Protecting Your Business Online: Website Cloning Response Kit

Quick-Action Checklist

- Confirm and document the cloned site
- Use WHOIS lookup to identify host/registrar
- Submit takedown requests
- Report to search engines and Canadian authorities
- Notify your web host and clients
- Register popular domain variants
- Monitor with suggested tools

Step-by-Step Guide to Responding

1. **Document the Cloning**

   o Capture screenshots and record the domain name.

   o Compare it with your legitimate site to identify copied content.

2. **Submit a Takedown Request to the Hosting Provider**

   o Use WHOIS lookup (e.g., https://lookup.icann.org) to identify the host.

   o Contact the hosting provider directly with the included template.

3. **Contact the Domain Registrar**

   o Use the registrar's abuse form or email.

   o Provide evidence of trademark/copyright infringement.

4. **Report the Clone Site to Search Engines**

   o Google: https://support.google.com/websearch/troubleshooter/3111061

5. **Inform Your Audience**

   o Use the included message template to warn clients of fraudulent activity.

6. **Consider Legal Action**

   o If damage is significant, consult a lawyer who specializes in IP or cybercrime.

Sample Takedown Request: Hosting Provider

Subject: Urgent Takedown Request – Cloned Website Hosting Infringement

Dear [Hosting Provider],

My name is [Your Name], and I am the owner/operator of the legitimate website [www.yoursite.ca]. A fraudulent copy of our website is being hosted at [fraudulent-url.com], which violates our intellectual property rights.

Please find attached:

- Screenshots showing the copied content

- Our site ownership details

- A WHOIS record showing your platform is hosting the clone

We respectfully request that this fraudulent website be taken down immediately under your abuse policy.

Thank you for your swift attention.

Sincerely,

[Your Full Name]

[Outfitter Business Name]

[Email Address]

Sample Takedown Request: Domain Registrar

Subject: Request to Suspend Fraudulent Domain – Cloned Website

Dear [Registrar Abuse Team],

I am writing to notify you that the domain [fraudulent-url.com] is hosting a cloned version of our website, [www.yoursite.ca], and is likely intended to mislead consumers.

This is a clear case of copyright and potential trademark infringement. Please suspend this domain or take appropriate action under your abuse policies.

Evidence attached:

- Screenshots

- Ownership of original domain

- WHOIS details

Thank you,

[Your Full Name]

[Outfitter Business Name]

[Email Address]

Sample Client Communication Template

Subject: Fraud Alert – Cloned Website Warning

Dear [Client Name],

We've recently discovered a fraudulent website impersonating our business under a similar name or domain (e.g., .com instead of .ca).

Please be aware that our only official website is: [www.yoursite.ca]. If you see anything suspicious, do not engage—report it to us directly.

We are taking steps to address this issue and thank you for your continued support.

Sincerely,

[Your Name]

[Business Name]

Tips for Prevention & Monitoring

- Register common variants of your domain (e.g., .com, .net, .org, .ca)
- Use tools like:
    - https://www.domaintools.com/
    - https://www.namechk.com/
    - https://whois.domaintools.com/
- Set up Google Alerts for your business name and key phrases

🚧 **Report Fraudulent Sites in Canada**

- **RCMP National Cybercrime Coordination Unit**: https://www.cyber.gc.ca

- **Canadian Centre for Cyber Security**: https://cyber.gc.ca/en/

- **Competition Bureau Canada (for deceptive marketing)**: https://www.competitionbureau.gc.ca/

GOABC is committed to helping our members protect their businesses and reputations online. This toolkit offers essential tools, not legal representation. We encourage members to seek legal or IT support where needed.