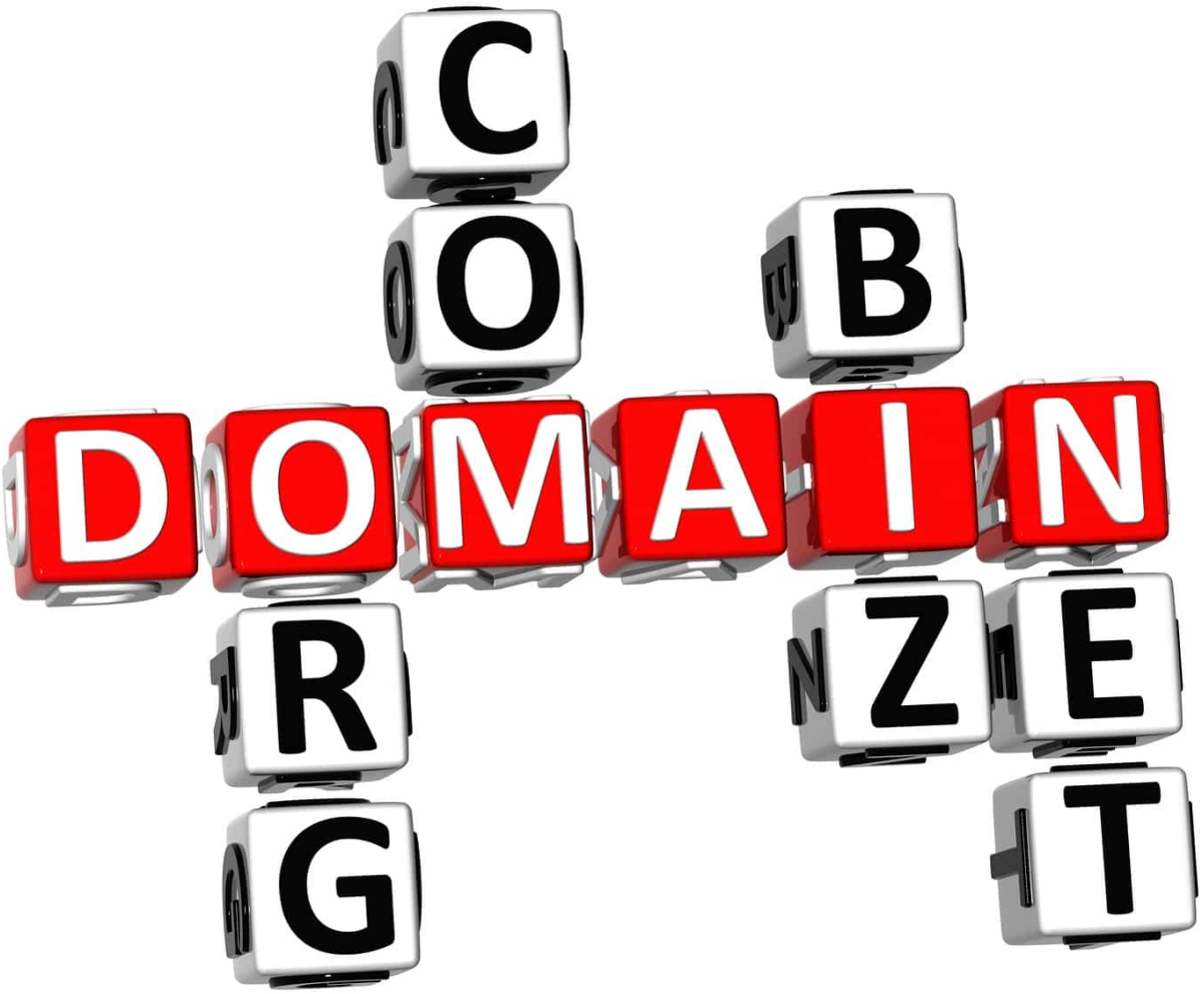
How to Maintain Your Domain’s Integrity for Better Cybersecurity with a Domain Name API

Posted on March 2, 2020



In a technologically-forward world we live in today, cybercriminals are employing more sophisticated attacks to compromise domains. In the latest report by the Federal Bureau of Investigation (FBI), email frauds such as business email compromise (BEC) scams via spoofed domains have caused users $26 billion in losses.

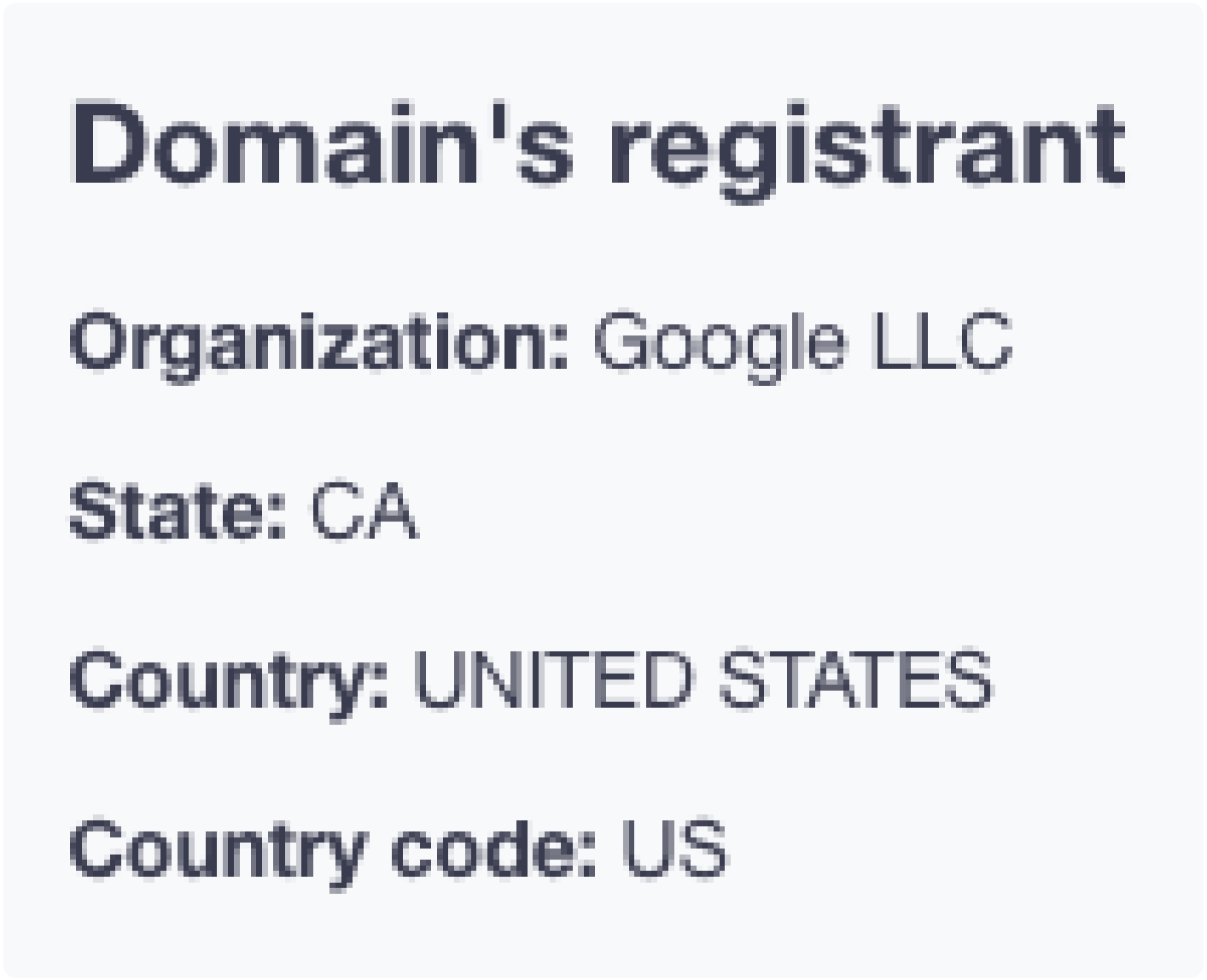
For this reason, domain name security is now more important than ever. You can never be sure who is getting to you except when you take the time to get to know them. And that is possible with the use of domain name tools like WHOIS API.

Domain Integrity Best Practices Aided by WHOIS API

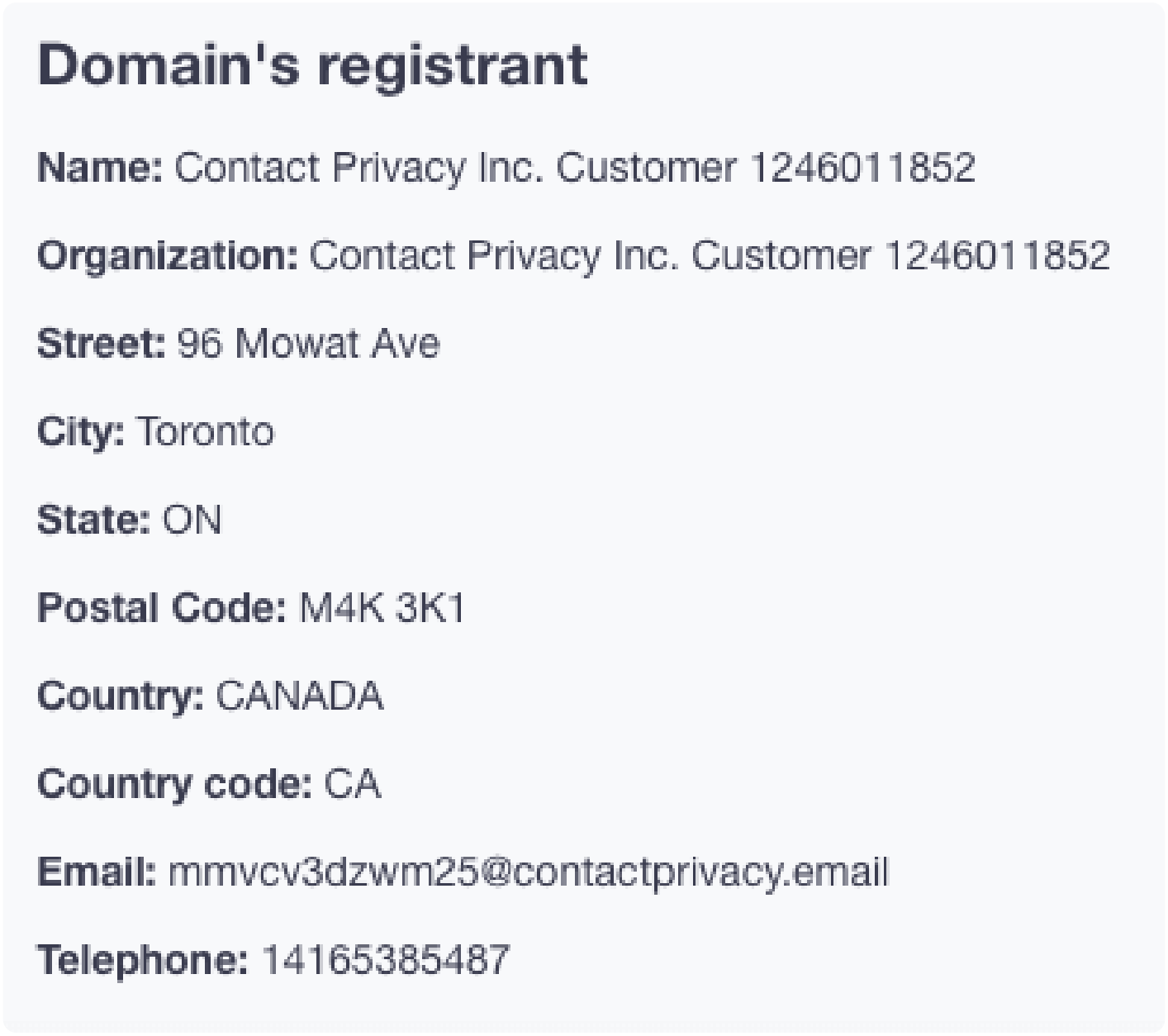
Make your organization the owner of your domain

While technical, administrative, and billing contacts are required when registering a domain and using specific employees' names and contact details are okay for those, we don't recommend using private contact information for your corporate domain's registrant. It could lead to losing domain ownership if that individual leaves the company. And let's face it, reclaiming ownership of your domain could take a long time and cost a lot of money.

Using your organization's name as the domain registrant also increases its authority. When users investigate your domain using a **domain registration API** for whatever purpose, be it validating its authenticity, seeing a legitimate company tied to it lessens suspicions that it has anything to do with malicious activity. Take a look at the following examples:


Domain's registrant
Organization: Google LLC
State: CA
Country: UNITED STATES
Country code: US

google[.]com



savetogooglephotos[.]com (a confirmed phishing site spoofing Google obtained from PhishTank)

Now, when you see these WHOIS records, it’s clear that the first one inspires more confidence.

Register your domain name for the maximum period allowed

A one-year registration, while easy on your budget, may cause you to lose ownership if you forget to renew it. While losing ownership to a non-malicious user should be okay since you can just offer to repurchase it, a more unscrupulous new owner could ask for a hefty price that you may not be able to afford. That means all the hard work you put into gaining domain authority goes down the drain. Worse still, if the new owner is a cybercriminal, your old domain may serve as home to a phishing website preying on your clients and customers.

Cybercriminals are also known for using newly registered domains (NRDs) for illicit purposes and for a short period of time only. In fact, cybersecurity specialists often advise users to stay away from NRDs as these may cause redirects to malicious sites, turn out to be malware hosts or phishing and similar pages, or parked sites that make money from pay-per-click (PPC) ads.

Security experts say that a domain's age can be a telltale sign of its legitimacy. In fact, when investigating a cybercrime, they would often look at when a company (most likely being spoofed by criminals) was established and compare this with the suspect domain's registration details indicated in its WHOIS record. If those don't match, they're likely to tag the domain as malicious. Let's take a look at another example:

Parsed domain name: paypal.com

Domain name extension: .com

Estimated domain age: 7490 day(s)

Contact email: hostmaster@paypal.com

Created date: Thu, 15 Jul 1999 05:32:11 GMT

Updated date: Mon, 16 Dec 2019 23:30:19 GMT

Registrar name: MarkMonitor, Inc.

Registar Internet Assigned Numbers Authority ID: 292

WHOIS server: whois.markmonitor.com

Domain EEP status codes by ICANN list: clientUpdateProhibited clientTransferProhibited clientDeleteProhibited serverUpdateProhibited serverTransferProhibited serverDeleteProhibited

Custom field name 1: RegistrarContactEmail

Custom field value 1: abusecomplaints@markmonitor.com

Custom field name 2: RegistrarContactPhone

Custom field value 2: +1.2083895770

Custom field name 3: RegistrarURL

paypal[.]com

paypal[.]official-support[.]cf (a confirmed phishing site spoofing Google obtained from PhishTank)

As is shown, the second phishing domain is most likely not to be associated with PayPal. PayPal was established in 1998. Its domain registration matches this date as it has been up and running since 1999, while the phishing site's domain only went live this year.

Other steps to take to make sure your domain remains yours include:

- **Lock your domain name:** Leaving it "unlocked" can put you at the risk of losing it to someone else. You can do that through the domain name management system as soon as

you register it. You can check if your domain is locked using a **domain name API**:The status “client transfer prohibited, server delete prohibited, and server transfer prohibited” shows that the domain name apple[.]com is locked. All companies should do this to ensure their domain integrity.

- **Provide backup payment details:** Forgetting to pay for registration renewal could also cause you to lose your domain. And so, providing a backup payment method is highly advisable.

- **Provide backup contact information:** If your company decided to use specific individuals as technical, administrative, and billing contacts, make sure that you have a backup contact in case they leave the company. It’s easier to retrieve access to your domain account if they’re gone.

Register variations of your domain name.

Scammers are always on the prowl for look-alikes of popular domains for their attacks. They use conventional hacking techniques such as typosquatting that allow them to use your brand to trick unsuspecting users into providing confidential details such as their payment information. That puts your brand reputation at risk. Registering variations of your domain name limits the likelihood that your brand will get dragged into phishing and other attacks.

For this, you may need the help of other domain monitoring and research tools. Generating possible variations of your domain name may be time-consuming but is doable with Brand Monitor. Its Typos feature automatically generates misspelled variations of your search term (your brand or domain). Choose the ones that can be easily confused with yours and register them as well.

If someone else owns them, you can use a **domain registration API** to retrieve their contact details. You can then buy them from their current owners if you wish to. Bank of America can, for instance, purchase bankofmeríca[.]com as it could easily be mistaken for its domain. Of course, when you run this domain on WHOIS API, you'll know that it isn't the same as the bank's actual domain. It uses the Latin character "í" for "i." Without a **domain name API**, though, that could fool many users.

Only by making domain name security a top priority can you ensure smooth business operations. Beefing up your security means mitigating risks even before your organization gets affected. Always be wary of the different ways in which cybercriminals carry out attacks and protect your domain with tools such as WHOIS API and others to maintain your domain's integrity — which translates into how clients and customers perceive your company.