The Equifax Settlement Case: Shielding Financial Service Customers from Phishing with Domain Research Monitoring

Data breaches continue to plague organizations today. In the first six months of 2019 alone, 3,813 data breaches were recorded, exposing more than 4.1 billion records. This figure translates to more than a 50% increase in victim volume over the past four years. Worse still, three of these recently recorded data breaches made it to the all-time list of top incidents.

Of all these unfortunate events, we decided to take a closer at Equifax's case. First, because it has been the financial sector's biggest breach victim to date. Second, because it shows how cybercriminals insist on exploiting every vulnerability there is. It's indeed possible that malicious entities are now trying to trick victims into disclosing more personally identifiable information (PII) on fake Equifax settlement websites.

We then used the Domain Research Suite (DRS) to show how potential targets can avoid falling prey to instances of phishing and cybersquatting attacks.

Table of Contents

The Attack: Phishers Are Not Done with the Biggest Financial Services Data Breach of All Time

The financial services sector is a lucrative target for cyber attackers, especially now that nearly all transactions are done online. Compared with other industries, the sector is hit by 300 times more security incidents. From one incident in 2017, the number of breaches rose to 25 in 2018. These figures underscore the importance of risk mitigation strategies for financial service providers, given that cybercriminals continuously devise ways to steal PII.

The Equifax data breach affected close to 143 million account holders in the U.S. and more than 400,000 in the U.K. The stolen PII included customers' complete names, birth dates, telephone numbers, email addresses, and Social Security numbers. The attackers also got hold of the credit card numbers of at least 209,000 of the service provider's customers.

Equifax reported the breach in September 2017 and after two years agreed to a global settlement amounting to $425 million. That isn't the end of the story, however. Phishers jumped at the chance to scam those who had already lost their PII. Several fake Equifax settlement websites cropped up, intending to do more harm.

The Victim

Equifax is among the three major credit bureaus or credit reporting agencies (CRAs) in the U.S. It collects information from more than 800 million consumers and over 88 million businesses across the globe. It builds reports for customers to establish their credit histories. While it does not directly gather information from customers, it does keep confidential records provided by banks, credit card companies, and employers.

The Attack Vector

Scammers are targeting Equifax breach victims with emails touting links to phishing sites where they can supposedly file for settlement claims.

The Case Facts: Exploiting Web Platform Vulnerabilities

In 2017, the Equifax breach started with an initial hack of its consumer complaint portal. The attackers exploited an unpatched Apache Struts vulnerability that allowed them to carry out random commands remotely.

A patch for the said bug has been available since March 2017, so how did Equifax still succumb to the breach? Take a look at the following investigation details:

- **November 2016:** The Secure Sockets Layer (SSL) certificate on the consumer complaint portal expired.
- **8 March 2017:** Equifax's security staff learned of a critical vulnerability in specific versions of Apache Struts from the U.S. Computer Emergency Readiness Team (CERT) at the U.S. Department of Homeland Security.
- **9 March 2017:** Equifax circulated news of the vulnerability through an internal alert to more than 400 company employees. The developer who was aware of the company's use of Apache Struts software was not included in the 400-person email distribution list. His manager was on the distribution list but failed to forward it to anyone on his team. As such, the

key developer never received the alert.

- **14 March 2017:** Equifax added new rules to its intrusion prevention system (IPS) to help thwart efforts to exploit the vulnerability. None of its subsequent scans identified the vulnerable version of Apache Struts running on its network. But since it lacked a comprehensive inventory of its IT assets, it did not know that the vulnerable software version remained on its system.
- **13 May 2017:** The hackers first entered Equifax's online dispute portal. They had 78 days to maneuver around the target's network undetected.
- **29 July 2017:** Equifax confirmed the breach's occurrence on its network.
- **31 July 2017:** The CEO was alerted to the compromise.
- **15 August 2017:** Consumer PII was likely stolen on this date.
- **22 August 2017:** The CEO notified the Board of Directors about the incident.
- **7 September 2017:** Equifax publicly announced the breach.

The findings of the investigative team proved an oversight on Equifax's part.

Cleaning Up After the Fact

Apart from installing new SSL certificates on its systems in July 2017, Equifax set up a website—equifaxsecurity2017.com—to provide breach remediation resources to its affected customers. Unfortunately, this site was spoofed by phishers, which potentially worsened matters for the victims. It didn't help that Equifax's official social media accounts mistakenly directed people to securityequifax2017.com as well. They were, however, fortunate that the site's owner redirected more than 200,000 visitors to the proper Equifax site.

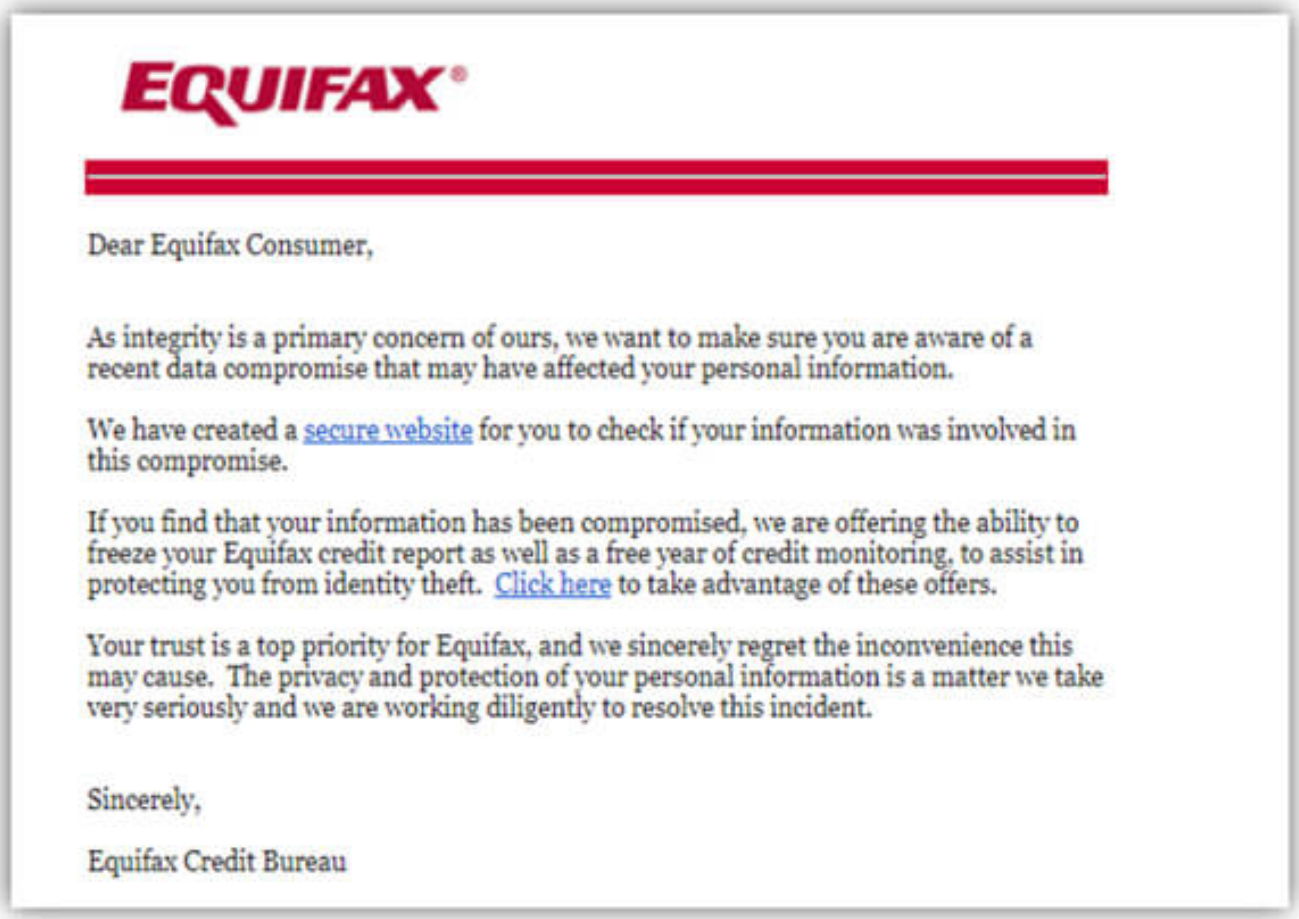
At present, Equifax has to deal with fake versions of its breach settlement site. Just this July, both the Federal Trade Commission (FTC) and Equifax released memos informing victims of ongoing phishing campaigns against Equifax settlement claimants.

Possible Solution: Preventing Phishing with the Domain Research Suite

Scammers are always on the lookout for websites to spoof so they can effectively lure victims into parting with their login credentials. The promise of getting remuneration for the 2017 Equifax breach is just one of their many social engineering tricks. And while it is every individual's responsibility to take care of his/her online credentials, we all know that phishing works because targets are convinced of the seeming authenticity of the emails and sites related to campaigns.

In this case, organizations may be able to take matters into their own hands as they don't want their customers to suffer more than they already have. How? By making sure that their brands are not used in phishing campaigns.

Let's take the Equifax breach settlement case as an example. Attackers who created spoofed versions of the site typically sent breach victims an email that looks like this:



EQUIFAX®

Dear Equifax Consumer,

As integrity is a primary concern of ours, we want to make sure you are aware of a recent data compromise that may have affected your personal information.

We have created a secure website for you to check if your information was involved in this compromise.

If you find that your information has been compromised, we are offering the ability to freeze your Equifax credit report as well as a free year of credit monitoring, to assist in protecting you from identity theft. Click here to take advantage of these offers.

Your trust is a top priority for Equifax, and we sincerely regret the inconvenience this may cause. The privacy and protection of your personal information is a matter we take very seriously and we are working diligently to resolve this incident.

Sincerely,

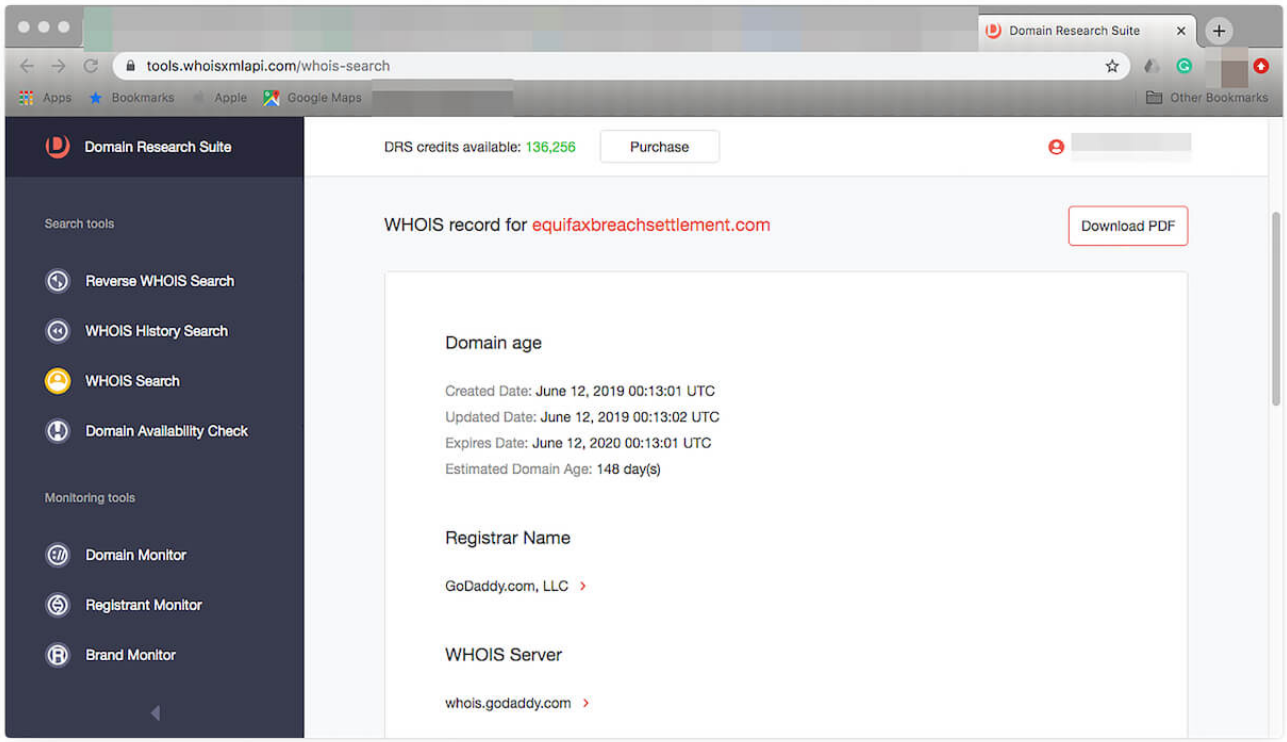
Equifax Credit Bureau

Source: https://blog.knowbe4.com/scam-of-the-week-equifax-settlement-phishing

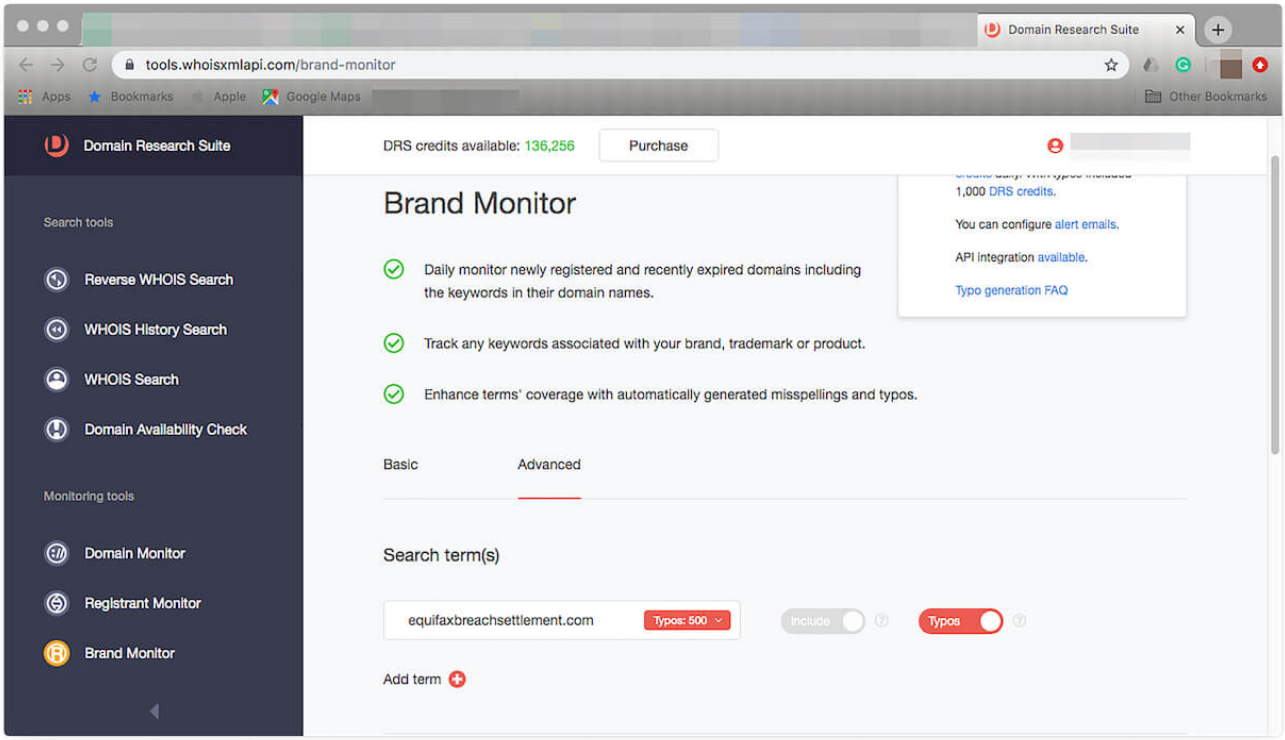
One way companies like Equifax can prevent breach victims from suffering further damage is educating customers about phishing. They can, for instance, help clients spot differences between a real and a fake email. It is also possible to pool a list of potential phishing sites and domains used in phishing emails and warn customers not to click URLs embedded in fraudulent communications. One tool that can help credit reporting agencies and other financial institutions to do that is DRS. Here's how it's done.

- 1. Log in to the dashboard found at https://tools.whoisxmlapi.com/reverse-whois-search with your WhoisXML API credentials.
- 2. We know that the real Equifax breach settlement website's URL is equifaxbreachsettlement.com. So, let's take a look at its WHOIS record using WHOIS Search, which is part of DRS. Click WHOIS Search on the dashboard menu on the left. Type "equifaxbreachsettlement.com" into the

input field and click Search. You should see this:

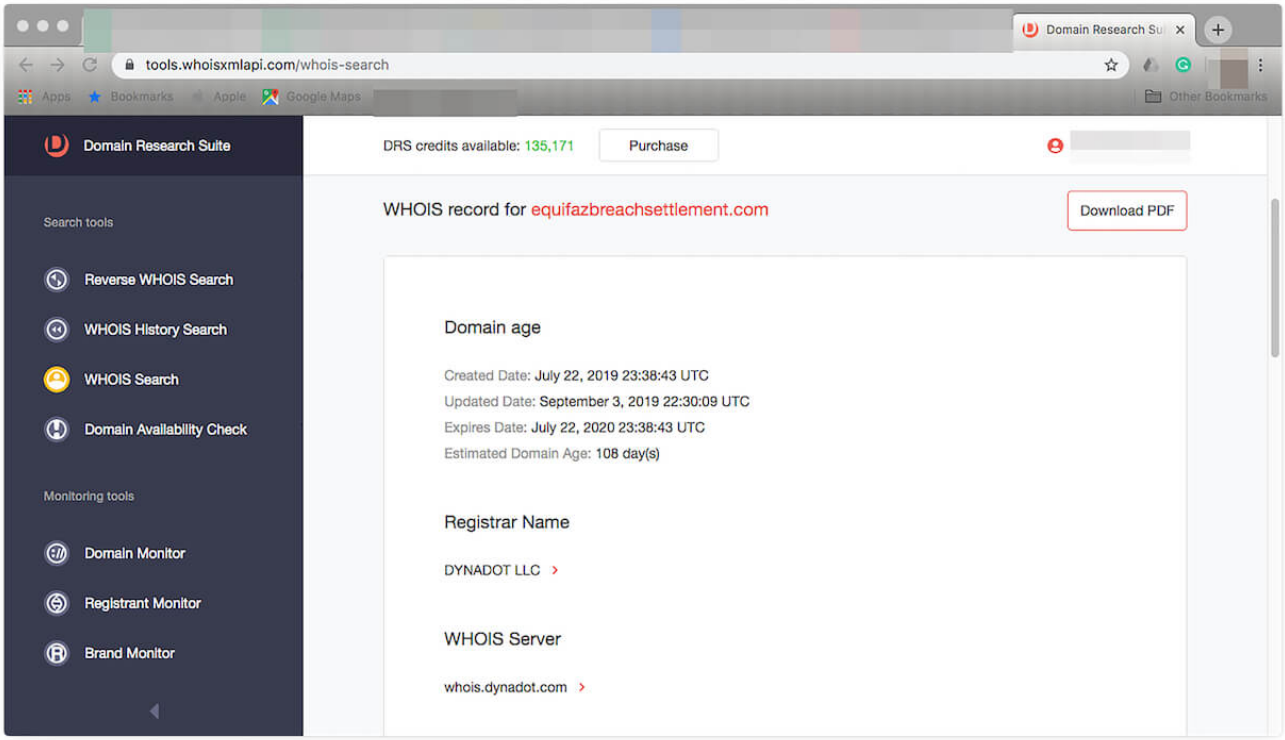


- 3. Now, let's use Brand Monitor — another DRS component—to spot potential fake versions of the Equifax data breach settlement site. Just choose Brand Monitor on the DRS menu on the left. Once in Brand Monitor, choose the Advanced tab. Type "equifaxbreachsettlement.com" into the input field and toggle the Typos feature on. The tool instantly tells you that 500 misspelled variations of the domain would be included in your tracker. Any of these could be potential phishing sites.



- 4. Then, click the Add to monitoring button to get the results. This step adds the domain to your tracker. A list of the misspelled domain variants is shown after 24 hours. A sample in JSON format is shown below.

- 5. Let’s take a look at a suspiciously looking domain from among the results such as equifazbreachsettlement[.]com. Click WHOIS Search from the DRS menu on the left to do further research. This would help confirm if Equifax owns it.



- 6. A comparison with the real Equifax data breach settlement site's WHOIS record details reveals the following differences:

Detail	**equifaxbreachsettlement.com (Real Domain)**	**equifazbreachsettlement[.]com (Misspelled Domain Variant)**
Created date	12 June 2019 13:01 UTC	22 July 2019 23:38:43 UTC
Updated date	12 June 2019 13:02 UTC	3 September 2019 22:30:09 UTC
Expires	12 June 2020 13:01 UTC	22 July 2020 23:38:43 UTC
Estimated domain age	148 days	108 days
Registrar name	GoDaddy.com, LLC	DYNADOT LLC
WHOIS server	whoisgodaddy.com	whois.dynadot.com
Nameservers	PDNS13.DOMAINCONTROL.COM PDNS14.DOMAINCONTROL.COM	ns1.dynadot.com ns2.dynadot.com
Status	clientTransferProhibited clientUpdateProhibited clientRenewProhibited clientDeleteProhibited	clientTransferProhibited

Registrant organization	JND Legal Administration	Super Privacy Service LTD c/o Dynadot
Registrant state/province	Washington	California
Registrant country	UNITED STATES	UNITED STATES
Administrative country	UNITED STATES	UNITED STATES
Technical country	UNITED STATES	UNITED STATES

- 7. A closer look at the WHOIS records of the two domains shows that equifazbreachsettlement[.]com is probably not owned by Equifax and is most likely unsafe to access. Then again, users would only land on this site if they mistyped the real settlement site's URL or clicked a link that pointed to it. The fact that it was anonymously registered could also be a means for its owner to stay under the authorities' radar. To prevent access to the most likely malicious site, you may find it a good idea to include it in your blacklist.
- 8. Should the owner of equifazbreachsettlement[.]com turn out to be a phisher, including his/her name in Registrant Monitor for tracking may also be a good idea. We know that phishers always register several domains when they run campaigns. Registrant Monitor would alert you every time he/she registers a domain. You can include all of his/her domains in your blacklist as well. Note, however, that like Brand Monitor, Registrant Monitor issues the first set of results after 24 hours, but you should see your latest tracker in the list.
- 9. We continue our investigation with Screenshot API which allows you to take screenshot of a malicious site or domain without ever visiting it. By using the tool, we found that equifazbreachsettlement[.]com immediately redirects to ww25.aquafaxbreachsettlement[.]com. These redirected domains appear to be a money collector parking page:

- 10. Although parking pages for ad money collection is legal in general, doing it through domain name typosquatting is not a benign act. This is especially true if the page is viewed by someone with moderate IT skills, e.g. elderly people who intend to file a claim and can be easily misled to other pages. While we cannot confirm this is the case for the domain at hand, parking pages may also hide phishing pages that show up only if they are visited with a URL string containing a token in the link of a phishing message. This is a good way of hiding them from crawlers, robots, and investigators. In conclusion, you can never know what might be behind a parking page.

Concluding Thoughts: Lessons Learned from the Equifax Breach

Financial service providers are prime cyber attack targets because they directly

deal with money. Three out of the top 10 most-spoofed brands—PayPal (top 2), Bank of America (top 5), and CIBC (top 7)—are from the industry. What's more, half of the 200,000 phishing domains recorded between December 2018 and May 2019 targeted the sector.

What these numbers show is that the Equifax data breach story isn't just an isolated case. Some of the most significant attacks we have seen against organizations in the sector include:

- **Capital One:** Just this July, a former Amazon Web Services (AWS) engineer was arrested for orchestrating the breach that affected 100 million Capital One customers in the U.S. and another 6 million in Canada.
- **Heartland Payment Systems:** In January 2009, this attack exposed the records of 130 million customers and left the processor an estimated settlement bill of $140 million.
- **JPMorgan Chase:** In 2014, this attack affected 7 million small businesses and 76 million households.

Given the financial services threat landscape, providers have to be at the top of their game with robust approaches to cybersecurity. Lax procedures, as shown, can result in massive data breaches. And even settling damages, as the Equifax case reveals, can make matters worse.

Here are some specific actions financial entities can take:

- Proactively tackle identified vulnerabilities as sometimes all it takes for letting hackers in is a system misconfiguration. They can use tools like a threat intelligence platform as an aid to detect commonly exploited attack vectors.
- Stop attackers from squatting their sites. They can work with applications like the Domain Research Suite and its components to detect new domain registrations that are likely to serve as an accessory to phishing and other fraudulent ends.

- As a means to further study suspicious domains, cybersecurity teams can rely on Domain Reputation API to calculate risk scores and block all communications to and from suspicious domains like the ones used to host fake settlement websites to avoid further danger.

For more information about how WhoisXML API tools can help mitigate and prevent data breaches resulting from phishing, cybersquatting, and other domain name abuses, feel free to contact us at support@whoisxmlapi.com.