5 Domain Name Scams Targeting Website Owners

Posted on November 14, 2025

Your domain name is one of the most valuable digital assets you own. It is your address and a central hub for your business, and because of this, your domain name is a prime target for opportunistic scammers.

It's not just about stealing a domain name from you — there are other types of domain name scams. In this post, we discuss some of the most pervasive domain name scams, detailing how each of them works and the steps you can take to avoid falling victim to them.

1. Domain Slamming

Domain slamming is a type of domain name scam where a shady registrar tricks domain owners into transferring their domain names to them. It is also known as a *fake domain renewal scam* since the offending registrar sends urgent-looking notices, either by email or snail mail, claiming the target domain is about to expire and requires immediate renewal.

These notices are designed to appear very serious, complete with professional-looking logos and references to the actual domain name and expiration date (information easily obtained from public WHOIS records).

If the victim falls for the trick, they unknowingly transfer their domain registration to a new registrar. Instead of simply paying a renewal fee, they are signing an agreement to switch registrars and pay a grossly inflated rate — sometimes ten times the normal price — for the transfer and future renewals. Victims end up overpaying and inadvertently moving their valuable domain to a company with shady practices and poor security.

Example

Here’s an example of domain name slamming that involved Domain Registry of America, an ICANN-accredited registrar that had been suspended since 2014. However, other shady registrars still use similar tactics to this day.

Domain
RENEWAL GROUP

Domain Name Renewal Service

Call us at 1-905-479-2533 24 hours a day
or visit us at www.domainrenewalgroup.com

As a courtesy to domain name holders, we are sending you this reminder that your domain name registration is due to expire in the next few months. When you switch today to the Domain Renewal Group, you can take advantage of our best savings. Your registration for: **domainincite.com** will expire on **February 27, 2012**. Act today!

Domain name:	domainincite.com
Reply Requested By:	October 31, 2011

Registering your name with us will ensure you retain exclusive rights to it on the Web, and now is the time to transfer and renew your name from your current Registrar to the Domain Renewal Group. Failure to renew your domain name by the expiration date may result in a loss of your online identity making it difficult for your customers and friends to locate you on the Web.

Privatization of Domain Registrations and Renewals now allows the consumer the choice of Registrars when initially registering and also when renewing a domain name. Domain name holders are not obligated to renew their domain name with their current Registrar or with the Domain Renewal Group. We would like you to transfer and renew your name from your current Registrar; review our prices and decide for yourself. You are under no obligation to pay the amounts stated below, unless you accept this offer. **This notice is not a bill**, it is rather an easy means of payment should you decide to switch your domain name registration to the Domain Renewal Group.

Term	Period Covered	Price
1 year	Until -- Feb 27, 2013	**£ 25.00**
2 years (Recommended)	Until -- Feb 27, 2014	**£ 40.00 (save £ 10)**
5 years (Best Value)	Until -- Feb 27, 2017	**£ 75.00 (save £ 50)**

The following names are currently available for you to register and secure, protecting your domain name from being duplicated.

Other Available Domains	Period Covered	Price
domainincite.net	2 Years	£ 40.00
domainincite.org	2 Years	£ 40.00

Registration of the above domain names includes DNS, URL and Email Forwarding to a website and mailbox you designate.

Transfer and renew your domain name online at **www.domainrenewalgroup.com** 24 hours a day, 7 days a week or call our Customer Service Department at +1 905 479 2533 to transfer and renew your domain name today.

Please detach this stub and include it with your payment.

Check the appropriate boxes of the Domain names you would like to order.

See reverse for payment address:

Current Domain name

domainincite.com

1 Year ..... £ 25.00 ☐
2 Year ..... £ 40.00 ☐
5 Year ..... £ 75.00 ☐

Available Domain names (***optional***)

domainincite.net
1 Year ..... £ 25.00 ☐
2 Year ..... £ 40.00 ☐
5 Year ..... £ 75.00 ☐

domainincite.org
1 Year ..... £ 25.00 ☐
2 Year ..... £ 40.00 ☐
5 Year ..... £ 75.00 ☐

Total $ _____

KEVIN MURPHY

34100

Please print your domain name on your check.
If paying by credit card, please enter your information below:

Card Number:

Expiry: ☐☐ / ☐☐

Signature

You must provide a valid email address to complete your renewal

Domain Incite

How to Protect Yourself

- **Know your registrar**: Keep a record of your current, legitimate domain registrar (e.g., Namecheap, GoDaddy, Google Domains) and the exact domain expiration date. If a notice comes from any other company, it is a scam. You can always log into your account with the registrar and check the expiration date for every domain that you have with them.

- **Enable domain locking**: This security feature, also known as ClientTransferProhibited, prevents unauthorized transfers of your domain to another registrar. This can be enabled in the domain settings when you log into your registrar's account. To see if your domain has this feature already enabled, use WHOIS Lookup to see the domain status codes.

```
  <rawText>Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-08-02T02:17:33+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns4.google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
Name Server: ns2.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-11-04T17:48:58+0000 <<<
```

- **Set up auto-renewal**: Enabling auto-renewal ensures that your domain is paid for and renewed automatically with the same registrar, neutralizing the fear and urgency that domain slamming notices try to exploit.

Learn more about other domain risks.

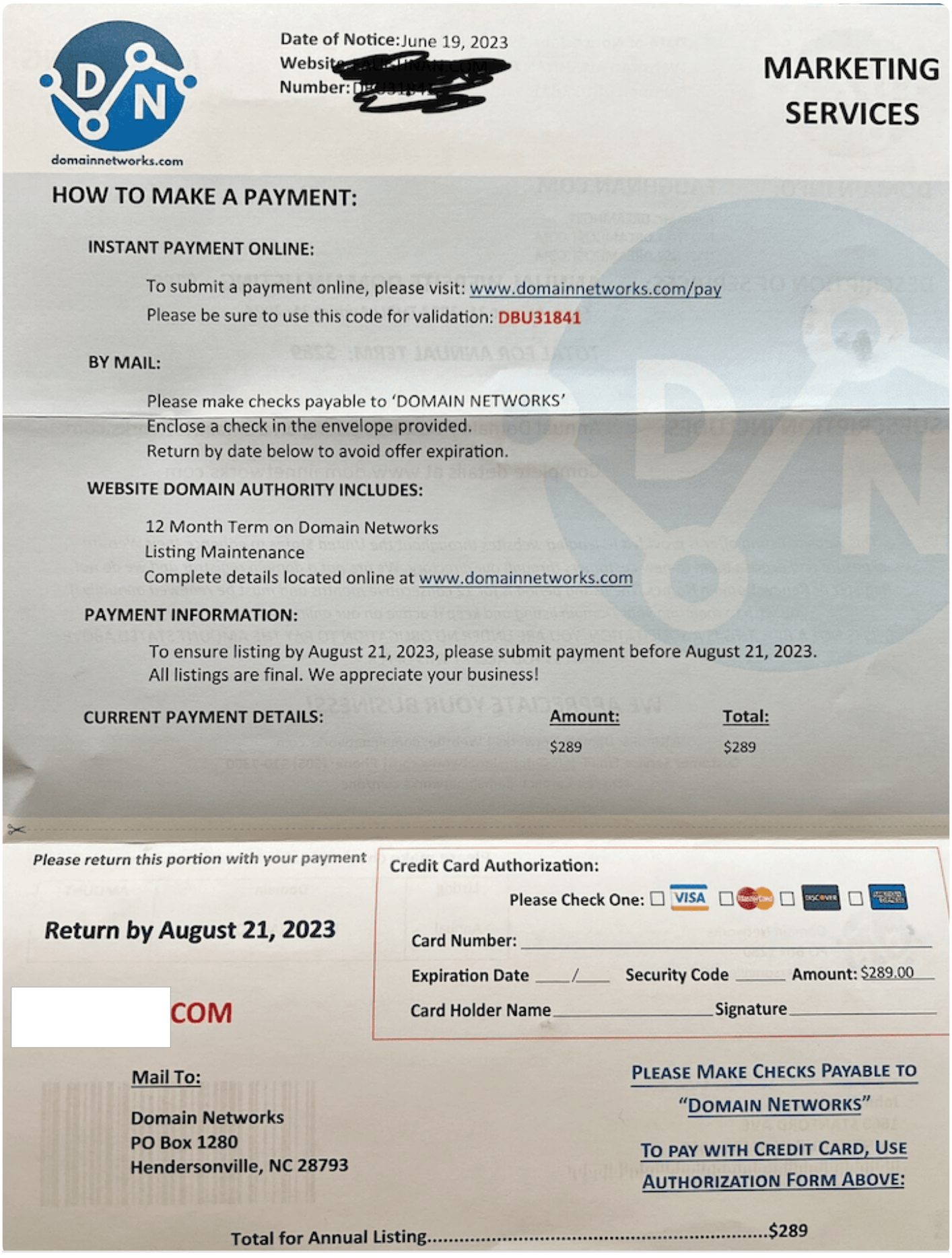
2. Fake Invoice Scams

In this scheme, scammers send official-looking invoices that aren't for renewal but for entirely made-up services, such as an expensive, unrequested domain listing service or a search engine optimization (SEO) service that was never ordered. These fake invoices are typically sent via postal mail to small businesses that process invoices without closely vetting the service description. They prey on the hope that someone will simply pay the bill without realizing the service was never requested or rendered.

Examples

A high-profile fake invoice case involved a Canadian firm operating under names like ILS Corp. and Domain Listing Service Corp. According to a report by SC World, this firm sent misleading invoices to small businesses for services that were never ordered or provided. They even registered slight variants of the victim's domain to create an additional layer of legitimacy. The Federal Trade Commission (FTC) took action, freezing the assets of the defendants and imposing a multi-million-dollar suspended judgment based on the harm caused to consumers. However, the defendants couldn’t pay, so they were fined US$10,000 instead.

Other recent examples of this scam include the “Web Listings” and “DomainNetworks” snail mail scam, where companies respectively named Web Listings, Inc. and DomainNetworks, sent out letters to domain owners. The letters were made to look like a bill for SEO or marketing services. Here’s an example:



domainnetworks.com

Date of Notice: June 19, 2023
Website: [redacted]
Number: [redacted]

MARKETING SERVICES

HOW TO MAKE A PAYMENT:

INSTANT PAYMENT ONLINE:

To submit a payment online, please visit: www.domainnetworks.com/pay
Please be sure to use this code for validation: **DBU31841**

BY MAIL:

Please make checks payable to 'DOMAIN NETWORKS'
Enclose a check in the envelope provided.
Return by date below to avoid offer expiration.

WEBSITE DOMAIN AUTHORITY INCLUDES:

12 Month Term on Domain Networks
Listing Maintenance
Complete details located online at www.domainnetworks.com

PAYMENT INFORMATION:

To ensure listing by August 21, 2023, please submit payment before August 21, 2023.
All listings are final. We appreciate your business!

CURRENT PAYMENT DETAILS:	Amount:	Total:
	$289	$289

Please return this portion with your payment

Return by August 21, 2023

[redacted]COM

Credit Card Authorization:

Please Check One: ☐ VISA ☐ ☐ DISCOVER ☐

Card Number: _____

Expiration Date ____/____ Security Code _____ Amount: $289.00

Card Holder Name _____ Signature _____

Mail To:

Domain Networks
PO Box 1280
Hendersonville, NC 28793

PLEASE MAKE CHECKS PAYABLE TO "DOMAIN NETWORKS"

TO PAY WITH CREDIT CARD, USE AUTHORIZATION FORM ABOVE:

Total for Annual Listing.....$289

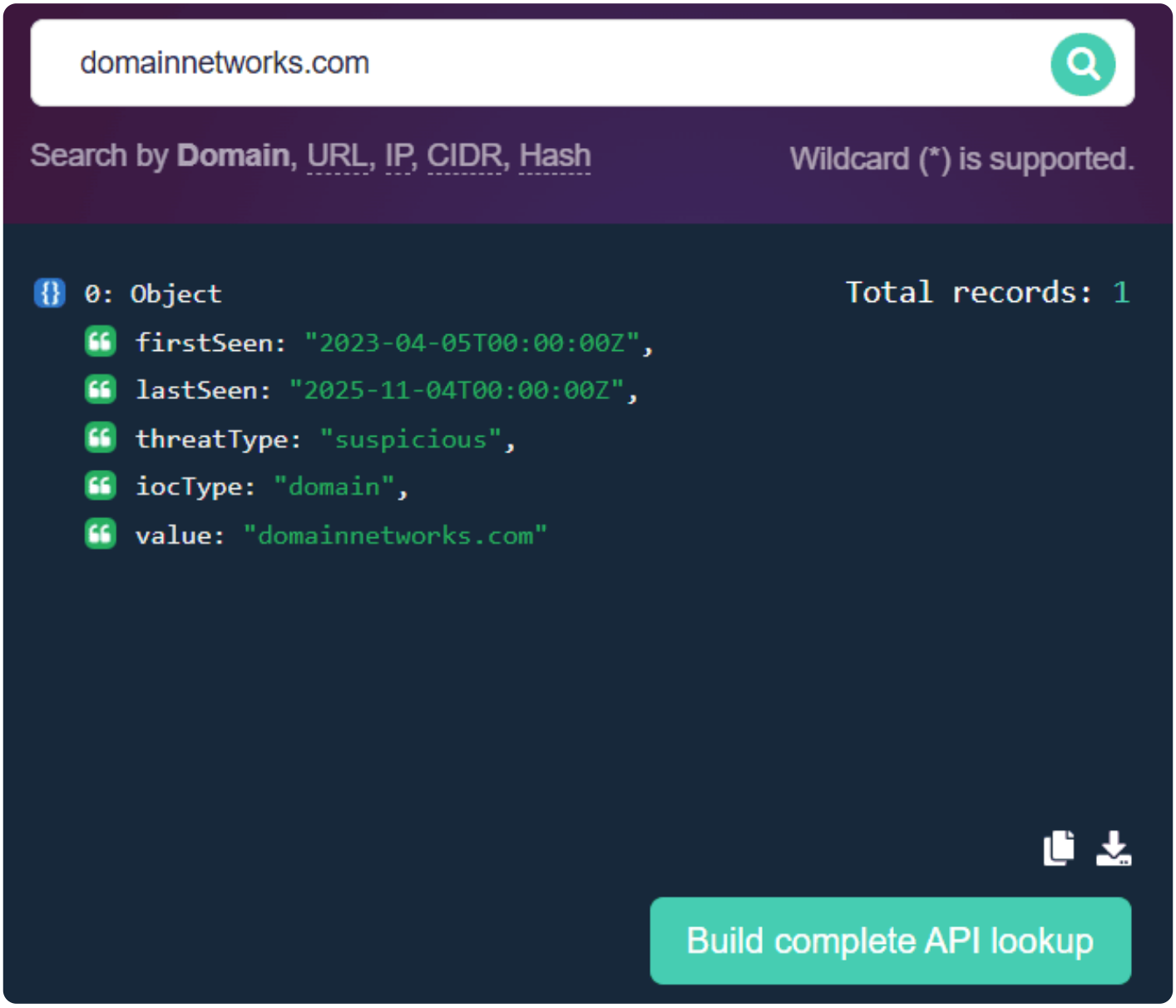
KrebsonSecurity

How to Protect Yourself

- **Implement a strict policy for handling invoices**: Establish a clear, non-negotiable protocol: all bills should be checked against an internal record of ordered services. If a vendor is unknown or the service was not explicitly ordered by a recognized manager, the payment must be flagged and verified before processing.

- **Investigate the company name on the invoice**: Perform a Google search using the company name, combined with terms such as "scam," "fraud," or "complaint," to see if there are any warnings from previous victims.

- **Verify any domain names listed on the invoice**: Use WHOIS Lookup to learn more about the website that appears on the invoice, or quickly check the Threat Intelligence API to see if the domain is safe, suspicious, or malicious. The domain domainnetworks[.]com on the DomainNetworks scam, for example, is flagged as suspicious:



- **Conduct regular security awareness training**: Educate your financial staff on the prevalence of fake service invoices.
- **Read the fine print**: Look for telltale disclaimers that state the document is a solicitation or advertisement and not an actual bill. These are often hidden in tiny font.

3. Domain Appraisal Scams

Domain appraisal scams target domain owners with an offer to sell their domain that might seem too good to be true. A scammer contacts you, claiming they or a well-funded client wants to buy your domain for a huge sum of money.

The next step is the trap: the buyer insists you must first obtain a certificate of appraisal from a specific appraisal service they recommend.

Example

Here is an example of an actual email from a scammer:

> *Dear sir,*
>
> *we are interested to buy your domain name.COM and offer 65% of the appraised market value.*
>
> *As of now we accept appraisals from one of these leading companies:*
>
> *sed o.com*
> *pozde.com*
> *accuratedomains.com*
>
> *Should you already have an appraisal please forward it to us.*
>
> *We appreciate your business,*
>
> *Sincerely,*
>
> *R. Thomas*
> *DNR, Inc.*

Source: Domain Name Wire

The domain appraisal service requires you to pay a fee. Unsurprisingly, this service is associated with the same scammer, and once you pay the appraisal fee, the supposed buyer disappears. The appraisal is either worthless or non-existent.

How to Protect Yourself

- **Don’t pay for appraisals**: If the buyer demands an appraisal, let them pay for it.

- **Use reputable marketplaces**: If you decide to sell your domain, use an established domain marketplace that offers secure escrow and appraisal services, which typically charge a percentage of the final sale rather than an upfront fee.

4. Typosquatting

Typosquatting is a form of brand impersonation that capitalizes on a simple human error: typing a URL incorrectly or not looking at a misspelled URL long enough to see the typo.

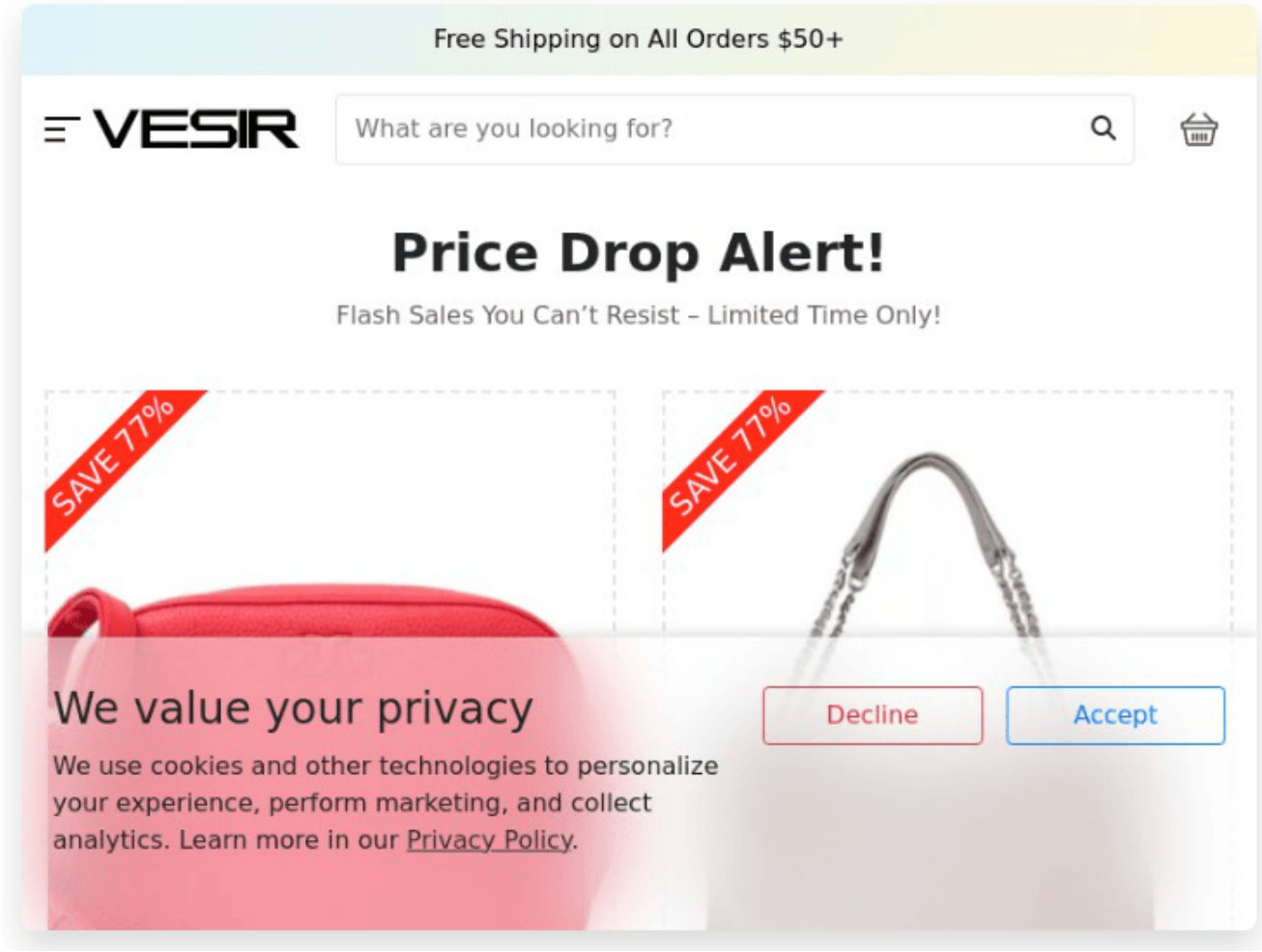
Exploiting this, scammers register misspelled versions of popular domain names to trick users into sharing their private information on fake sites that either just sit on the internet and wait for the users to make a typo or are advertised through phishing emails.

These misspellings involve subtle substitutions, like using 'l' instead of 'i', adding a common suffix, or using a different top-level domain (TLD). For consumers, visiting these typosquatting domains leads to stolen login credentials, malware infections, financial loss through fake transactions, or just buying counterfeit goods. For businesses, these domains can lead to significant brand damage, as well as lost traffic and revenue.

Examples

For example, a user attempting to visit gucci.com might think that guccl[.]com, gucci-beauty.com, or guccil[.]shop is the real address.

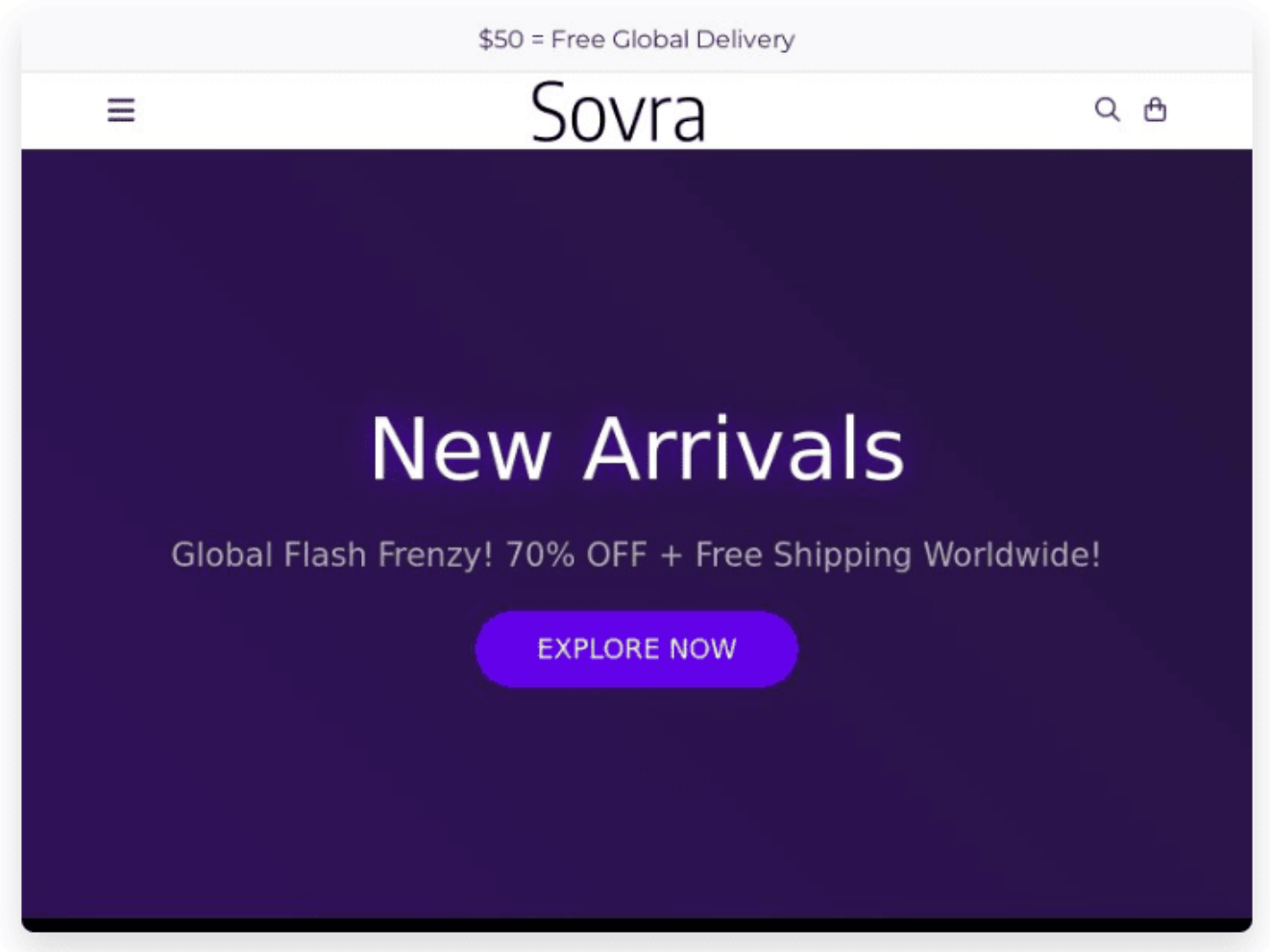
The bogus sites may look legitimate, mimicking the layout and branding of the real company or selling similar products and services. The Website Screenshot Lookup result of some Gucci typosquatting domains, for example, shows e-commerce content, just like the imitated brand.



Website screenshot of guccix1[.]shop



Website screenshot of guccil[.]shop



Website screenshot of guccivibe[.]shop

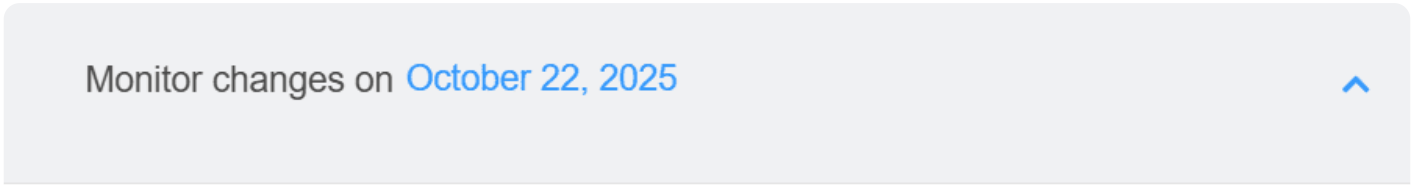


Website screenshot of guccirp[.]com

How to Protect Yourself

- **Monitor typosquatting domain registrations**: Use tools like Brand Monitor to get notified when domains impersonating your company name are registered. To illustrate, we searched for “Gucci” on the Brand Monitor in the Domain Research Suite and found that 27 typosquatting domains were added on October 22, 2025.





Domains added: 27

gucciexq.shop
guccify.shop
guccix9a.com
guccif.shop
guccichic.shop
gucciluxe.shop
gucciluxex.shop
guccil.shop
guccidesign.shop
guccid.shop

Show more

Domains dropped: 11

gucci-beauty.asia
gucci-id.asia
guccicheats.com
guccicosmetics.com
gucciemall.com
gucciiphonecase.com
guccishop-jp.com
kruchegucci.com
leagucciardi.com
leagucciardi.design

Show more

Domains updated: 29

gucci-beauty.com
gucci-by-gucci-pour-homme.com
gucci-by-gucci.com
gucci-cosmetics.com

Domains discovered: 1

gucciaimpresores.es

- **Defensive domain registration**: Businesses may choose to register common misspellings and variants of their primary domain (e.g., swapping .com for .co, or using a plural form) to prevent squatters from claiming them and to protect their customers. For example, Amazon does this at scale. Try visiting amazn.com or amozon.com and they'll redirect you to the correct domain.

- **Add predictive threat intelligence to your corporate firewall or DNS filter**: To protect employees, use advanced cybersecurity intelligence sources, such as the Typosquatting Data Feed or the First Watch Malicious Domains Data Feed. With these, you can proactively block access to predicted malicious domains, including typosquatting domains.

- **Conduct security awareness training**: Conduct regular training sessions and simulated phishing campaigns that use typosquatting domains. Teach staff to always check the full URL in the address bar (not just the link text) and to hover their mouse over a link to preview the destination URL before clicking.

5. Trademark Protection Scam

This scam preys on a business owner's fear of losing their trademark or brand name in a new market. The target receives an email or phone call from someone claiming to represent a domain registration service or the Intellectual Property Office (IPO). The message states that a company (often based overseas) is attempting to register your domain name using various country-code top-level domains (ccTLDs), and there is usually a great sense of urgency. Here's an example of such an email, posted on LinkedIn:

Dear CEO, (It's very urgent, please transfer this email to your CEO. If this email affects you, we are very sorry, please ignore this email. Thanks)

We are a Network Service Company which is the domain name registration center in China. We received an application from **Rui De Ltd** on September 15, 2025. They want to register "publicmediasolution" as their Internet Keyword and "XXXXXXXXXXX.cn", "" vvvvvvvvvvvv.com.cn", "abababababab .net.cn", "abcabcabcabc.org.cn" domain names. But after checking it, we find "xxxxxxxxxxxxx" conflict with your company name or trademark. In order to deal with this matter better, so we send you email and confirm whether this company is your distributor or business partner in China or not?

Best Regards

Mike Zhang | *Service Manager* Domain Registrar (Head Office)

No. 300, Xuanhua Road, Changning District, Shanghai200050, China Tel: +86-2161918696 | Fax: +86-2161918697 | Mob: +86-1582177 1823

Source: LinkedIn

The scammer would then offer to protect your brand by registering all these additional domain extensions on your behalf, but only if you pay an exorbitant fee right away. The threat is that if you don't act immediately, the other company will gain legal standing and cause major trademark infringement issues. In reality, no one is registering anything, and you are simply paying a high fee for unnecessary domains or, worse, nothing at all.

How to Protect Yourself

- **Consult a trademark attorney**: If you receive a communication that genuinely concerns your intellectual property, do not respond directly to the sender. Contact your legal team or a trademark attorney immediately for advice.

- **Monitor the use of your brand name in domain registrations**: Use Brand Monitor to receive notifications when your brand name is registered under various TLDs.
- **Only use trusted registrars**: If you decide to defensively register other TLDs, do so directly through your current, verified, and trusted domain registrar.
- **Implement security awareness training**: Ensure that employees are trained on how scammers exploit authority and fear to create a sense of urgency. They should also be taught to immediately report and never act upon unsolicited communications that threaten legal or financial loss if immediate action isn't taken.

Conclusion

A healthy level of skepticism and a thorough understanding of the schemes detailed above are your first and best lines of defense against domain name scams. Slow down and think first. Scammers rely on urgency to make you click, pay, or sign over control of domain names. Always pause, independently verify the source, and never pay an unexpected invoice without checking your records.

There are also resources that can help you stay ahead of scammers.

- Tools like WHOIS Lookup let you instantly verify your domain's actual registration status.
- Services such as Brand Monitor proactively scan the internet for fraudulent lookalike domains that target your brand.
- Additionally, security solutions like Threat Intelligence API and First Watch Malicious Domains Data Feed help protect your employees by preventing them from accidentally visiting known malicious domains and those that are likely to turn malicious.