Website Spoofing & Online Scam Preparedness Checklist

This checklist provides actionable steps for your clients to prevent website spoofing and online scams, and to respond effectively if an incident occurs.

I. Immediate Incident Response (If a Scam is Active)

- **Public Warning:**
  - □ Post prominent warnings on your official website (`yourcompany.com`), social media, and email newsletters.
  - □ Clearly state the fraudulent domain (`fakecompany.com`) and advise customers to only use the official site.
  - □ Provide instructions for scammed customers (e.g., report to bank, authorities).
- **Reporting to Authorities:**
  - □ File a detailed complaint with the **FBI Internet Crime Complaint Center (IC3)** at `ic3.gov`.
  - □ Report the scam to the **Federal Trade Commission (FTC)** at `ReportFraud.ftc.gov`.
  - □ Submit a report to the **Better Business Bureau (BBB) Scam Tracker** at `bbb.org/scamtracker`.
  - □ Contact **local law enforcement** if there is immediate danger or significant financial loss.
- **Engaging Domain & Hosting Providers:**
  - □ Use the **ICANN Lookup tool** (`lookup.icann.org`) to identify the domain registrar and hosting provider of the fraudulent site.
  - □ Immediately report the fraudulent activity (phishing, trademark infringement, malware) to both the domain registrar and hosting provider.
- **Report to Google for De-indexing:**
  - □ To prevent the copycat website from appearing in Google Search results, report it directly to Google.
  - □ **Phishing Report:** Use Google's Phishing Report form if the page is designed to steal personal information by posing as your legitimate site.
  - □ **Copyright Infringement (DMCA Takedown):** If the copycat site uses your copyrighted material (e.g., logo, unique text, images), file a Copyright Removal

Request (DMCA Takedown). This can lead to the removal of the infringing page from search results.
  - □ **Spam Report:** For general spammy content or deceptive practices, use Google's Spam Report form.
  - □ Provide the specific URL(s) of the infringing content and detailed evidence.

- **Legal Recourse:**
  - □ Consult an **intellectual property attorney** to discuss legal options.
  - □ Initiate a **Uniform Domain-Name Dispute-Resolution Policy (UDRP)** proceeding through an ICANN-approved provider (e.g., National Arbitration Forum) if applicable.
  - □ Explore legal action under the **Anticybersquatting Consumer Protection Act (ACPA)** for "bad faith intent to profit."
  - □ Ensure your brand name and logo are **properly trademarked** with the USPTO.
  - □ **Document everything:** Keep meticulous records of all communications, evidence of the scam, client complaints, and financial losses.

II. Proactive Prevention: Domain & Brand Protection

- **Strategic Domain Registration:**
  - □ Register common misspellings and typographical errors of your primary domain name.
  - □ Register your domain name across various popular Top-Level Domains (TLDs) (e.g., `.net`, `.org`, `.biz`).
  - □ Configure all defensively registered domains to automatically redirect to your legitimate, official website.

- **Continuous Monitoring:**
  - □ Subscribe to a reputable **domain monitoring service** that tracks new domain registrations similar to your brand.
  - □ Ensure the service offers detection for typosquatting, brand impersonation, phishing, and fraudulent SSL certificates.
  - □ Utilize services with automated or managed takedown capabilities for malicious domains.
  - □ Implement **brand monitoring tools** to track mentions of your brand across the internet and social media.

III. Proactive Prevention: Website & Email Security

- **Website Security Fundamentals:**
  - □ Ensure all client websites use **HTTPS/SSL certificates** for encrypted

connections (look for the padlock symbol).

- □ Implement a **Web Application Firewall (WAF)** to filter malicious traffic and protect against web-based attacks (e.g., SQL injection, XSS).
- □ Ensure robust **DDoS (Distributed Denial of Service) protection** is in place to prevent website downtime.
- □ Keep all website **software, plugins, and themes consistently updated** to the latest versions.
- □ Choose a **secure and reputable web hosting provider** with built-in security measures (firewalls, malware scanning, DDoS mitigation).
- □ Implement **regular, automated website backups** and store them securely off-site or in a separate cloud environment.

- **Authentication & Access Control:**

  - □ Enforce **strong, unique password policies** for all accounts, especially administrative access.
  - □ Mandate **Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA)** for all internal systems and client-facing accounts wherever possible.
  - □ Implement **Zero Trust principles** by limiting user access and permissions based on the principle of least privilege.

- **Email Security:**

  - □ Implement and properly configure **Sender Policy Framework (SPF)** records for all email domains.
  - □ Implement and properly configure **DomainKeys Identified Mail (DKIM)** for all email domains.
  - □ Implement and properly configure **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** policies (starting with `p=none` for monitoring, then `p=quarantine`, then `p=reject`).

IV. Proactive Prevention: Education & Awareness

- **Employee Training:**

  - □ Conduct **regular, updated training** for all employees on how to identify phishing emails, spoofed websites, and social engineering tactics.
  - □ Emphasize scrutinizing URLs, checking sender email addresses, and being wary of urgent or unexpected requests.
  - □ Establish a clear **protocol for reporting suspicious emails and websites** to the IT department or designated security personnel.
  - □ Conduct **phishing simulations** to test and reinforce employee awareness in a controlled environment.
  - □ Promote **password hygiene** and the use of password managers.

- **Customer Education:**

- □ Provide clear, accessible resources (e.g., blog posts, FAQs, dedicated webpage) on **"How to Spot a Scam"**.
- □ Advise customers to **carefully check URLs** for misspellings, extra characters, or unusual TLDs, even if HTTPS is present.
- □ Instruct customers to **manually type official website addresses** or use trusted bookmarks instead of clicking links in emails.
- □ Warn customers about common red flags: poor grammar/spelling, malicious pop-ups, missing privacy policies, or requests for direct bank transfers as the only payment method.
- □ Clearly communicate that your company will **never ask for sensitive information** (passwords, full credit card numbers) via unsolicited email or phone calls.
- □ Provide a **clear and easy way for customers to report suspicious activity** directly to your company.

V. Incident Preparedness: Response & Communication

- **Incident Response Plan (IRP):**

  - □ Develop a comprehensive **Incident Response Plan (IRP)** outlining procedures for before, during, and after a security incident.
  - □ Define clear **roles and responsibilities** for a cross-functional incident response team (IT, security, legal, communications, leadership).
  - □ Establish phases: **Preparation, Identification, Containment, Eradication, Recovery, and Post-Incident Activity/Lessons Learned**.
  - □ Conduct **regular cybersecurity drills** (e.g., tabletop exercises, simulated attacks) to test the plan and team readiness.

- **Crisis Communication Strategy:**

  - □ Develop a **crisis communication plan** defining purpose, target audiences (employees, customers, media, regulators), key messages, and designated spokespersons.
  - □ Prioritize **transparency, empathy, and clarity** in all communications.
  - □ Prepare **holding statements** to ensure consistent messaging across all spokespeople.
  - □ Establish **secure internal communication channels** for the incident response team.
  - □ Plan for **external communication channels** (e.g., dedicated webpage, press releases, email alerts, telephone helplines).
  - □ Ensure timely **notification to relevant regulatory bodies** (e.g., GDPR, if applicable).
  - □ Commit to **ongoing dialogue** with stakeholders even after the immediate crisis, providing updates on recovery and preventative measures.