for counterfeiting and piracy. USTR. https://ustr.gov

U.S. Copyright Office. (n.d.). Search copyright records. U.S. Copyright Office. https://www.copyright.gov

USCSI Institute. (2025, November 21). AI-powered phishing detection and prevention strategies for 2026. USCSI Institute. https://www.uscsinstitute.org/cybersecurity-insights/blog/ai-powered-phishing-detection-and-prevention-strategies-for-2026

ZoomInfo. (n.d.). ZoomInfo professional intelligence database. ZoomInfo. https://www.zoominfo.com

Index

A

About Us page analysis, 9–11
Accreditation verification, 29–30
Address verification, 20–21
AI cloaking technique, 33, 34
AI-generated content detection, 19, 35–36
AI image detectors, 25, 35
Animated team profile images, 28
ANEC research on trust marks, 28
Anti-Phishing Working Group (APWG), 5, 14
Authorized resellers, 27–28

B

Background checks, individual, 26–27
Better Business Bureau (BBB), 10, 29
Billing address verification, 18
Browser security indicators, 17, 36
Buzzword saturation in reviews, 31

C

Certificate Authority (CA), 18, 36
Certificate Transparency (crt.sh), 18, 35
Certification (vs. accreditation), 29–30
Channel partners, 27–28
Checkout security, 17–18
CNAM lookup, 21
Color analysis, product images, 15–16
Consumer complaints, e-commerce, 14
Contact form verification, 22
Copyright notice verification, 22
Corporate background check, 11–13
Counterfeit product categories, 15
Customer reviews, fake indicators, 30–31

D

Dead links, homepage, 7
Deepfakes, 5, 19–20, 34–35
Deepfake detection tools, 35–36
Deepfake statistics, 34
Digital certificate verification, 18
Digital footprint verification, 10
Domain registration check, 35, 36
Duplicate reviews, 31

E

E-commerce fraud, 14
ELA (Error Level Analysis), 25, 35
Email address verification, 21–22
Email checker tools, 22
EXIF metadata analysis, 25

F

FotoForensics.com, 25, 35
FTC consumer guidance, 18, 32
Fake review indicators, 30–32
Fake logo identification, 6

G

Generative AI website cloning, 5, 7, 33–34
Google Safe Browsing, 35, 36
Google Transparency Report, 36

H

Homepage layout indicators, 7–8
HTTPS verification, 17–18

Grammar errors as red flags, 10, 31

I

Image tampering detection, 25–26
iProov study on deepfake detection, 5, 34
InVID/WeVerify plugin, 20, 35

K

KnowBe4 phishing report, 5, 34
Keepnet Labs deepfake statistics, 5, 34

L

Legal contracts, reading, 18
Licensing verification, 29–30
LinkedIn profile verification, 11–12
Logos, fake website, 6
Logo reverse image search, 6

M

Management team photo verification, 11–13
Malware risk, fake sites, 14
Mixed content security warning, 18, 36

N

NewsGuard AI content farm tracking, 5, 34
Norton Safe Web, 35

P

Panda Security AI cloning report, 5, 33
PhishTank, 35, 36
Phone number verification, 20–21
Pixel quality, logo assessment, 6
Plagiarism detection, policy pages, 8
Privacy Policy verification, 8–9
Profile photo verification, 11–13

R

Refund policy, 17
Reverse email confirmation tools, 22
Reverse image search tools, 6, 23
Review plagiarism check, 32

S

ScamAdviser, 35
SEC EDGAR database, 13, 28
Social media verification, 26–27
SSL/TLS certificate verification, 17–18
Stock photo identification criteria, 23–25

T

Testimonials vs. third-party reviews, 30
TinEye reverse image search, 6, 23
Trapcall phone tracking, 21
Trust seals, 18, 28–29
Trust mark verification, 28–29

U

URLVoid, 35, 36
USTR counterfeiting report, 14

V

Video verification checklist, 20

W

WeVerify plugin, 20, 35

VoIP phone detection, 20–21
WHOIS domain lookup, 22, 35
Website cloning, AI-powered, 33–34

Z
ZoomInfo corporate database, 11

— End of Training Module 9 — Unit 23 —

© 2026 Association of Internet Research Specialists (AOFIRS) | aofirs.org

Association of Internet Research Specialists

This combined Research Report and Training Guide constitutes Unit 23 of the Certified Internet Research Specialist (CIRS™) Program developed by the Association of Internet Research Specialists (AOFIRS). It addresses one of the most critical competencies for professional online researchers: the systematic identification of fake, fraudulent, or deceptive websites.

Fake websites represent a sophisticated and growing threat to consumers, businesses, researchers, and institutions worldwide. The Anti-Phishing Working Group (APWG) identified nearly 1.8 million new phishing and fake websites in the latter half of 2024 alone. By 2026, generative AI tools have dramatically lowered the barrier to creating convincing fake sites—enabling the rapid cloning of entire websites, including layouts, SSL certificates, trust seals, and policy pages, within minutes.

This report provides a comprehensive, structured methodology for evaluating every major component of a website—from homepage logos and navigation to checkout processes, contact information, and third-party trust marks. Each section integrates foundational techniques developed through AOFIRS research methodologies with new 2025–2026 findings on AI-assisted fraud, deepfake proliferation, and browser-based detection tools.

Identifying Fakes in Website Content Pages

May 10, 2026

Submitted by:
Naveed Manzoor

USVA7777904052027

Association of Internet Research Specialist | AOFIRS